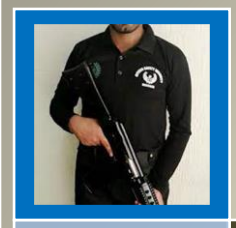
Deming Certification & Rating Pvt. Ltd.
Email: - info@demingcert.com
Contact: - 02502341257/9322728183
Website: - www.demingcert.com
No. 108, Mehta Chambers, Station Road, Novghar, Behind Tungareswar Sweet,
Vasai West, Thane District, Mumbai- 401202, Maharashtra, India



ISO 18788:2015 Management System for Private Security Operations

What is ISO 18788:2015 Management System for Private Security Operations?

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.

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.

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;
- — "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:

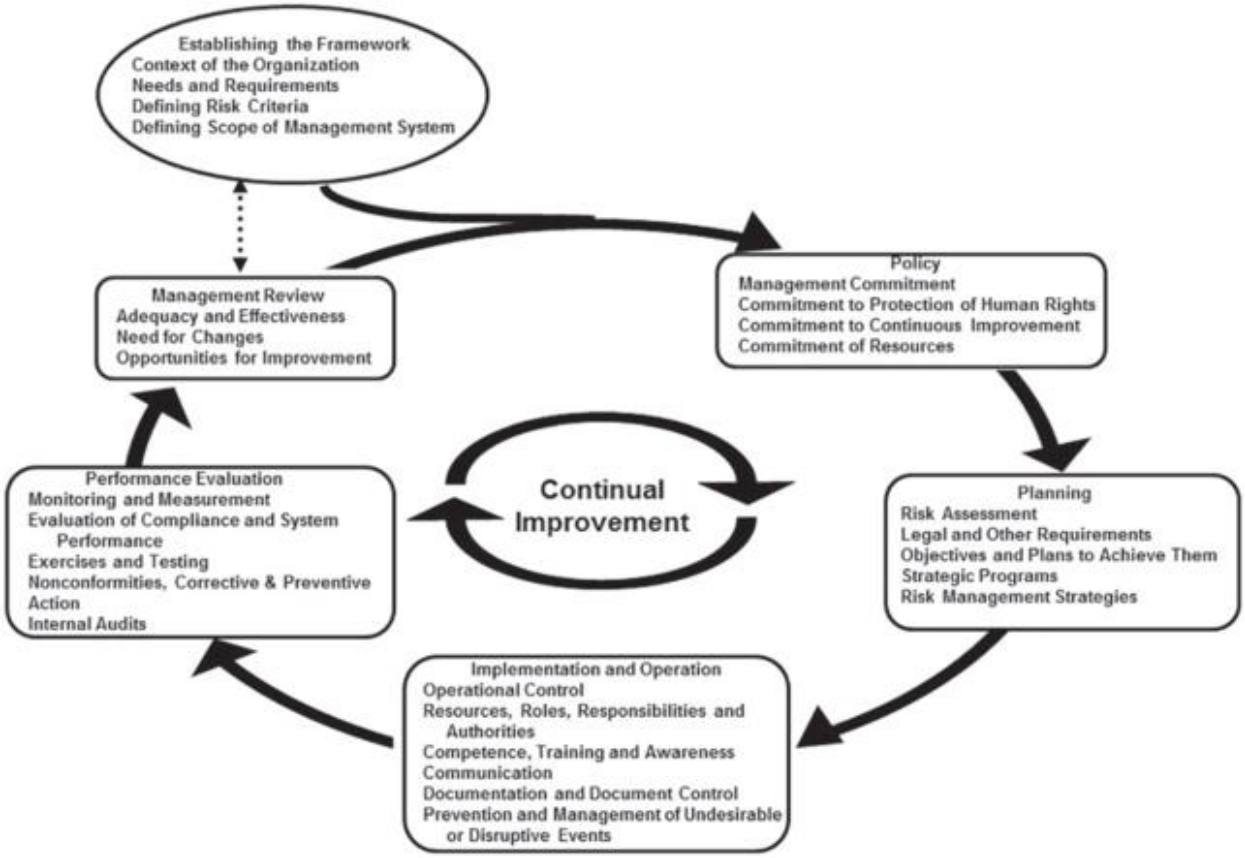
- a) establish and maintain a transparent governance and management framework in order to deter, detect, monitor, address, and prevent the occurrence and recurrence of incidents that have adverse impacts on human rights and fundamental freedoms;
- b) identify and operate in accordance with applicable 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 organization’s 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.

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



List of International Organization for Standardization standards

This is a list of published International Organization for Standardization (ISO) standards and other deliverables. For a complete and up-to-date list of all the ISO standards, see the ISO catalogue.

The standards are protected by copyright and most of them must be purchased. However, about 300 of the standards produced by ISO and IEC's Joint Technical Committee 1 (JTC 1) have been made freely and publicly available.

ISO Brand

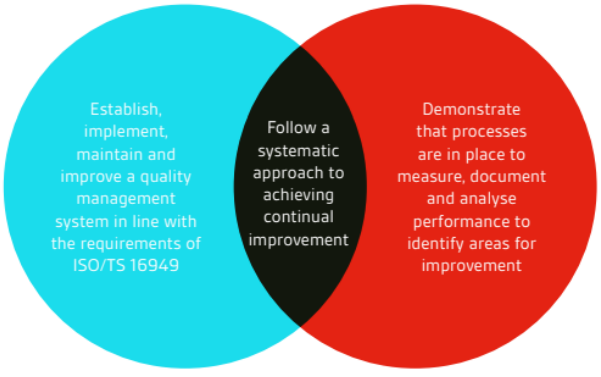
This is a dynamic list and may never be able to satisfy particular standards for completeness. You can help by adding missing items with reliable sources.

.

Which of the ISO standard provide guidelines for management system?
ISO 27001: Information Security Management System

ISO 27001 is the standard for an Information Security Management System (ISMS). The basic objective of the standard is to provide a model for establishing and maintaining an effective IT information management system based on the process approach.

The principal requirements of the standard are illustrated below:

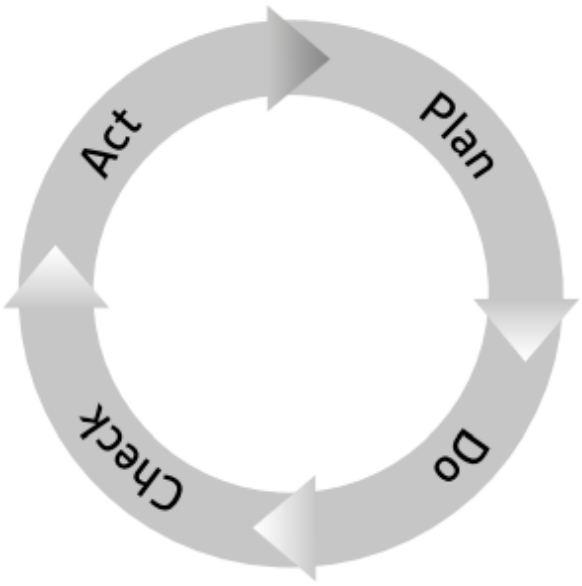


The next few pages of the guide takes you through the Plan-Do-Check-Act (PDCA) methodology, common in all ISO management systems and how DCS can help and support you on your ISO/TS 16949 journey.

Understanding the principles of continual improvement

Act

Correct and improve your plans to meet and exceed your planned results



Plan

Establish objectives and draft your plans (analyse your organization's current systems, establish overall objectives, set interim targets for review and develop plans to achieve them)

Check

Measure and monitor your actual results against your planned objectives

Do

Implement your plans within a structured management framework