INTERNATIONAL STANDARD

ISO 18788

First edition
2015-09-15

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)

© ISO 2015



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

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

© ISO 2015 – All rights reserved

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

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

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

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

— "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

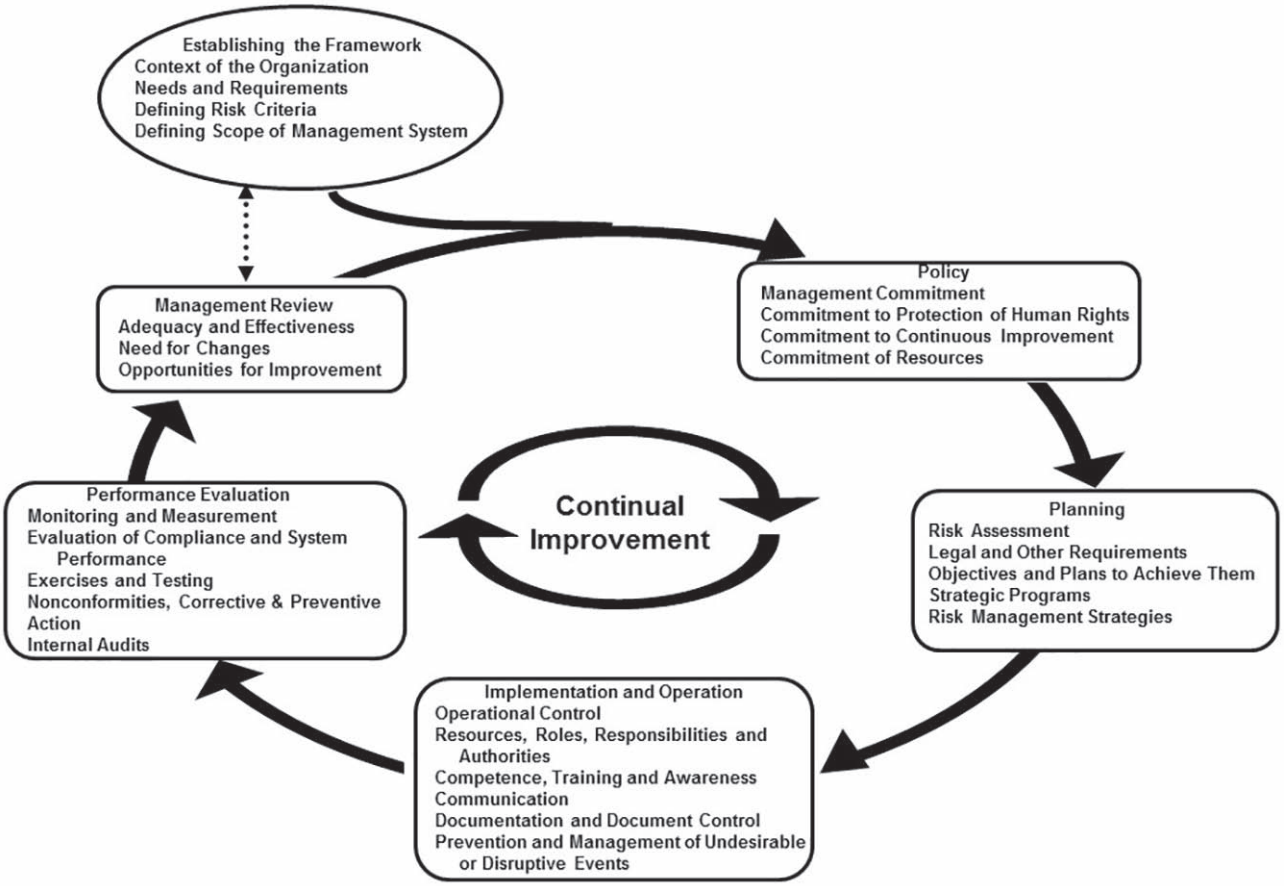


Figure 1 — Security operations management system (SOMS) flow diagram

© ISO 2015 – All rights reserved

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

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