BS ISO 18788:2015+A1:2024

BSI Standards Publication

Management system for private security operations — Requirements with guidance for use

Documents
Document Sharing Hub

Full document details: BS ISO 18788:2015+A1:2024

National foreword

This British Standard is the UK implementation of ISO 18788:2015+A1:2024. It supersedes BS ISO 18788:2015, which is withdrawn.

The start and finish of text introduced or altered by amendment is indicated in the text by tags. Tags indicating changes to ISO text carry the number of the ISO amendment. For example, text altered by ISO amendment 1 is indicated by A1⟩ ⟨A1.

The UK participation in its preparation was entrusted to Technical Committee GW/8, Security Managements Systems in Complex Environments.

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

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2024
Published by BSI Standards Limited 2024

ISBN 978 0 539 30754 2

ICS 03.080.20; 13.310

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

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 September 2015.

Amendments/corrigenda issued since publication

Date	Text affected
31 March 2024	Implementation of ISO amendment 1:2024

AVA Documents
Document Sharing Hub

Full document details: BS ISO 18788:2015+A1:2024

INTERNATIONAL STANDARD

ISO 18788: 2015+A1

First edition
2015-09-15

Amendment 1
2024-02

Management system for private security operations — Requirements with guidance for use

Système de management des opérations de sécurité privée — Exigences et lignes directrices pour son utilisation

Reference number
ISO 18788:2015(E)

Documents
Document Sharing Hub

© ISO 2015

Full document details: BS ISO 18788:2015+A1:2024

COPYRIGHT PROTECTED DOCUMENT

© ISO 2015, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

© ISO 2015 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO 18788:2015+A1:2024

Contents

Page

Foreword ..... **v**
Introduction ..... **vi**
1 Scope **1**
2 Normative references **2**
3 Terms and definitions **2**
4 Context of the organization **14**
4.1 Understanding the organization and its context 14
4.1.1 General 14
4.1.2 Internal context 14
4.1.3 External context 14
4.1.4 Supply chain and subcontractor mapping and analysis 15
4.1.5 Defining risk criteria 15
4.2 Understanding the needs and expectations of stakeholders 15
4.3 Determining the scope of the security operations management system 16
4.4 Security operations management system 16
5 Leadership **17**
5.1 Leadership and commitment 17
5.1.1 General 17
5.1.2 Statement of Conformance 17
5.2 Policy 18
5.3 Organization roles, responsibilities and authorities 18
6 Planning **19**
6.1 Actions to address risks and opportunities 19
6.1.1 General 19
6.1.2 Legal and other requirements 20
6.1.3 Internal and external risk communication and consultation 20
6.2 Security operations objectives and planning to achieve them 21
6.2.1 General 21
6.2.2 Achieving security operations and risk treatment objectives 22
7 Support **22**
7.1 Resources 22
7.1.1 General 22
7.1.2 Structural requirements 23
7.2 Competence 24
7.2.1 General 24
7.2.2 Competency identification 24
7.2.3 Training and competence evaluation 25
7.2.4 Documentation 25
7.3 Awareness 25
7.4 Communication 25
7.4.1 General 25
7.4.2 Operational communications 26
7.4.3 Risk communications 26
7.4.4 Communicating complaint and grievance procedures 26
7.4.5 Communicating whistle-blower policy 26
7.5 Documented information 27
7.5.1 General 27
7.5.2 Creating and updating 27
7.5.3 Control of documented information 28
8 Operation **29**
8.1 Operational planning and control 29

AVA Documents
Document Sharing Hub

© ISO 2015 – All rights reserved

Full document details: BS ISO 18788:2015+A1:2024

8.1.1 General 29
8.1.2 Performance of security-related functions 30
8.1.3 Respect for human rights 30
8.1.4 Prevention and management of undesirable or disruptive events 30
8.2 Establishing norms of behaviour and codes of ethical conduct 30
8.3 Use of force 30
8.3.1 General 30
8.3.2 Weapons authorization 31
8.3.3 Use of force continuum 31
8.3.4 Less-lethal force 32
8.3.5 Lethal force 32
8.3.6 Use of force in support of law enforcement 32
8.3.7 Use of force training 33
8.4 Apprehension and search 33
8.4.1 Apprehension of persons 33
8.4.2 Search 33
8.5 Operations in support of law enforcement 33
8.5.1 Law enforcement support 33
8.5.2 Detention operations 34
8.6 Resources, roles, responsibility and authority 34
8.6.1 General 34
8.6.2 Personnel 34
8.6.3 Procurement and management of weapons, hazardous materials and munitions 36
8.6.4 Uniforms and markings 36
8.7 Occupational health and safety 36
8.8 Incident management 36
8.8.1 General 36
8.8.2 Incident monitoring, reporting and investigations 37
8.8.3 Internal and external complaint and grievance procedures 37
8.8.4 Whistle-blower policy 38

9 Performance evaluation 38
9.1 Monitoring, measurement, analysis and evaluation 38
9.1.1 General 38
9.1.2 Evaluation of compliance 39
9.1.3 Exercises and testing 39
9.2 Internal audit 39
9.3 Management review 40
9.3.1 General 40
9.3.2 Review input 40
9.3.3 Review output 41

10 Improvement 41
10.1 Nonconformity and corrective action 41
10.2 Continual improvement 42
10.2.1 General 42
10.2.2 Change management 42
10.2.3 Opportunities for improvement 42

Annex A (informative) **Guidance on the use of this International Standard 43**

Annex B (informative) **General principles 89**

Annex C (informative) **Getting started – Gap analysis 92**

Annex D (informative) **Management systems approach 93**

Annex E (informative) **Qualifiers to application 96**

Bibliography 97

© ISO 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 18788:2015+A1:2024

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

The committee responsible for this document is Technical Committee ISO/TC 292, *Security and resilience*.

© ISO 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 18788:2015+A1:2024

Introduction

0.1 General

This International Standard specifies requirements and provides guidance for organizations conducting or contracting security operations. It provides a business and risk management framework for the effective conduct of security operations. It is specifically applicable to any organization operating in circumstances where governance may be weak or rule of law undermined due to human or naturally caused events. Using a Plan-Do-Check-Act approach, this International Standard provides a means for organizations conducting or contracting security operations to demonstrate:

a) adequate business and risk management capacity to meet the professional requirements of clients and other stakeholders;

b) assessment and management of the impact of their activities on local communities;

c) accountability to law and respect for human rights;

d) consistency with voluntary commitments to which the organization subscribes.

NOTE 1 This International Standard is not intended to place additional burdens on general guarding services outside these specific circumstances.

This International Standard draws on provisions from, and provides a mechanism to demonstrate compliance with, relevant principles, legal obligations, voluntary commitments and good practices of the following documents:

— *Montreux Document on Pertinent International Legal Obligations and Good Practices for States related to Operations of Private Military and Security Companies during Armed Conflict* (09/2008);

— *International Code of Conduct for Private Security Service Providers (ICoC)* (11/2010);

— *Guiding Principles on Business and Human Rights; Implementing the United Nations "Protect, Respect and Remedy" Framework (2011)*.

NOTE 2 The *International Code of Conduct* reflects 1) the legal obligations and good practices of the *Montreux Document* (including the provisions detailing the human rights law and humanitarian law applicable to security providers), and 2) the relevant principles of the "Protect, Respect and Remedy" framework as operationalized in the *Guiding Principles on Business and Human Rights*.

NOTE 3 Although specifically addressed to states and armed conflict, the *Montreux Document* is also instructive in similar conditions and for other entities.

Private security operations perform an important role in protecting state and non-state clients engaged in relief, recovery, and reconstruction efforts; commercial business operations; development activities; diplomacy; and military activity. This International Standard is applicable for any type of organization conducting or contracting security operations, particularly in environments where governance might be weak or the rule of law undermined due to human or naturally caused events. The organization, in close coordination with legitimate clients and state actors, needs to adopt and implement the standards necessary to ensure that human rights and fundamental freedoms are adhered to in order to safeguard lives and property, and that untoward, illegal, and excessive acts are prevented. This means that organizations engaging in security operations manage the utilization of tactics, techniques, procedures, and equipment, including weapons, in such a way as to achieve both operational and risk management objectives. The purpose of this International Standard is to improve and demonstrate consistent and predictable security operations maintaining the safety and security of their clients within a framework that aims to ensure respect for human rights, national and international laws, and fundamental freedoms.

NOTE 4 For the purposes of this International Standard, national laws can include those of the country of the organization, countries of its personnel, the country of operations and country of the client.

© ISO 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 18788:2015+A1:2024

This International Standard builds on the principles found in international human rights law and international humanitarian law (IHL). It provides auditable criteria and guidance that support the objectives of the *Montreux Document on Pertinent International Legal Obligations and Good Practices for States related to Operations of Private Military and Security Companies during Armed Conflict* of 17 September 2008; the *International Code of Conduct for Private Security Service Providers (ICoC)* of 9 November 2010; and the *Guiding Principles on Business and Human Rights; Implementing the United Nations "Protect, Respect and Remedy" Framework 2011*.

This International Standard provides a means for organizations, and their clients, to implement the legal obligations and recommended good practices of the *Montreux Document* and to provide demonstrable commitment, conformance and accountability to respect the principles outlined in the *ICoC*, as well as other international documents related to human rights and voluntary commitments, such as *Guiding Principles on Business and Human Rights; Implementing the United Nations "Protect, Respect and Remedy" Framework 2011* and *Voluntary Principles on Security and Human Rights* (2000).

Given that organizations that conduct and contract security operations have become important elements for supporting peace, stability, development and commercial efforts in regions where the capacity of societal institutions have become overwhelmed by human and natural caused disruptive events, their operations face a certain amount of risk. The challenge is to determine how to cost-effectively manage risk while meeting the organization's strategic and operational objectives within a framework that protects the safety, security and human rights of internal and external stakeholders, including clients and affected communities. Organizations need to conduct their business and provide services in a manner that respects human rights and laws. Therefore, they – and their clients – have an obligation to carry out due diligence to identify risks, prevent incidents, mitigate and remedy the consequences of incidents, report them when they occur, and take corrective and preventive actions to avoid a reoccurrence. This International Standard provides a basis for clients to differentiate which organizations can provide services at the highest professional standards consistent with stakeholder needs and rights.

Protecting both tangible and intangible assets is a critical task for the viability, profitability and sustainability of any type of organization (public, private, or not-for-profit). This transcends the protection of just physical, human and information assets; it also includes protecting the image and reputation of companies and their clients. Protecting assets requires a combination of strategic thinking, problem solving, process management and the ability to implement programmes and initiatives to correspond with the context of the organization's operations and their risks.

Core to the success of implementing this International Standard is embedding the values of the *Montreux Document* and the *ICoC* into the culture and range of activities of the organization. Integrating these principles into enterprise-wide management of the organization requires a long-term commitment to cultural change by top management, including leadership, time, attention and resources – both monetary and physical. By using this International Standard, organizations can demonstrate their commitment to integration of the principles of the *Montreux Document* and the *ICoC* into their management system and their day-to-day operations. This International Standard is designed to be integrated with other management systems within an organization (e.g. quality, safety, organizational resilience, environmental, information security and risk standards). One suitably designed management system can thus fulfil the requirements of all these standards.

In this International Standard, the following verbal forms are used (further details can be found in the ISO/IEC Directives, Part 2):

— "shall" indicates an auditable requirement: it is used to indicate requirements strictly to be followed in order to conform to the document and from which no deviation is permitted;

— "should" indicates a recommendation: it is used to indicate that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required, or that (in the negative form) a certain possibility or course of action is deprecated but not prohibited;

— "may" indicates a permission: it is used to indicate a course of action permissible within the limits of the document;

© ISO 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 18788:2015+A1:2024

— "can" indicates a possibility or a capability: it is used for statements of possibility and capability, whether material, physical or causal.

Information marked as "NOTE" is for guidance in understanding or clarifying the associated requirement.

Items presented in lists are not exhaustive, unless otherwise stated, and the order of the list does not specify a sequence or priority, unless so stated. The generic nature of this International Standard allows for an organization to include additional items, as well as designation of a sequence or priority based on the specific operating conditions and circumstances of the organization.

0.2 Human rights protection

While states and their entities need to respect, uphold and protect human rights, all segments of society (public, private and not-for-profit) have a shared responsibility to act in a way that respects and does not negatively impact upon human rights and fundamental freedoms (see Clause A.2).

Clients and organizations conducting and contracting security operations have a shared responsibility to establish policies and controls to assure conformance with the principles of the *Montreux Document* and the *ICoC*. By implementing this International Standard, organizations can:

a) establish and maintain a transparent governance and management framework in order to deter, detect, monitor, address ,and prevent the occurrence and recurrence of incidents that have adverse impacts on human rights and fundamental freedoms;

b) identify and operate in accordance with applicable international, national and local laws and regulations;

c) conduct comprehensive internal and external risk assessments associated with safety, security and human rights risks;

d) implement risk control measures that support the rule of law, respect human rights of stakeholders, protect the interests of the organization and its clients, and provide professional services;

e) ensure suitable and sufficient operational controls based on identified risks are implemented and managed to enhance the occupational health and safety and the welfare of persons working on behalf of the organization;

f) effectively communicate and consult with public and private stakeholders;

g) conduct effective screening and training of persons working on the organizations behalf;

h) ensure that the use of force is reasonably necessary, proportional and lawful;

i) conduct performance evaluations of services rendered and the achievement of objectives;

j) develop and implement systems for reporting and investigating allegations of violations of international law, local law or human rights, as well as mitigating and remedying the consequences of undesirable or disruptive events.

0.3 Management systems approach

The management systems approach encourages organizations to analyse organizational and stakeholder requirements and define processes that contribute to success. It provides a basis for establishing policies and objectives, establishing procedures to realize desired outcomes, and measuring and monitoring the achievement of objectives and outcomes. A management system provides the framework for continual improvement to increase the likelihood of enhancing the professionalism of security operations while assuring the protection of human rights and fundamental freedoms. It provides confidence to both the organization and its clients that the organization is able to manage its contractual, security and legal obligations, as well as respect human rights. Additional information on management systems standards is provided in Annex D.

Figure 1 illustrates the management systems approach used in this International Standard.

© ISO 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 18788:2015+A1:2024

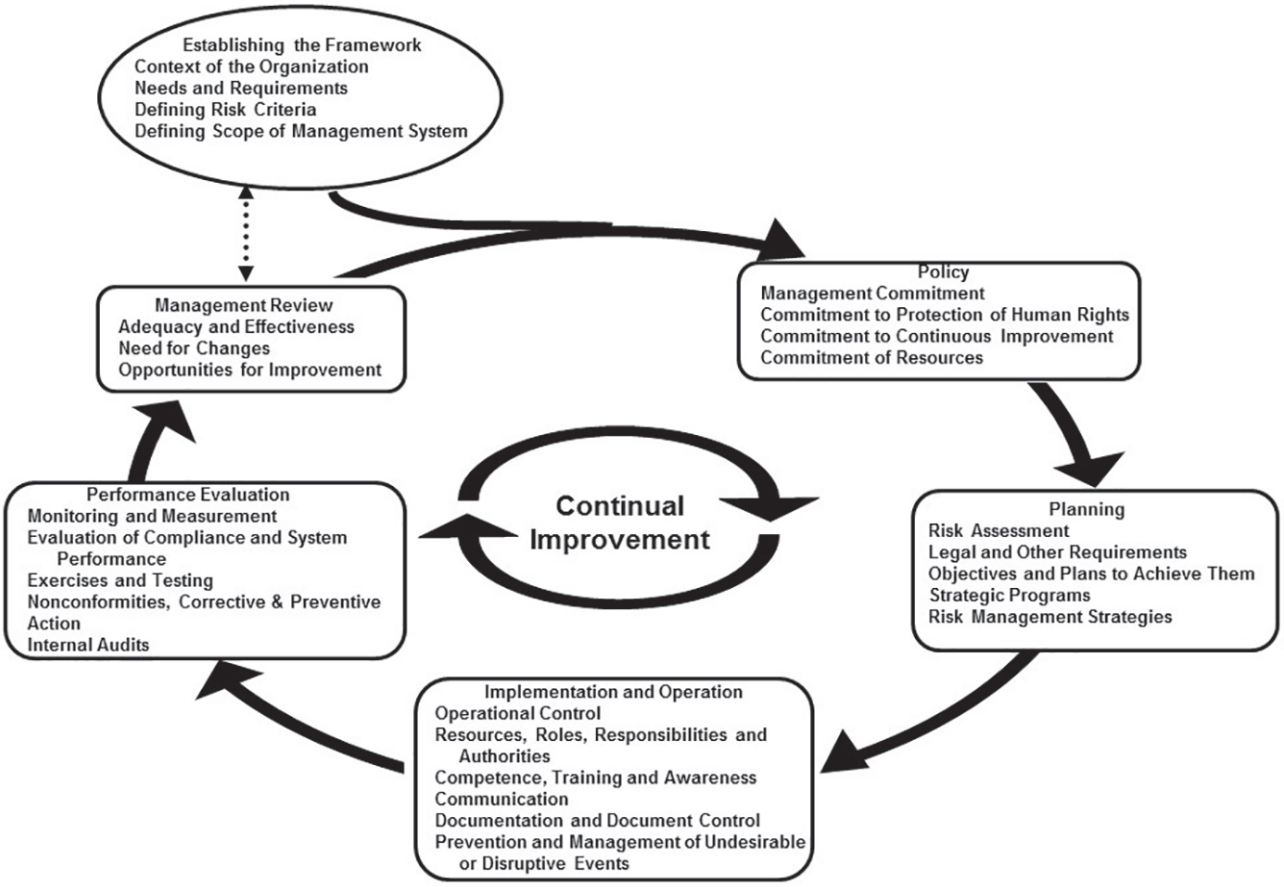

Figure 1 — Security operations management system (SOMS) flow diagram

© ISO 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 18788:2015+A1:2024

Documents
Document Sharing Hub

Management system for private security operations — Requirements with guidance for use

1 Scope

This International Standard provides a framework for establishing, implementing, operating, monitoring, reviewing, maintaining and improving the management of security operations.

It provides the principles and requirements for a security operations management system (SOMS). This International Standard provides a business and risk management framework for organizations conducting or contracting security operations and related activities and functions while demonstrating:

a) conduct of professional security operations to meet the requirements of clients and other stakeholders;

b) accountability to law and respect for human rights;

c) consistency with voluntary commitments to which it subscribes.

This International Standard also provides a means for organizations and those who utilize security services to demonstrate commitment to the relevant legal obligations, as well as to the good practices provided in the *Montreux Document on Pertinent International Legal Obligations and Good Practices for States related to Operations of Private Military and Security Companies during Armed Conflict*, and conformance with the principles and commitments outlined in the *International Code of Conduct for Private Security Service Providers (ICoC)*. This International Standard is specifically aimed at any organization operating in circumstances where governance may be weak and the rule of law undermined due to human or naturally caused events.

NOTE 1 This International Standard is not intended to place additional burdens on general guarding services outside these specific circumstances.

Applicable laws can include all kinds of laws including, but not limited to, national, regional, international or customary laws. It is the sole responsibility of the user of this International Standard to determine the applicable laws and to abide by them. This International Standard does not provide any advice or guidance concerning applicable laws, the conflict between laws, or the interpretation of the laws, codes, treaties or documents mentioned within it.

This International Standard is applicable to any organization that needs to:

a) establish, implement, maintain and improve an SOMS;

b) assess its conformity with its stated security operations management policy;

c) demonstrate its ability to consistently provide services that meet client needs and are in conformance with applicable international, national and local laws and human rights requirements.

The generic principles and requirements of this International Standard are intended to be incorporated into any organization's integrated management system based on the Plan-Do-Check-Act (PDCA) model; it is not intended to promote a uniform approach to all organizations in all sectors. The design and implementation of security operations plans, procedures and practices are expected to take into

© ISO 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 18788:2015+A1:2024

account the particular requirements of each organization: its objectives, context, culture, structure, resources, operations, processes, products and services.

NOTE 2 Consistent with the goal of public and private organizations to comply with all applicable laws and respect human rights, it is intended that clients refer to this International Standard when retaining private security services. It is intended that organizations use this International Standard's management system principles and requirements to conduct their own due diligence and management of services and to construct their contracting and contract administration process to support conformance with this International Standard.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

Montreux Document on Pertinent International Legal Obligations and Good Practices for States related to Operations of Private Military and Security Companies during Armed Conflict (09/2008)[1)]

International Code of Conduct for Private Security Service Providers(ICoC) (11/2010)[2)]

Guiding Principles on Business and Human Rights; Implementing the United Nations "Protect, Respect and Remedy" Framework 2011[3)]

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO Guide 73:2009 and the following apply.

3.1
asset
anything that has tangible or intangible value to an *organization* (3.34)

Note 1 to entry: Tangible assets include human (considered the most valued in this International Standard), physical and environmental assets.

Note 2 to entry: Intangible assets include information, brand and reputation.

3.2
audit
systematic, independent and documented *process* (3.43) for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled

Note 1 to entry: An audit can be an internal audit (first party) or an external audit (second party or third party), and it can be a combined audit (combining two or more disciplines).

Note 2 to entry: An internal audit is conducted by the *organization* (3.34) itself, or by an external party on its behalf.

Note 3 to entry: "Audit evidence" and "audit criteria" are defined in ISO 19011.

3.3
auditor
person who conducts an *audit* (3.2)

[SOURCE: ISO 19011:2011, 3.8]

1) Available from: http://www.un.org/ga/search/view_doc.asp?symbol=A/63/467

2) Available from: http://icoca.ch/

3) Available from: http://www.ohchr.org/documents/issues/business/A.HRC.17.31.pdf

© ISO 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 18788:2015+A1:2024

3.4
client
entity or person that hires, has formerly hired, or intends to hire an *organization* (3.34) to perform *security operations* (3.63) on its behalf, including, as appropriate, where such an organization subcontracts with another company or local forces

EXAMPLE Consumer; contractor; end-user; retailer; beneficiary; purchaser.

Note 1 to entry: A client can be internal (e.g. another division) or external to the organization.

3.5
competence
ability to apply knowledge and skills to achieve intended results

3.6
communication and consultation
continual and iterative *processes* (3.43) that an *organization* (3.34) conducts to provide, share or obtain information, and to engage in dialogue with *stakeholders* (3.24) and others regarding the management of *risk* (3.50)

Note 1 to entry: The information can relate to the existence, nature, form, *likelihood* (3.27), severity, evaluation, acceptability, treatment or other aspects of the management of risk and *security operations management* (3.64).

Note 2 to entry: Consultation is a two-way process of informed communication between an organization and its stakeholders or others on an issue, prior to making a decision or determining a direction on that issue. Consultation is:

— a process which impacts on a decision through influence rather than power; and

— an input to decision making, not joint decision making.

[SOURCE: ISO Guide 73:2009, 3.2.1, modified]

3.7
community
group of associated *organizations* (3.34), individuals and groups sharing common interests

Note 1 to entry: Impacted communities are the groups of people and associated organizations affected by the provision of security services, projects or operations.

3.8
conformity
fulfilment of a *requirement* (3.45)

3.9
continual improvement
recurring activity to enhance *performance* (3.36)

3.10
consequence
outcome of an *event* (3.19) affecting *objectives* (3.33)

Note 1 to entry: An event can lead to a range of consequences.

Note 2 to entry: A consequence can be certain or uncertain and can have positive or negative effects on objectives.

Note 3 to entry: Consequences can be expressed qualitatively or quantitatively.

Note 4 to entry: Initial consequences can escalate through cumulative effects from one event setting off a chain of events.

Note 5 to entry: Consequences are graded in terms of the magnitude or severity of the impacts.

[SOURCE: ISO Guide 73:2009, 3.6.1.3, modified]

© ISO 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 18788:2015+A1:2024

3.11
correction
action to eliminate a detected *nonconformity* (3.32)

3.12
corrective action
action to eliminate the cause of a *nonconformity* (3.32) and to prevent recurrence

3.13
criticality analysis
process (3.43) designed to systematically identify and evaluate an *organization's* (3.34) *assets* (3.1) based on the importance of its mission or function, the group of people at *risk* (3.50), or the significance of an *undesirable* (3.75) or *disruptive event* (3.15) on the organization's ability to meet expectations

3.14
critical control point
CCP
point, step, or *process* (3.43) at which controls can be applied and a threat or hazard can be prevented, eliminated, or reduced to acceptable levels

3.15
disruptive event
occurrence or change that interrupts planned activities, operations, or functions, whether anticipated or unanticipated

3.16
documented information
information required to be controlled and maintained by an *organization* (3.34) and the medium on which it is contained

Note 1 to entry: Documented information can be in any format and media, and from any source.

Note 2 to entry: Documented information can refer to:

— the *management system* (3.29), including related *processes* (3.43);

— information created in order for the organization to operate (documentation);

— evidence of results achieved (*records* (3.44)).

3.17
effectiveness
extent to which planned activities are realized and planned results achieved

3.18
exercises
activities to evaluate *security operations management* (3.64) programmes, rehearsing the roles of team members and staff, and testing the *organization's* (3.34) systems (e.g. technology, reporting protocols, administration) to demonstrate security operations management, *competence* (3.5) and capability

Note 1 to entry: Exercises include activities performed for the purpose of training and conditioning persons working on behalf of the organization in appropriate responses with the goal of achieving maximum *performance* (3.36).

3.19
event
occurrence or change of a particular set of circumstances

Note 1 to entry: The nature, *likelihood* (3.27), and *consequence* (3.10) of an event cannot be fully knowable.

Note 2 to entry: An event can be one or more occurrences, and can have several causes.

Note 3 to entry: The likelihood associated with the event can be determined.

© ISO 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 18788:2015+A1:2024

Note 4 to entry: An event can consist of a non-occurrence of one or more circumstances.

Note 5 to entry: An event with a consequence is sometimes referred to as an "*incident* (3.21)".

[SOURCE: ISO Guide 73:2009, 3.5.1.3, modified]

3.20
human rights risk analysis
HRRA
process (3.43) to identify, analyse, evaluate and document human rights-related *risks* (3.50) and their impacts, in order to manage risk and to mitigate or prevent adverse human rights impacts and legal infractions

Note 1 to entry: The HRRA is part of the *organization's* (3.34) *requirement* (3.45) to undertake human rights due diligence to identify, prevent, mitigate and account for how it addresses impacts on human rights.

Note 2 to entry: The HRRA is framed by relevant international human rights principles and conventions and forms a fundamental part of the organization's overall *risk assessment* (3.54).

Note 3 to entry: The HRRA includes an analysis of the severity of actual and potential human rights impacts that the organization may cause or contribute to through its *security operations* (3.63), or which may be linked directly to the organization's operations, projects or services through its business relationships. The HRRA process should include consideration of the operational context, draw on the necessary human rights expertise, and involve direct, meaningful engagement with those *stakeholders* (3.24) whose rights may be at risk.

Note 4 to entry: The analysis of the *consequences* (3.10) of adverse human rights impacts are measured and prioritized in terms of the severity of the impacts.

Note 5 to entry: HRRAs should be undertaken at regular intervals, recognizing that human rights risks may change over time.

Note 6 to entry: HRRAs will vary in complexity with the size of the organization, the risk of severe human rights impacts and the nature and context of its operations.

Note 7 to entry: The HRRA is sometimes referred to as a "human rights risk assessment", a "human rights impact assessment", or a "human rights risk and impact assessment". The language used in this International Standard is consistent with risk vocabulary used in ISO standards.

3.21
incident
event (3.19) with *consequences* (3.10) that has the capacity to cause loss of life, harm to *assets* (3.1), or negatively impact human rights and fundamental freedoms of internal or external *stakeholders* (3.24)

3.22
inherently dangerous property
property that, if in the hands of an unauthorized individual, would create an imminent threat of death or serious bodily harm

EXAMPLE Lethal weapons; ammunition; explosives; chemical agents; biological agents and toxins; nuclear or radiological materials.

3.23
integrity
property of safeguarding the accuracy and completeness of *assets* (3.1)

[SOURCE: ISO/IEC 27000:2014, 2.40, modified]

© ISO 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 18788:2015+A1:2024

3.24
interested party
stakeholder
person or *organization* (3.34) that can affect, be affected by, or perceive itself to be affected by a decision or activity

Note 1 to entry: A decision maker can be a stakeholder.

Note 2 to entry: Impacted communities and local populations are considered to be external stakeholders.

Note 3 to entry: Throughout this International Standard, the use of the term "stakeholder" is consistent with its usage in *security operations* (3.63).

3.25
key performance indicator
KPI
quantifiable measure that an *organization* (3.34) uses to gauge or compare *performance* (3.36) in terms of meeting its strategic and operational *objectives* (3.33)

3.26
less-lethal force
degree of force used that is less likely to cause death or serious injury to overcome violent encounters and appropriately meet the levels of resistance encountered

3.27
likelihood
chance of something happening

Note 1 to entry: In *risk management* (3.58) 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 to entry: 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: ISO Guide 73:2009, 3.6.1.1]

3.28
management plan
clearly defined and documented plan of action, typically covering the key personnel, *resources* (3.48), services and actions needed to implement the *event* (3.19) management *process* (3.43)

3.29
management system
set of interrelated or interacting elements of an *organization* (3.34) to establish *policies* (3.38) and *objectives* (3.33) and *processes* (3.43) to achieve those objectives

Note 1 to entry: A management system can address a single discipline or several disciplines.

Note 2 to entry: The system elements include the organization's structure, roles and responsibilities, *planning* (3.37), operation.

Note 3 to entry: The scope of a management system may include the whole of the organization, specific and identified functions of the organization, specific and identified sections of the organization, or one or more functions across a group of organizations.

Note 4 to entry: Management systems are used by organizations to develop their policies and to put these into effect via objectives and *targets* (3.72), using:

— an organizational structure where the roles, responsibilities, authorities, etc., of people are defined;

© ISO 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 18788:2015+A1:2024

— systematic processes and associated *resources* (3.48) to achieve the objectives and targets;

— *measurement* (3.30) and evaluation methodology to assess *performance* (3.36) against the objectives and targets, with feedback of results used to plan improvements to the system;

— a *review* (3.49) process to ensure problems are corrected and opportunities for improvement are recognized and implemented, when justified.

3.30
measurement
process (3.43) to determine a value

3.31
monitoring
determining the status of a system, a *process* (3.43) or an activity

Note 1 to entry: To determine the status, there may be a need to check, supervise or critically observe.

3.32
nonconformity
non-fulfilment of a *requirement* (3.45)

3.33
objective
result to be achieved

Note 1 to entry: An objective can be strategic, tactical, or operational.

Note 2 to entry: Objectives can relate to different disciplines (such as financial, health and safety and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and *process* (3.43)).

Note 3 to entry: An objective can be expressed in other ways, e.g. as an intended outcome, a purpose, an operational criterion, as a *security operations objective* (3.65) or by the use of other words with similar meaning (e.g. aim, goal, or *target* (3.72)).

Note 4 to entry: In the context of *security operations management* (3.64) systems, security operations objectives are set by the *organization* (3.34), consistent with the *security operations policy* (3.66), to achieve specific results.

3.34
organization
person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its *objectives* (3.33)

Note 1 to entry: The concept of organization includes, but is not limited to sole-trader, company, corporation, firm, enterprise, authority, partnership, charity or institution, government or public entity, or part or combination thereof, whether incorporated or not, public or private.

3.35
outsource (verb)
make an arrangement where an external *organization* (3.34) performs part of an organization's function or *process* (3.43)

Note 1 to entry: An external organization is outside the scope of the *management system* (3.29), although the outsourced function or process is within the scope.

3.36
performance
measurable result

Note 1 to entry: Performance can relate either to quantitative or qualitative findings.

Note 2 to entry: Performance can relate to the management of activities, *processes* (3.43), products (including services), systems or *organizations* (3.34).

AVA Documents
Document Sharing Hub

© ISO 2015 – All rights reserved

Full document details: BS ISO 18788:2015+A1:2024

3.37
planning
part of management focused on setting *security operations objectives* (3.65) and specifying necessary operational *processes* (3.43) and related *resources* (3.48) to fulfil the security operations objectives

3.38
policy
intentions and direction of an *organization* (3.34), as formally expressed by its *top management* (3.74)

3.39
prevention
measures that enable an *organization* (3.34) to avoid, preclude or limit the impact of an *undesirable* (3.75) or potentially *disruptive event* (3.15)

3.40
preventive action
action to eliminate the cause of a potential *nonconformity* (3.32) or other undesirable potential situation

Note 1 to entry: There can be more than one cause for a potential nonconformity.

Note 2 to entry: Preventive action is taken to prevent occurrence whereas *corrective action* (3.12) is taken to prevent recurrence.

[SOURCE: ISO 9000:2015, 3.12.1]

3.41
private security service provider
private security company
PSC
organization (3.34) which conducts or contracts *security operations* (3.63) and whose business activities include the provision of *security* (3.62) services either on its own behalf or on behalf of another

Note 1 to entry: Private security companies and private security service providers are collectively known as PSCs.

Note 2 to entry: PSCs provide services to *clients* (3.4) with the aim of ensuring their security and that of others.

Note 3 to entry: PSCs typically work in circumstances where governance may be weak or rule of law undermined due to human or naturally caused *events* (3.19) and provide services for which personnel may be required to carry weapons in the *performance* (3.36) of their duties in accordance with the terms of their contract.

Note 4 to entry: Examples of security services provided by PSCs may include: guarding; close protection; physical protection measures; security awareness and training; risk, security and threat assessment; the provision of protective and defensive measures for individuals compounds, diplomatic and residential perimeters; escort of transport; and policy analysis.

Note 5 to entry: For the purposes of this International Standard, a joint venture is considered part of the organization.

Note 6 to entry: For the purposes of this International Standard, PSC operations fall within the legal boundaries for private security operations.

3.42
procedure
specified way to carry out an activity or a *process* (3.43)

Note 1 to entry: Procedures can be documented or not.

[SOURCE: ISO 9000:2015, 3.4.5]

3.43
process
set of interrelated or interacting activities which transforms inputs into outputs

© ISO 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 18788:2015+A1:2024

3.44
record
document stating results achieved or providing evidence of activities performed

Note 1 to entry: Records can be used, for example, to document traceability and to provide evidence of verification, *preventive action* (3.40) and *corrective action* (3.12).

Note 2 to entry: Generally records need not be under revision control.

[SOURCE: ISO 9000:2015, 3.8.10]

3.45
requirement
need or expectation that is stated, generally implied or obligatory

Note 1 to entry: "Generally implied" means that it is custom or common practice for the *organization (3.34)* and *stakeholders* (3.24) that the need or expectation under consideration is implied.

Note 2 to entry: A specified requirement is one that is stated, for example in *documented information* (3.16).

3.46
residual risk
risk (3.50) remaining after *risk treatment* (3.61)

Note 1 to entry: Residual risk can contain unidentified risk.

Note 2 to entry: Residual risk can also be known as "retained risk".

[SOURCE: ISO Guide 73:2009, 3.8.1.6]

3.47
resilience
adaptive capacity of an *organization* (3.34) in a complex and changing environment

[SOURCE: ISO Guide 73:2009, 3.8.1.7]

3.48
resources
assets (3.1), facilities, equipment, materials, products, or waste that has potential value and can be used

[SOURCE: ANSI/ASIS SPC.1-2009]

3.49
review
activity undertaken to determine the suitability, adequacy and *effectiveness* (3.17) of the *management system* (3.29) and its component elements to achieve established *objectives* (3.33)

3.50
risk
effect of uncertainty on *objectives* (3.33)

Note 1 to entry: An effect is a deviation from the expected — positive or negative.

Note 2 to entry: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an *event* (3.19), its *consequence* (3.10), or *likelihood* (3.27).

Note 3 to entry: Risk is often characterized by reference to potential "events" (as defined in ISO Guide 73:2009, 3.5.1.3) and "consequences" (as defined in ISO Guide 73:2009, 3.6.1.3), or a combination of these.

Note 4 to entry: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated "likelihood" (as defined in ISO Guide 73:2009, 3.6.1.1) of occurrence.

© ISO 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 18788:2015+A1:2024

Note 5 to entry: Objectives can have different aspects (such as protection of human rights, security management, legal compliance, financial, health and safety and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and *process* (3.43)).

Note 6 to entry: Risks may be due to intentional, unintentional and natural sources.

3.51
risk acceptance
informed decision to take a particular *risk* (3.50)

Note 1 to entry: Risk acceptance can occur without *risk treatment* (3.61) or during the *process* (3.43) of risk treatment.

Note 2 to entry: Accepted risks are subject to *monitoring* (3.31) and *review* (3.49).

[SOURCE: ISO Guide 73:2009, 3.7.1.6]

3.52
risk analysis
process (3.43) to comprehend the nature of *risk* (3.50) and to determine the level of risk

Note 1 to entry: Risk analysis provides the basis for *risk evaluation* (3.56) and decisions about *risk treatment* (3.61).

Note 2 to entry: Risk analysis includes risk estimation.

[SOURCE: ISO Guide 73:2009, 3.6.1]

3.53
risk appetite
amount and type of *risk* (3.50) that an *organization* (3.34) is prepared to pursue, retain or take

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

3.54
risk assessment
overall *process* (3.43) of *risk identification* (3.57), *risk analysis* (3.52) and *risk evaluation* (3.56)

[SOURCE: ISO Guide 73:2009, 3.4.1]

3.55
risk criteria
terms of reference against which the significance of a *risk* (3.50) is evaluated

Note 1 to entry: Risk criteria are based on organizational *objectives* (3.33), and external and internal context.

Note 2 to entry: Risk criteria can be derived from standards, laws, policies and other *requirements* (3.45).

[SOURCE: ISO Guide 73:2009, 3.3.1.3]

3.56
risk evaluation
process (3.43) of comparing the results of *risk analysis* (3.52) with *risk criteria* (3.55) to determine whether the *risk* (3.50) and/or its magnitude is acceptable or tolerable

Note 1 to entry: Risk evaluation assists in the decision about *risk treatment* (3.61).

[SOURCE: ISO Guide 73:2009, 3.7.1]

3.57
risk identification
process (3.43) of finding, recognizing and describing *risks* (3.50)

Note 1 to entry: Risk identification involves the identification of risk sources, *events* (3.19), their causes and their potential *consequences* (3.10).

© ISO 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 18788:2015+A1:2024

Note 2 to entry: Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and *stakeholder's* (3.24) needs.

[SOURCE: ISO Guide 73:2009, 3.5.1]

3.58
risk management
coordinated activities to direct and control an *organization* (3.34) with regard to *risk* (3.50)

[SOURCE: ISO Guide 73:2009, 2.1]

3.59
risk register
record (3.44) of information about identified *risks* (3.50)

Note 1 to entry: Compilation for all risks identified, analysed and evaluated in the *risk assessment* (3.54) *process* (3.43), including information on the risk register includes information on *likelihood* (3.27), *consequences* (3.10), treatments and risk owners.

3.60
risk tolerance
organization's (3.34) or *stakeholder's* (3.24) readiness to bear the *risk* (3.50) after *risk treatment* (3.61) in order to achieve its *objectives* (3.33)

Note 1 to entry: Risk tolerance can be influenced by *client* (3.4), stakeholder, legal, or regulatory *requirements* (3.45).

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

3.61
risk treatment
process (3.43) to modify *risk* (3.50)

Note 1 to entry: 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;

— removing the risk source;

— changing the *likelihood* (3.27);

— changing the *consequences* (3.10);

— sharing the risk with another party or parties (including contracts and risk financing); and

— retaining the risk by informed decision.

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

Note 3 to entry: Risk treatment can create new risks or modify existing risks.

[SOURCE: ISO Guide 73:2009, 3.8.1]

3.62
security
condition of being protected against hazards, threats, *risks* (3.50), or loss

Note 1 to entry: In the general sense, security is a concept similar to safety. The distinction between the two is an added emphasis on being protected from dangers that originate from outside.

Note 2 to entry: The term "security" means that something not only is secure, but that it has been secured.

[SOURCE: ANSI/ASIS SPC.1-2009]

© ISO 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 18788:2015+A1:2024

3.63
security operations
activities and functions related to the protection of people, tangible and intangible *assets* (3.1)

Note 1 to entry: Security operations may require the carrying and operating a weapon in the *performance* (3.36) of their duties.

Note 2 to entry: The concept includes the *ICoC* definition of security services: guarding and protection of persons and objects, such as convoys, facility, designated sites, property or other places (whether armed or unarmed) or any other activity for which the personnel of companies are required to carry or operate a weapon in the performance of their duties.

3.64
security operations management
coordinated activities to direct and control an *organization* (3.34) with regard to *security operations* (3.63)

Note 1 to entry: Direction and control with regard to security operations management generally includes establishment of the *policy* (3.38), *planning* (3.37) and *objectives* (3.33) directing operational *processes* (3.43) and *continual improvement* (3.9).

3.65
security operations objective
something sought, or aimed for, related to *security operations* (3.63)

Note 1 to entry: Security operations objectives are generally based on the *organization's* (3.34) *security operations policy* (3.66)

Note 2 to entry: Security operations objectives are generally specified for relevant functions and levels in the organization.

3.66
security operations policy
overall intentions and direction of an *organization* (3.34) related to *security operations* (3.63) as formally expressed by *top management* (3.74)

Note 1 to entry: Generally, the security operations policy is consistent with the overall *policy* (3.38) of the organization and provides a framework for the setting of *security operations objectives* (3.65).

Note 2 to entry: *Security operations management* (3.64) principles presented in this International Standard can form a basis for the establishment of a security operations policy consistent with the principles and obligations outlined in the *ICoC* and *Montreux Document*.

3.67
security operations programme
ongoing management and governance *process* (3.43) supported by *top management* (3.74) and resourced to ensure that the necessary steps are taken to coordinate the efforts achieve the *objectives* (3.33) of the *security operations management (3.64)* system

3.68
security operations personnel
persons working on behalf of the *organization* (3.34) who are engaged directly or indirectly in *security operations* (3.63)

3.69
self-defence
protection of one's person or property against some injury attempted by another

[SOURCE: Black's Law Dictionary]

© ISO 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 18788:2015+A1:2024

3.70
subcontracting
contracting with an external party to fulfil an obligation arising out of an existing contract

Note 1 to entry: When a party is contracted to perform a range of services, it may subcontract one or more of those services to a "subcontractor" or local forces.

Note 2 to entry: Subsidiaries of a parent company may be considered a subcontracting *organization* (3.34).

3.71
supply chain
two-way relationship of *organizations* (3.34), people, *processes* (3.43), logistics, information, technology and *resources* (3.48) engaged in activities and creating value from the sourcing of materials through the delivery of products or services

Note 1 to entry: The supply chain may include vendors, subcontractors, manufacturing facilities, logistics providers, internal distribution centres, distributors, wholesalers and other entities that lead to the end user.

3.72
target
detailed *performance* (3.36) *requirement* (3.45) applicable to the *organization* (3.34) (or parts thereof) that arises from the *objectives* (3.33) and that needs to be set and met in order to achieve those objectives

3.73
threat analysis
process (3.43) of identifying, qualifying and quantifying the potential cause of an unwanted *event* (3.19), which may result in harm to individuals, *assets* (3.1), a system or *organization* (3.34), the environment, or the *community* (3.7)

3.74
top management
person or group of people who directs and controls an *organization* (3.34) at the highest level

Note 1 to entry: Top management has the power to delegate authority and provide *resources* (3.48) within the organization.

Note 2 to entry: If the scope of the *management system* (3.29) covers only part of an organization, then top management refers to those who direct and control that part of the organization.

Note 3 to entry: Top management may be referred to as the leadership of the organization.

3.75
undesirable event
occurrence or change that has the potential to cause loss of life, harm to tangible or intangible *assets* (3.1), or negatively impact the human rights and fundamental freedoms of internal or external *stakeholders* (3.24)

3.76
use of force continuum
increasing or decreasing the level of force applied as a continuum relative to the response of the adversary, using the amount of force reasonable and necessary

Note 1 to entry: The amount of force used should be the minimum reasonable amount needed to eliminate the threat presented, thereby minimizing the *risk* (3.50) and severity of any injury that may occur.

Note 2 to entry: Escalation/de-escalation of force response with a level of force should be appropriate to the situation at hand, acknowledging that the response may move from one part of the continuum to another in a matter of seconds.

© ISO 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 18788:2015+A1:2024

3.77
vulnerability analysis
process (3.43) of identifying and quantifying something that creates susceptibility to a source of *risk* (3.50) that can lead to a *consequence* (3.10)

4 Context of the organization

4.1 Understanding the organization and its context

4.1.1 General

The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its SOMS.

The design and implementation of a management system framework is based on an understanding of the organization and its internal and external context of operation. Therefore, the organization shall define and document its internal and external context, including its supply chain and subcontractors. These factors shall be taken into account when establishing, implementing and maintaining the organization's SOMS, and assigning priorities.

The organization shall evaluate internal and external factors that can influence the way in which the organization will manage risk. [A1] The organization shall determine whether climate change is a relevant issue. [A1]

4.1.2 Internal context

The organization shall identify, evaluate and document its internal context, including:

a) objectives, strategies and business mission of the organization;

b) policies, plans and guidelines to achieve objectives;

c) governance, roles and responsibilities, and accountabilities;

d) overall risk management strategy;

e) internal stakeholders;

f) values, ethos and culture;

g) information flow and decision-making processes;

h) capabilities, resources and assets;

i) procedures, processes and practices;

j) activities, functions, services and products;

k) brand and reputation.

4.1.3 External context

The organization shall define and document its external context, including:

a) the cultural and political context;

b) legal, regulatory, technological, economic, natural and competitive environment;

c) contractual agreements, including other organizations within the contract scope;

d) infrastructure dependencies and operational interdependencies;

© ISO 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 18788:2015+A1:2024

e) supply chain and contractor relationships and commitments;

f) key issues and trends that may impact on the processes and/or objectives of the organization;

g) perceptions, values, needs and interests of external stakeholders (including local communities in areas of operation);

h) operational forces and lines of authority.

In establishing its external context, the organization shall ensure that the objectives and concerns of external stakeholders are considered when developing security operations management criteria.

4.1.4 Supply chain and subcontractor mapping and analysis

The organization shall identify and document its upstream and downstream supply chain, particularly its use of subcontractors who may have an impact on risk, and the potential to cause an undesirable or disruptive event. Managing supply chain risk shall be included in an organization's overall security operations management programme where significant risks have been identified and there is a potential to cause an undesirable or disruptive event. The organization shall define and document the level in their supply chain and subcontractors to include in their security operations management programme.

4.1.5 Defining risk criteria

The organization shall define and document criteria to evaluate the significance of risk. The risk criteria shall reflect the organization's values, objectives and resources. When defining the risk criteria the organization shall consider:

a) critical activities, functions, services, products and stakeholder relationships;

b) the operating environment and inherent uncertainty in operating in environments of weakened governance or rule of law;

c) the potential impact related to a disruptive or undesirable event;

d) legal and regulatory requirements and other requirements (e.g. contractual obligations, human rights commitments) to which the organization subscribes;

e) the organization's overall risk management policy;

f) the nature and types of threats and consequences that can occur to its assets, business and operations;

g) how the likelihood, consequences and level of risk will be determined;

h) needs of and impacts on stakeholders – particularly life, safety and human rights (see A.6.1.2.3);

i) reputational and perceived risk;

j) level of risk tolerance or risk aversion of the organization and its clients;

k) how combinations and sequence of multiple risks will be taken into account.

While risk criteria are established at the beginning of the risk assessment process, they are dynamic and shall be continually monitored and reviewed for appropriateness.

4.2 Understanding the needs and expectations of stakeholders

The organization shall determine

— the stakeholders that are relevant to the SOMS;

— the relevant requirements of these stakeholders.

© ISO 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 18788:2015+A1:2024

Top management shall ensure that internal and external stakeholder interests are identified, evaluated and documented, in order to achieve the objectives of its contracts and minimize risks.

When identifying internal and external stakeholder needs and requirements, the organization shall consider its:

a) stakeholders' risk appetite;

b) contractual obligations specified by the client;

c) legal and regulatory requirements and voluntary commitments;

d) human rights responsibilities and impacts relevant to the services provided;

e) impact on and interactions with external stakeholders (such as local communities, clients and other security providers);

f) records and documentation requirements for delivery of services and non-conformances.

A1 NOTE Relevant stakeholders can have requirements related to climate change. A1

4.3 Determining the scope of the security operations management system

The organization shall determine the boundaries and applicability of the SOMS to establish its scope (i.e. the whole organization, or one or more of its constituent parts or functions). The organization shall define the scope of the SOMS in terms of and appropriate to its size, nature and complexity from a perspective of continual improvement.

When determining this scope, the organization shall consider:

— the organization's objectives, external and internal issues referred to in 4.1.2;

— the requirements referred to in 4.1.3;

— risk factors that could adversely affect the operations and activities of the organization within the context of their potential likelihood and consequences.

The scope shall be available as documented information. The organization shall identify all elements of its operations where the SOMS apply and exclusions if applicable.

The organization shall define the scope consistent with the need to respect applicable international, national and local laws and human rights, while protecting and preserving the integrity of the organization, including relationships with stakeholders.

A Statement of Applicability shall define the relevant clauses of Annex A that apply to the organization's scope, legal and contractual obligations and operating environment based on its risk assessment and human rights impact analysis (see 6.1). Where the risk assessment and human rights analysis identify specific clauses of Annex A as being relevant and applicable to the organization's scope, legal and contractual obligations and operating environment, these shall be addressed and implemented by the organization. Specific exclusions and their justifications shall be documented.

4.4 Security operations management system

The organization shall establish, implement, maintain and continually improve an SOMS, including the processes needed and their interactions, in accordance with the requirements of this International Standard. The organization shall establish documented desired outcomes for its management system and continually improve its effectiveness in accordance with the requirements set out in this International Standard.

The SOMS shall implement the principles and commitments of the *ICoC*.

When the organization contracts, subcontracts or outsources any process or activity that falls within the scope of application of this International Standard, the organization shall ensure that control of such subcontracted or outsourced process or activity shall be identified and managed within its SOMS.

© ISO 2015 – All rights reserved
AVA Documents Document Sharing Hub
Full document details: BS ISO 18788:2015+A1:2024

5 Leadership

5.1 Leadership and commitment

5.1.1 General

Top management shall demonstrate leadership and commitment with respect to the development and implementation of the SOMS and continually improving its effectiveness by:

— ensuring that the security operations policy and security operations objectives are established and are compatible with the strategic direction of the organization;

— ensuring the integration of the SOMS requirements into the organization's business processes;

— ensuring that the resources needed for the SOMS are available to establish, implement, operate, monitor, review, maintain and improve the SOMS;

— communicating the importance of effective security operations management and of conforming to the SOMS requirements and its legal responsibilities;

— ensuring that the SOMS achieves its intended outcome(s);

— directing and supporting persons to contribute to the effectiveness of the SOMS;

— promoting continual improvement;

— supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility;

— conducting at planned intervals, management reviews of the SOMS.

NOTE Reference to "business" in this International Standard can be interpreted broadly to mean those activities that are core to the purposes of the organization's existence.

Top management shall provide evidence of active leadership for the SOMS by overseeing its establishment and implementation, and motivating individuals to integrate security operations consistent with respect for human rights as an integral part of the mission of the organization and its culture.

5.1.2 Statement of Conformance

Top management shall develop, document and publish a Statement of Conformance indicating the organization's commitment to and conformance with its responsibility to respect human rights as reflected in the provisions of its SOMS and the following:

a) *International Code of Conduct for Private Security Service Providers*;

b) *Montreux Document on Pertinent International Legal Obligations and Good Practices for States related to Operations of Private Military and Security Companies during Armed Conflict*;

c) *Guiding Principles on Business and Human Rights; Implementing the United Nations "Protect, Respect and Remedy" Framework 2011*;

d) any other applicable internationally recognized human rights commitments (e.g. *Voluntary Principles on Security and Human Rights*).

The Statement of Conformance also stipulates the organization's human rights expectations of its stakeholders linked directly to its operations.

The Statement of Conformance shall be:

a) documented, maintained and implemented;

© ISO 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 18788:2015+A1:2024

b) publicly available and communicated internally and externally to all relevant stakeholders;

c) visibly endorsed by top management.

5.2 Policy

Top management shall establish a security operations policy that:

— is appropriate to the purpose of the organization;

— provides a framework for setting security operations objectives

— includes a commitment to satisfy applicable legal and other requirements, including voluntary commitments to which the organization subscribes;

— includes a commitment to continual improvement of the SOMS;

— provides a commitment to respect human rights;

— provides a commitment to avoid, prevent and reduce the likelihood and consequences of disruptive or undesirable events.

The security operations policy shall:

— be available as documented information;

— be communicated within the organization;

— be communicated to all appropriate people working for or on behalf of the organization;

— be available to stakeholders, as appropriate;

— be visibly endorsed by top management;

— be reviewed at planned intervals and when significant changes occur.

5.3 Organization roles, responsibilities and authorities

Top management shall ensure that the responsibilities and authorities for relevant roles are assigned and communicated within the organization.

Top management shall assign one or more individuals within the organization who – irrespective of other responsibilities – shall have defined competencies, roles, responsibility and authority for:

a) ensuring that the SOMS conforms to the requirements of this International Standard;

b) reporting on the performance of the SOMS to top management;

c) ensuring that an SOMS is established, communicated, implemented and maintained in accordance with the requirements of this International Standard;

d) identifying, monitoring and managing the needs and expectations of stakeholders set out in 4.2;

e) ensuring that adequate resources are made available;

f) promoting awareness of SOMS requirements throughout the organization;

g) reporting on the performance of the SOMS to top managers for review and as a basis for continuous improvement.

Top management shall ensure that those responsible for implementing and maintaining the SOMS have the necessary authority and competence to do so and are held accountable for its operation.

© ISO 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 18788:2015+A1:2024

6 Planning

6.1 Actions to address risks and opportunities

6.1.1 General

When planning for the SOMS, the organization shall consider the issues referred to in 4.1.2 and the requirements referred to in 4.1.3 and determine the risks and opportunities that need to be addressed to:

— give assurance that the SOMS can achieve its intended outcome(s);

— prevent, or reduce, undesirable effects;

— achieve continual improvement.

The organization shall establish, implement and maintain a formal and documented risk assessment process for its security operations, including its relevant supply chain partners and subcontractor activities. The risk assessment process shall include:

a) risk identification – identify and assess threats, vulnerabilities, consequences and human rights risks to identify strategic, tactical and operational risks due to intentional, unintentional and natural events that have a potential for direct or indirect consequences on the organization's activities, assets, operations, functions and impacted stakeholders, as well as its ability to abide by principles of human rights;

b) risk analysis – systematically analyse risk (likelihood and consequence analysis, including human rights risk analysis) to determine those risks that have a significant impact on activities, functions, services, products, supply chain, subcontractors, stakeholder relationships, local populations and the environment;

c) risk evaluation – systematically evaluate and prioritize risk controls and treatments and their related costs to determine how to bring risk within an acceptable level consistent with risk criteria.

The organization shall:

a) document and keep this information up-to-date and secure;

b) periodically review whether the security operations management scope, policy, risk criteria and risk assessment are still appropriate given the organization's internal and external context;

c) re-evaluate risks within the context of changes within the organization or made to the organization's operating environment, procedures, functions, services, partnerships and supply chains;

d) evaluate the direct and indirect benefits and costs of options to manage risk and enhance reliability and resilience;

e) evaluate the actual effectiveness of risk treatment options post-incident and after exercises;

f) ensure that the prioritized risks and impacts are taken into account in establishing, implementing and operating its SOMS;

g) monitor and evaluate the effectiveness of risk controls and treatments.

The risk assessment shall identify activities, operations and processes that need to be managed, outputs shall include:

a) a prioritized risk register identifying treatments to manage risk;

b) justification for risk acceptance;

c) identification of critical control points (CCP);

© ISO 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 18788:2015+A1:2024

d) requirements for outsourcing and subcontractor controls.

Consistent with its security operations, the organization shall establish a process to monitor, assess, evaluate and respond to changes in the risk environment.

The organization shall plan:

a) actions to address these risks and opportunities;

b) how to:

— integrate and implement the actions into its SOMS processes;

— evaluate the effectiveness of these actions.

6.1.2 Legal and other requirements

The organization shall ensure that applicable and relevant legal and other requirements are considered and incorporated when establishing, implementing and maintaining its SOMS.

The organization shall:

a) identify applicable and relevant legal, regulatory, contractual, licensing and other requirements and commitments related to its business and security operations;

b) identify applicable human rights responsibilities relevant to its business and security operations in addition to those required under law;

c) determine how these requirements apply to its operations and those of any subcontractors or joint ventures within the scope of application of this International Standard.

The organization shall document this information and keep it up to date. It shall communicate relevant information on legal and other requirements to persons working on its behalf and other relevant third parties, including subcontractors. Organizations and their customers have a legal and ethical responsibility to comply with these obligations.

NOTE For the purposes of this International Standard, national laws can include those of the country of the organization, the countries of its personnel, the country of operations and the country of the client.

6.1.3 Internal and external risk communication and consultation

The organization shall establish, implement and maintain a formal and documented communication and consultation process with internal and external stakeholders in the risk assessment process to ensure that:

a) operational objectives and interests of the client (including the persons, organizations, communities and/or activities being protected) are understood;

b) risks are adequately identified and communicated;

c) interests of other internal and external stakeholders are understood;

d) risks and their treatments are communicated with appropriate stakeholders;

e) dependencies and linkages with subcontractors and within the supply chain are understood;

f) security operations risk assessment process interfaces with other management disciplines;

g) risk assessment is being conducted within the appropriate internal and external context and parameters relevant to the organization and its subcontractors and supply chain.

© ISO 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 18788:2015+A1:2024

6.2 Security operations objectives and planning to achieve them

6.2.1 General

The organization shall establish security operations objectives at relevant functions and levels.

The security operations objectives shall:

a) be consistent with the security operations policy;

b) be measurable (if practicable);

c) take into account applicable requirements;

d) be monitored;

e) be communicated;

f) be updated as appropriate.

The organization shall retain documented information on the security operations objectives.

When planning how to achieve its security operations objectives, the organization shall determine

— what will be done;

— what resources will be required;

— who will be responsible;

— when it will be completed;

— how the results will be evaluated.

The organization shall establish, implement and maintain documented objectives and targets to manage risks in order to anticipate, avoid, prevent, deter, mitigate, respond to and recover from disruptive or undesirable events. Documented objectives and targets shall establish internal and external expectations for the organization, its subcontractors and the supply chain that are critical to mission accomplishment, product and service delivery, and functional operations.

Objectives shall be derived from and consistent with the security operations policy and risk assessment, including the commitments to:

a) minimize risk by reducing likelihood and consequence;

b) respect international, national and local laws and human rights;

c) financial, operational and business requirements (including subcontractor and supply chain commitments);

d) continual improvement.

When establishing and reviewing its objectives and targets, an organization shall consider its financial, operational and business requirements, the legal, regulatory and other requirements, its human rights impacts, its significant risks, its technological options and the views of stakeholders.

Targets associated with the key performance indicators shall be measurable qualitatively and/or quantitatively. Targets shall be derived from and consistent with the security operations objectives and shall be:

a) to an appropriate level of detail;

b) commensurate to the risk assessment;

© ISO 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 18788:2015+A1:2024

c) specific, measurable, achievable, relevant and time-based (where practicable);

d) communicated to all appropriate employees and third parties including subcontractors and supply chain partners with the intent that these persons are made aware of their individual obligations;

e) reviewed periodically to ensure that they remain relevant and consistent with the security operations objectives and amended accordingly.

6.2.2 Achieving security operations and risk treatment objectives

The organization shall establish, implement and maintain programmes for achieving its security operations and risk treatment objectives. The programmes shall be optimized and prioritized in order to control and treat risks associated with its operations, subcontractors and supply chain. The organization shall establish, implement and maintain a formal and documented risk treatment process, which considers:

a) removing the risk source, where possible;

b) removing or reducing the likelihood of an event and its consequences;

c) removing, reducing, or mitigating harmful consequences;

d) sharing the risk with other parties, including risk insurance;

e) spreading the risk across assets and functions;

f) accepting risk or pursuing opportunities through informed decision;

g) avoiding or temporarily halting activities that give rise to the risk.

Top management shall:

a) assess the benefits and costs of options to remove, reduce, or retain risk;

b) evaluate its security operations programmes to determine if these measures have introduced new risks;

c) periodically review the risk treatment to reflect changes to the external environment, including legal, regulatory and other requirements, and changes to the organization's policy, facilities, information management system(s), activities, functions, products, services and supply chain.

7 Support

7.1 Resources

7.1.1 General

The organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the SOMS.

The organization shall consider:

a) existing, and possible additional, internal resources, capabilities and limitations;

b) which services and goods are to be sourced externally.

Resources available include relevant information, management tools, human resources including people with relevant experience and specialist skills and knowledge, technical and protective equipment and logistic support, whether internal or contracted externally.

© ISO 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 18788:2015+A1:2024