BS ISO 18788:2015

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

bsi.

...making excellence a habit.™

National foreword

This British Standard is the UK implementation of ISO 18788:2015.

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 secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Published by BSI Standards Limited 2015

ISBN 978 0 580 85900 7

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

BS ISO 18788:2015

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)

COPYRIGHT PROTECTED DOCUMENT

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

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*.

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 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.

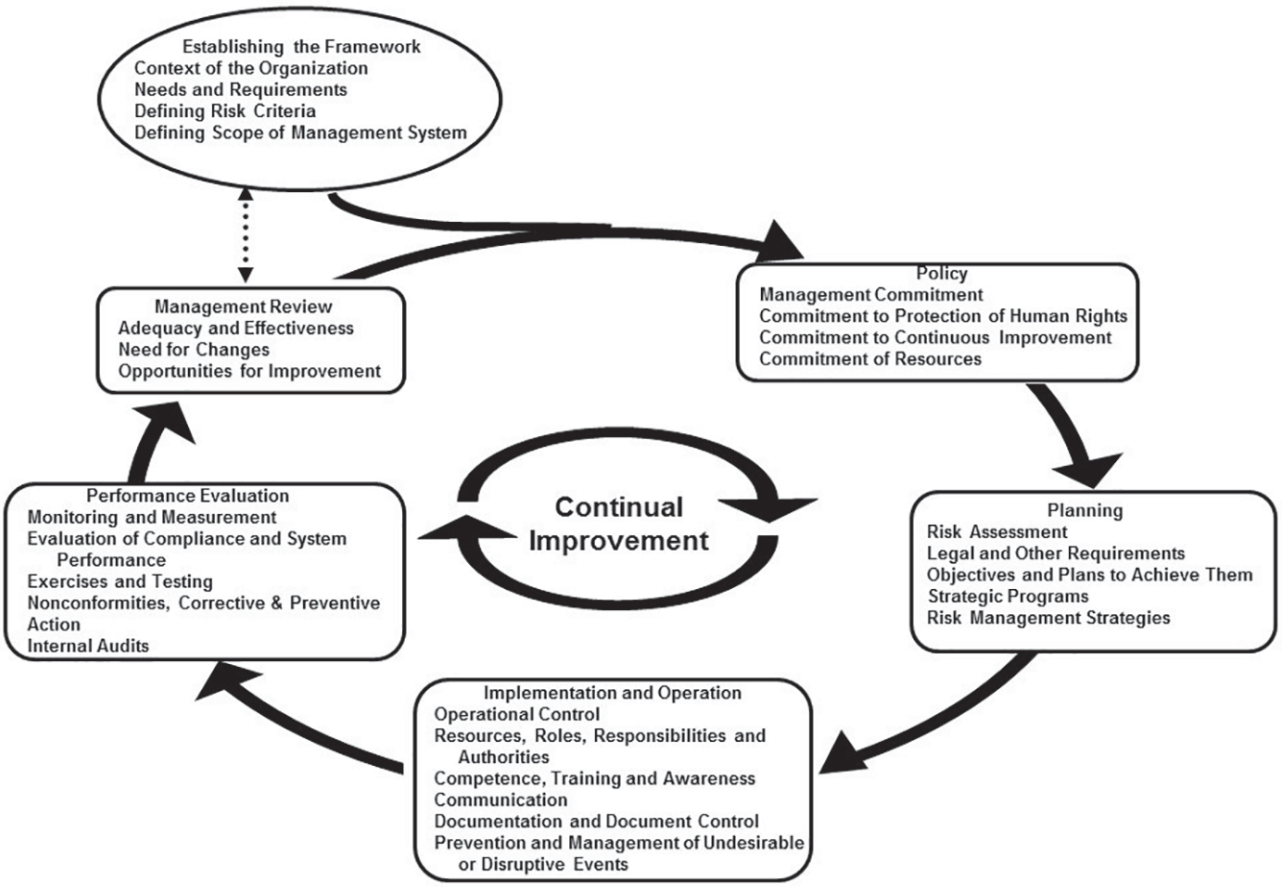


Figure 1 — Security operations management system (SOMS) flow diagram

INTERNATIONAL STANDARD **ISO 18788:2015(E)**

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

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

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]

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.

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 atrisk.

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]

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;

— 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).

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

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.

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).

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]

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]

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.

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.

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;

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.

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.

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.

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;

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.

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);

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.

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;

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.

7.1.2 Structural requirements

7.1.2.1 General

The organization shall be a legal entity or a defined part of a legal entity. It shall have a clearly defined management structure showing control and accountability at each level of the organization (including its subsidiaries within the scope).

7.1.2.2 Organizational structure

A clearly defined management structure shall identify roles, responsibilities, authorities and accountabilities for its operations and services. The organization shall:

a) document its organizational structure, showing duties, responsibilities and authorities of management;

b) define and document if the organization is a defined part of a legal entity and the relationship to other parts of the same legal entity;

c) define any joint venture or partnering arrangements within the SOMS scope.

7.1.2.3 Insurance

The organization shall demonstrate that it has insurance to cover risks and associated liabilities arising from its operations and activities consistent with its risk assessment. When outsourcing or subcontracting services, operations or functions, the organization shall ensure insurance coverage for the subcontracted activities, as appropriate.

7.1.2.4 Outsourcing and subcontracting

The organization shall have a clearly defined process for subcontracting or outsourcing activities, functions and operations. The organization shall establish, document, communicate and monitor compliance with specific terms of reference and codes of conduct to its subcontractors and outsource partners with regards to security operations and respect for human rights.

The organization shall have a documented agreement covering subcontracted or outsourced arrangements including:

a) commitment by subcontractors to abide by the same legal, ethical and human rights commitments and obligations as held by the organization and as described in this International Standard;

b) process for reporting of risks, as well as the occurrence and response to undesirable and disruptive events;

c) confidentiality and conflict of interest agreements;

d) clear definition and documentation of the services to be provided;

e) command and control scope and limitations;

f) definition of the support relationship between the contractor and the subcontractor;

g) conformance to the applicable provisions of this International Standard.

7.1.2.5 Financial and administrative procedures

The organization shall develop financial and administrative procedures and controls to support the provision of effective security and risk management in all planning and operations, in anticipation and in response to a disruptive or undesirable event. Procedures shall be:

a) established to ensure that fiscal decisions can be expedited;

b) in accordance with established authority levels and accounting principles;

c) established in consultation and coordination with the client.

7.2 Competence

7.2.1 General

The organization shall:

— determine the necessary competence of person(s) doing work under its control that affects its security operations performance;

— ensure that these persons are competent on the basis of appropriate education, training, or experience;

— where applicable, take actions to acquire the necessary competence and evaluate the effectiveness of the actions taken;

— retain appropriate documented information as evidence of competence.

NOTE Applicable actions can include, for example, the provision of training to, the mentoring of, or the reassignment of currently employed persons, or the hiring or contracting of competent persons.

7.2.2 Competency identification

The organization shall identify competencies, level of competency and training needs associated with its security operations, particularly the performance of each individual's functions, consistent with legal and contractual obligations and respect for human rights.

The organization shall establish, implement and maintain procedures to ensure persons performing tasks on its behalf demonstrate an appropriate level of competency in each of the following areas:

a) performance of their security functions;

b) assessing risks;

c) managing risks identified in the risk assessment and potential human rights impacts associated with their work;

d) applicable local and international laws, including criminal, human rights and international humanitarian laws including but not limited to:

   1) prohibition of torture or other cruel, inhuman, or degrading treatment;

   2) prohibition and awareness of sexual exploitation and abuse or gender based violence;

   3) recognition and prevention of human trafficking and slavery;

   4) measures against bribery, corruption and similar crimes;

e) culture, such as customs and religion, of the environment in which they are operating;

f) procedures to reduce the likelihood and/or consequences of a disruptive or undesirable event, including response and mitigation procedures to respond to and report events;

g) incident reporting and documentation procedures;

h) first-aid, health and safety procedures;

i) use of weapons including mechanical operations and live fire qualification with the specific weapon(s) authorized and as specified by the organization appropriate to specific security-related tasks;

j) limitations on the use of force related to its security operations;

k) communications protocols, means and procedures;

l) complaint procedures for internal and external stakeholders.

7.2.3 Training and competence evaluation

The organization shall provide competence-based training and establish a means to measure degrees of proficiency or levels of competency. Persons working on behalf of the organization shall be trained to demonstrate the level of competence and proficiency required.

The organization shall:

a) establish competence-based metrics for its training programmes;

b) provide training to instil an understanding that respect for human rights is part of the organization's core values and governance;

c) provide initial and regular classroom, physical, mechanical and live-fire training and evaluation for all personnel authorized to carry lethal, less lethal, or non-lethal weapons in the performance of their duties;

d) provide recurrence training for weapons and the use of force as required by law, or contractual requirements or more frequently to retain the level of competency identified by the organization;

e) identify other competencies that require periodic refresher training to maintain the required level of performance or to incorporate new requirements;

f) provide training on the importance of conformity with the SOMS policy and procedures and with the requirements of the SOMS, as well as potential consequences of departure from specified procedures of the SOMS and security operations.

7.2.4 Documentation

The organization shall retain records of:

a) identified competencies and measurement metrics;

b) training programmes;

c) associated records of training and evaluation for person working on its behalf.

7.3 Awareness

Persons doing work under the organization's control shall be aware of:

— the security operations policy;

— their contribution to the effectiveness of the SOMS, including the benefits of improved security operations performance;

— the implications of not conforming with the SOMS requirements.

7.4 Communication

7.4.1 General

The organization shall determine the need for internal and external communications relevant to the SOMS, including:

— on what it will communicate;

— when to communicate;

— with whom to communicate;

— how to communicate.

The organization shall establish, implement and maintain procedures for:

a) communicating with internal and external stakeholders;

b) receiving, documenting and responding to communications from internal and external stakeholders;

c) defining and assuring availability of the means of communication during atypical situations and disruptions;

d) regular testing of communications system for normal and abnormal conditions.

Communication procedures shall consider the sensitive nature of operational information and legal restrictions on information sharing.

7.4.2 Operational communications

The organization shall develop communication procedures to share information about the security team activity, location, operational and logistic status, relevant threat information and incident reporting to company management, clients, other private security teams and relevant civil or military authorities. This shall include procedures for requesting immediate assistance from military or civil authorities, other security teams and emergency medical support.

The organization shall ensure that spoken and written communications can be received and understood by all levels and operators and that all levels can respond in a language or means that can be understood by appropriate, internal and external stakeholders.

Security teams shall be able to communicate security-related information to the party they are protecting in a form the protected party understands.

7.4.3 Risk communications

The organization shall decide, based on safeguarding life as the first priority and in consultation with stakeholders, whether to communicate externally about significant risks, their impacts and treatments to stakeholders and document its decision. If the decision is to communicate, the organization shall establish and implement (a) method(s) for this external communication, alerts and warnings (including with the media).

7.4.4 Communicating complaint and grievance procedures

Complaint and grievance procedures shall be communicated to internal and external stakeholders. Procedures shall be publicly available on a website and minimize obstacles to access caused by language, educational level, or fear of reprisal, as well as consider needs for confidentiality and privacy.

7.4.5 Communicating whistle-blower policy

The organization shall communicate to people working on its behalf, who have reasonable belief that a non-conformance of this International Standard has occurred, their right to anonymously report the non-conformance internally, as well as externally to appropriate authorities.

7.5 Documented information

7.5.1 General

The organization's SOMS shall include:

— documented information, including records, required by this International Standard;

— documentation of the security operations policy, Statement of Conformance, objectives and targets;

— a description of the scope of the SOMS;

— the Statement of Applicability;

— a description of the main elements of the SOMS and their interaction, and reference to related documents;

— documented information required for the effective implementation and operation of the SOMS;

— documented information determined by the organization as being necessary for the effectiveness of the SOMS.

NOTE The extent of documented information for an SOMS can differ from one organization to another due to:

— the size of organization and its type of activities, processes, products and services;

— the complexity of processes and their interactions;

— the competence of persons.

7.5.2 Creating and updating

7.5.2.1 General

When creating and updating documented information the organization shall ensure appropriate:

— identification and description (e.g. a title, date, author, or reference number);

— format (e.g. language, software version, graphics) and media (e.g. paper, electronic);

— review and approval for suitability and adequacy.

7.5.2.2 Records

The organization shall establish and maintain records to demonstrate conformity to the requirements of its SOMS.

Records include, among others:

a) records required by this International Standard;

b) licenses and operation permits;

c) personnel screening;

d) training records;

e) process monitoring records;

f) inspection, maintenance and calibration records;

g) pertinent subcontractor and supplier records;

h) incident reports;

i) records of incident investigations and their disposition;

j) audit results;

k) management review results;

l) external communications decision;

m) records of applicable legal requirements;

n) records of significant risk and impacts;

o) weapons inventory and receipts for weapons issuance;

p) records of management systems meetings;

q) security, security operations and human rights performance information;

r) communications with stakeholders.

7.5.3 Control of documented information

Documented information required by the SOMS and by this International Standard shall be controlled to ensure:

a) it is available and suitable for use, where and when it is needed;

b) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).

For the control of documented information, the organization shall address the following activities, as applicable:

— distribution, access, retrieval and use;

— storage and preservation, including preservation of legibility;

— control of changes (e.g. version control);

— retention and disposition.

The organization shall establish, implement and maintain procedures to:

a) approve documents for adequacy prior to issue;

b) protect sensitivity and confidentiality of information;

c) review, update as necessary, and re-approve documents;

d) record amendments to documents;

e) make updated and approved documents readily available;

f) ensure that documents remain legible and readily identifiable;

g) ensure that documents of external origin are identified and their distribution controlled;

h) prevent the unintended use of obsolete documents;

i) ensure the appropriate, lawful and transparent destruction of obsolete documents.

Documented information of external origin determined by the organization to be necessary for the planning and operation of the SOMS shall be identified, as appropriate, and controlled.

NOTE Access can imply a decision regarding the permission to view the documented information only, or the permission and authority to view and change the documented information.

The organization shall establish, implement and maintain procedures to protect the sensitivity, confidentiality and integrity of records including access to, identification, storage, protection, retrieval, retention and disposal of records. Records shall be retained as required by the contract and applicable law. Employment and service records shall be retained for a minimum of seven years or as required by applicable law. Organizations shall ensure the integrity of documents by rendering them securely backed-up, accessible only to authorized personnel, and protected from unauthorized disclosure, modification, deletion, damage, deterioration, or loss.

8 Operation

8.1 Operational planning and control

8.1.1 General

The organization shall plan, implement and control the processes needed to meet requirements, and to implement the actions determined in 6.1, by:

— establishing criteria for the processes;

— implementing control of the processes in accordance with the criteria;

— keeping documented information to the extent necessary to have confidence that the processes have been carried out as planned.

The organization shall identify the activities that are associated with the identified significant risks and consistent with its security operations management policy, risk assessment, objectives and targets, in order to ensure that they are carried out under specified conditions, which will enable it to:

a) comply with legal and other regulatory requirements, including permits and licensing of its operations;

b) accomplish the mission while protecting the client's reputation;

c) abide by local and applicable international laws, including international humanitarian, human rights and customary laws, as well as other obligations as described in this International Standard;

d) ensure the security, well-being and rights of persons working on behalf of the organization;

e) respect the rights of local communities;

f) implement risk management controls to minimize the likelihood and consequences of a disruptive or undesirable event;

g) achieve its security operations objectives and targets.

The organization shall establish, implement and maintain documented procedures to control situations where their absence could lead to deviation from the SOMS policy, objectives and targets.

The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.

The organization shall ensure that outsourced processes are controlled.

8.1.2 Performance of security-related functions

The organization shall establish, implement and maintain procedures to support the protection of people, tangible and intangible assets, and other security-related functions, including but not limited to:

a) managing risks identified in the risk assessment;

b) specific functions required by the client or competent authority;

c) other tasks and context specific functions.

8.1.3 Respect for human rights

The organization shall establish, implement and maintain procedures to treat all persons with dignity and with respect for their human rights and to report any non-conformance. The organization shall develop and communicate to all persons working on its behalf procedures for conduct consistent with the principles of respect for human rights; as well as any contractual, legal and regulatory requirement applicable to the organization's security operations.

8.1.4 Prevention and management of undesirable or disruptive events

The organization shall establish, implement and maintain procedures documenting how the organization will prevent, mitigate and respond to undesirable and disruptive events considering the following:

a) performance of security functions;

b) safeguarding of life and promoting safety of personnel and of internal and external stakeholders;

c) respect for life and human dignity;

d) anticipation and prevention of undesirable events as a first priority;

e) response and mitigation to prevent escalation of a disruptive event;

f) minimizing disruption to operations and services;

g) minimizing the potential for any adverse impact on a local community;

h) notification to appropriate authorities;

i) lessons learned and corrective and preventive actions to avoid a recurrence.

8.2 Establishing norms of behaviour and codes of ethical conduct

The organization shall establish, implement and maintain a Code of Ethics for norms of behaviour for all persons working on its behalf, including employees, subcontractors and outsource partners. The Code of Ethics shall be documented and establish the importance of professional conduct in security operations and clearly communicate respect for the human rights and dignity of human beings. The Code of Ethics shall ensure that all persons working on its behalf understand their responsibilities to prevent and report any abuses of human rights.

The organization shall communicate and document its Code of Ethics to all persons working on its behalf, as well as clients.

8.3 Use of force

8.3.1 General

The organization shall establish and document use of force procedures for persons working on its behalf. Where available, such procedures shall be governed by the rules for the use of force (RUF) published by

a competent legal authority for use in its security operations consistent with the requirements of this International Standard.

NOTE Competent legal authority includes, but is not limited to, the government of the state(s) where the organization is registered or has its principal place of management, governments exercising control over the area the organization is operating in, governments contracting with the organization for security, or a military commander exercising authority equivalent to military occupation of an area.

In the absence of authorized RUF, organizations shall base their procedures on published international guidance for use of force (e.g. United Nations Basic Principles on the Use of Force and Firearms by Law Enforcement Officials 1990 and the *Montreux Document*). The use of force procedures shall be consistent with the appropriate and relevant laws and undergo appropriate legal review before adoption.

The organization shall establish use of force procedures to be employed by security operations personnel in self-defence, including the defence of persons under the protection of the organization. The procedures shall include:

a) authorization for the use and carriage of weapons by its personnel;

b) the use of force continuum;

c) the use of less-lethal force;

d) the use of lethal force;

e) the use of force in support of law enforcement (if applicable);

f) training.

The organization shall establish and document procedures specific to its scope of operations and the conditions of the work performed at each location. The organization's use of force procedures shall be consistent with applicable law and contractual requirements, and shall be agreed with any other entity for which private security operations are being provided.

8.3.2 Weapons authorization

The organization shall establish and document procedures for authorizing its personnel to be armed in the performance of security operations. Authorizations shall:

a) only be granted to those personnel who the organization has determined to be suitable for the tasks to be performed and who have undergone background investigations appropriate for the duties performed;

b) be specific to a type and model of weapon(s) and shall only be issued after the individual has qualified on that type and model to a published standard identified in the use of force procedures which is appropriate to the weapon and expected duties.

All arming authorizations shall be in writing and signed (e.g. ink or digitally) by the appropriate authorizing official(s) before a weapon is issued to an individual. The organization shall retain documentation of individual qualification results for as long as the individual has authorization to be armed.

8.3.3 Use of force continuum

The organization shall establish and document procedures describing a use of force continuum, applying an appropriate amount of force reasonably necessary for the security operations. Elements of the continuum shall include:

a) use of force shall be reasonable in intensity, duration and magnitude based on the circumstances applicable at the time;

b) warning persons and providing the opportunity to withdraw or cease threatening actions when the situation or circumstances permit;

c) de-escalation of applied force if the situation and circumstances permit;

d) supervisory controls over initiating, escalating and de-escalating the use of force and the limitation of that authority.

Use of force continuum procedures shall be consistent with the inherent right of self-defence.

8.3.4 Less-lethal force

The organization's use of force procedures shall address the use of less-lethal force, namely that degree of force that is less likely to cause death or serious physical injury as well as the types of less-lethal force authorized and available to its personnel in the conduct of its security operations. The organization shall document procedures for the use of less-lethal force in accordance with applicable and relevant laws of self-defence including, but not limited to, the following circumstances:

a) against persons assaulting other persons or own self to prevent injury or continuation of the assault when alternatives to the use of force have failed or are not available;

b) against persons resisting a lawful apprehension when alternatives to the use of force have failed or are not available;

c) to prevent the loss or destruction of property under the protection of the organization.

8.3.5 Lethal force

Lethal force is justified only under conditions of necessity and may be used only when lesser means cannot be reasonably employed or have failed. The organization's use of force procedures shall identify applicable laws of self-defence for each of its security operations and address the use of lethal force in relation to the following:

a) inherent right of self-defence;

b) defence of others;

c) defence of property including inherently dangerous property or critical infrastructure that, if lost or destroyed, would create an imminent threat of death or serious bodily harm.

Lethal force is justified only under conditions of necessity when there is a reasonable belief that:

a) a person or persons present an imminent threat of death or serious bodily harm to the individual or others in the vicinity;

b) when necessary to prevent the actual theft or sabotage of inherently dangerous property;

c) to prevent the sabotage or destruction of critical infrastructure, the damage to which competent legal authority determines would create an imminent threat of death or serious bodily harm or injury.

8.3.6 Use of force in support of law enforcement

When authorized by a state to support law enforcement operations, the organization shall request RUF from the law enforcement authority or controlling military authority of the relevant state for this function. Where RUF is unavailable, the organization's use of force procedures shall additionally address the following elements derived from the United Nations, *Basic Principles on the Use of Force and Firearms by Law Enforcement Officials*:

— intentional lethal use of firearms shall only be made when strictly unavoidable in order to protect life;

NOTE This does not change the inherent right to use reasonable and necessary force in self-defence.

— the use of force continuum shall include visual or aural identification of the organization's personnel as law enforcement with clear warning of the intent to use firearms

a)

The organization shall develop training aids to be carried by its personnel to assist them in understanding, remembering and applying specific use of force procedures or applicable RUF.

8.4 Apprehension and search

8.4.1 Apprehension of persons

The organization's operational procedures shall address apprehending persons alleged to have committed an attack against persons or property protected by the security operations. The procedures shall describe the legal context under which persons may be held against their will, the limitations on the use of force in such apprehension, and procedures for when and to whom the organization will transfer custody of the person or persons being held.

8.4.2 Search

The organization's operational procedures will describe the circumstances under which third parties may be searched for weapons or other contraband. Search of persons at access control points shall describe the requirement to treat such persons in accordance with fundamental human rights, cultural considerations and personal dignity.

8.5 Operations in support of law enforcement

8.5.1 Law enforcement support

The organization shall only perform such law enforcement operations as specifically authorized to do so by the law enforcement or controlling military authority of the relevant state in accordance with applicable and relevant law. The organization shall develop additional procedures to support security operations in support of law enforcement to include:

a) uniforms and vehicle markings as directed by the relevant law enforcement or controlling military authority;

b) documenting procedures for rendering or assurance of assistance and medical aid to any injured or affected persons;

c) prompt reporting of incidents of injury or death caused by the use of force and firearms in law enforcement activities to law enforcement authorities, as well as to the organization's supervisory personnel;

d) if known, notification to supported law enforcement authorities of the names of persons injured or otherwise affected by law enforcement activities of the organization.

8.5.2 Detention operations

Guarding, transporting, or questioning persons under arrest, detained, or imprisoned by law enforcement authorities is outside the scope of this International Standard.

8.6 Resources, roles, responsibility and authority

8.6.1 General

Top management shall make available resources essential to establish, implement, maintain and improve the SOMS. Resources shall include information, management tools and human resources (including people with specialist skills and knowledge), and financial support.

Roles, responsibilities and authorities shall be defined, documented and communicated in order to facilitate effective security operations management, including control, coordination and supervisory responsibility with a defined line of succession.

To effectively deal with disruptive and undesirable events, the organization shall establish planning, security, incident management, response and/or recovery team(s) with defined roles, appropriate authority, adequate resources, including effective and safe equipment, and rehearsed operational plans and procedures.

Where an organization chooses to subcontract or outsource any process that affects conformity with the requirements of this International Standard, the organization shall ensure that such processes are controlled.

8.6.2 Personnel

8.6.2.1 General

The organization shall retain sufficient personnel (employees, contractors, or subcontractors) with the appropriate competence to fulfil its contractual obligations. Personnel shall be provided with adequate pay and remuneration arrangements, including insurance, commensurate to their responsibilities and context. The organization shall protect the confidentiality of this information as appropriate and provide personnel with relevant documents in language that is readily comprehensible for all parties.

The organization shall maintain documented information on all personnel:

a) as required by legal and contractual obligations;

b) to maintain contact with individuals and their immediate families;

c) to assist in personnel recovery in event of an incident;

d) needed for family notification of injury or death.

8.6.2.2 Selection, background screening and vetting ofpersonnel

The organization shall establish, document, implement and maintain procedures for background screening and vetting of all persons working on its behalf at all tiers to ensure they are fit and proper

for the tasks they will conduct (i.e. subcontractors, outsourced partners and subsidiaries). Wherever possible and consistent with data protection laws, the screening shall include:

a) consistency with legal and contractual requirements;

b) identity, minimum age and personal history verification;

c) education and employment history review;

d) military, police and security service records check;

e) review of possible criminal records;

f) review reports of human rights violations;

g) evaluation for substance abuse;

h) physical and mental evaluation for fitness with assigned activities;

i) evaluation for suitability to carry weapons as part of their duties.

Minimum age requirements may be set by local law, laws applicable in the organization's legal domicile, or may be required of or by the client. In no case, however, shall any person younger than eighteen years of age be employed in duties that require them to use a firearm or other weapon.

Screening shall include an attestation by personnel that nothing in their present or past conduct would contradict the organization's Code of Ethics, Statement of Conformance, or adherence to the clauses of this International Standard. Personnel shall be required to notify the organization of any change of circumstances that might lead to a review of their screening status.

Background screening involves the disclosure of highly sensitive information; therefore, the organization shall develop procedures to appropriately and strictly secure the confidentiality of information both internally and externally. Records shall be maintained consistent with relevant statutes of limitations.

Selection of qualified personnel shall be based on defined competencies, including knowledge, skills, abilities and attributes. Screening and selection measures shall be consistent with legal and contractual requirements, as well as consistent with the normative references of this International Standard.

8.6.2.3 Selection, background screening and vetting of subcontractors

The organization shall establish defined procedures for the selection, background screening and vetting of subcontractors. The organization is responsible for the subcontractor's work and is liable, as appropriate and within applicable law, for the conduct of the subcontractors. The organization shall:

a) ensure appropriate written contractual agreements with the subcontractor;

b) advise the client of the arrangement in writing and, when appropriate, obtain approval of the client;

c) maintain a register of all subcontractors it uses;

d) communicate the responsibilities of this International Standard to the subcontractor;

e) maintain a record of evidence of conformance or deviations with this International Standard for work subcontracted.

8.6.3 Procurement and management of weapons, hazardous materials and munitions

The organization that use weapons, hazardous materials, explosives and munitions shall establish documented procedures and records for the procurement, managements, accountability and traceability of weapons, including:

a) compliance with applicable and relevant national and international law (e.g. UN sanctions);

b) compliance with import and export controls, registrations, certifications, permits and transport requirements;

c) acquisition;

d) secure storage;

e) controls over their identification, issue, use, maintenance, return and loss;

f) records regarding to whom and when weapons are issued;

g) identification and accounting of all ammunition and weapons;

h) proper disposal with verification.

8.6.4 Uniforms and markings

Consistent with the security of their clients, other civilians and the requirements of law, the organization shall use uniforms and markings to identify its personnel and means of transport as belonging to the organization whenever they are carrying out activities in discharge of their contract. This identification should be visible at a distance and distinguishable from those used by military and police forces. The organization shall establish and document procedures for use of uniforms and markings, as well as procedures for determining and documenting when such identification would be inconsistent with the requirements of this clause.

8.7 Occupational health and safety

The organization shall establish, implement and maintain procedures to promote a safe and healthy working environment, including reasonable precautions to protect people working on its behalf in high-risk or life threatening operations, consistent with legal, regulatory and contractual obligations. Procedures shall include:

a) assessing occupational health and safety risks to people working on its behalf as well as the risks to external parties;

b) hostile environment training;

c) provision of personal protective equipment, appropriate weapons and ammunition;

d) medical and psychological health awareness training, care and support;

e) guidelines to identify and address workplace violence, misconduct, alcohol and drug abuse, sexual harassment and other improper behaviour.

8.8 Incident management

8.8.1 General

The organization shall establish, implement and maintain procedures to identify undesirable and disruptive events that can impact the organization, its activities, services, stakeholders, human rights and the environment. The procedures shall document how the organization will proactively prevent, mitigate and respond to events.

When establishing, implementing and maintaining procedures to expeditiously prepare for, mitigate and respond to a disruptive event, the organization shall consider each of the following actions:

a) safeguard life and assure the safety of internal and external stakeholders;

b) respect human rights and human dignity;

c) prevent further escalation of the disruptive event;

d) minimize disruption to operations;

e) notification of appropriate authorities;

f) protect image and reputation (of the organization and its client);

g) corrective and preventive actions.

8.8.2 Incident monitoring, reporting and investigations

The organization shall establish, implement and maintain procedures for incident monitoring reporting, investigations, disciplinary arrangements and remediation. Incidents involving use of force or weapons, any casualties, physical injuries, allegations of abuse, loss of sensitive information or equipment, substance abuse, or non-conformance with the principles of the *Montreux Document* and the *ICoC*, as well as applicable laws and regulations, shall be reported and investigated with the following steps taken, including:

a) documentation of the incident;

b) notification of appropriate authorities;

c) steps taken to investigate the incident;

d) identification of the root causes;

e) corrective and preventive actions taken;

f) any compensation and redress given to the affected parties.

The organization shall assure all persons working on its behalf are aware of their responsibilities and the mechanisms to monitor and report non-conformances and incidents.

Records of non-conformances and incidents shall be maintained and retained for a minimum of seven years or as specified by legal or regulation requirements.

8.8.3 Internal and external complaint and grievance procedures

The organization shall establish procedures to document and address grievances received from internal and external stakeholders (including clients and other affected parties). Effectiveness criteria for the grievance procedures shall be established and documented. The procedures shall be communicated to internal and external stakeholders to facilitate reporting by individuals of potential and actual non-conformances with this International Standard, or violations of international, national and local laws or human rights. The organization shall investigate allegations expeditiously and impartially, with due consideration to confidentiality and restrictions imposed by local law. The organization shall establish and document procedures for:

a) receiving and addressing complaints and grievances;

b) establishing hierarchical steps for the resolution process;

c) the investigation of the grievances, including procedures to;

   1) cooperate with official external investigation mechanisms;

2) prevent the intimidation of witnesses or inhibiting the gathering of evidence;

3) protect individuals submitting a complaint or grievance in good faith from retaliation;

d) identification of the root causes;

e) corrective and preventive actions taken, including disciplinary action commensurate with any infractions;

f) communications with appropriate authorities.

Grievances alleging criminal acts, violations of human rights, or imminent danger to individuals shall be dealt with immediately by the organization and other authorities, as appropriate.

8.8.4 Whistle-blower policy

The organization shall establish a whistle-blower policy for people working on its behalf, who have a reasonable belief that a non-conformance of this International Standard has occurred, and respect their right to anonymously report the non-conformance internally, as well as externally to appropriate authorities. The organization shall not take any adverse action against any individual for the act of making a report in good faith. The organization shall inform the client of reported violations of law or respect for human rights.

9 Performance evaluation

9.1 Monitoring, measurement, analysis and evaluation

9.1.1 General

The organization shall evaluate security operations management plans, procedures and capabilities through periodic assessments, testing, post-incident reports, lessons learned, performance evaluations and exercises. Significant changes in these factors should be reflected immediately in the procedures.

The organization shall keep records of the results of the periodic evaluations.

The organization shall determine:

— what needs to be monitored and measured;

— the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results;

— when the monitoring and measuring shall be performed;

— when the results from monitoring and measurement shall be analysed and evaluated.

The organization shall retain appropriate documented information as evidence of the results.

The organization shall evaluate the security operations performance and the effectiveness of the SOMS.

The organization shall establish, implement and maintain performance metrics and procedures to monitor and measure, on a regular basis, those characteristics of its operations that have material impact on its performance (including partnerships, subcontracts and supply chain relationships). The procedures shall include the documenting of information to monitor performance, applicable operational controls and conformity with the organization's security operations management objectives and targets.

The organization shall evaluate and document the performance of the systems which protect its assets (human and physical), as well as its communications and information systems.

9.1.2 Evaluation of compliance

Consistent with its commitment to compliance, the organization shall establish, implement and maintain procedures for periodically evaluating compliance with applicable legal, regulatory and human rights requirements.

The organization shall keep records of the results of the periodic evaluations.

9.1.3 Exercises and testing

The organization shall use exercises and other means to test the appropriateness and efficacy of its SOMS plans, processes and procedures, including stakeholder relationships and subcontractor interdependencies. Exercises of operational and incident management scenarios shall address issues identified in the risk assessment as well as stress test the risk management procedures to identify potential problems or weaknesses. Exercises shall be designed and conducted in a manner that limits disruption to operations and exposes people, assets and information to minimum risk.

Exercises shall be conducted regularly (at least annually), or following significant changes to the organization's mission and/or structure, or following significant changes to the external environment. A formal report shall be written after each exercise. The report shall assess the appropriateness and efficacy of the organization's SOMS plans, processes and procedures, including nonconformities, and shall propose corrective and preventive action.

Post-exercise reports shall form part of top management reviews.

9.2 Internal audit

9.2.1 The organization shall establish, implement and maintain a security operations management audit programme and conduct internal audits at planned intervals to provide information on whether the SOMS:

a) conforms to:

   — the organization's own requirements for its SOMS;

   — relevant legal, regulatory, human rights and contractual obligations;

   — the requirements of this International Standard;

b) is effectively and properly implemented and maintained;

c) performs as expected;

d) has been effective in achieving the organization's SOMS policy, objectives and targets.

9.2.2 The organization shall:

a) plan, establish, implement and maintain an audit programme(s) including the frequency, methods, responsibilities, planning requirements and reporting, which shall take into consideration the status and importance of the processes and areas concerned and the results of previous audits;

b) define the audit criteria, scope frequency, methods, responsibilities, planning requirements and reporting for each audit;

c) select auditors and conduct audits to ensure objectivity and the impartiality of the audit process (e.g. auditors should not audit their own work);

d) ensure that the results of the audits are reported to relevant management for the area being audited;

e) retain documented information as evidence of the implementation of the audit programme and the audit results.

The management responsible for the area being audited shall ensure that actions are taken without undue delay to eliminate detected nonconformities and their causes. Follow-up activities shall include the verification of the actions taken and the reporting of verification results.

9.3 Management review

9.3.1 General

Top management shall review the organization's SOMS, at planned intervals, to ensure its continuing suitability, adequacy and effectiveness. This review shall include assessing opportunities for improvement and the need for changes to the SOMS, including the SOMS policy and objectives. The results of the reviews shall be clearly documented and records shall be maintained.

The management review shall include consideration of:

a) the status of actions from previous management reviews;

b) changes in external and internal issues that are relevant to the SOMS;

c) information on the security operations performance, including trends in:

   — nonconformities and corrective actions;

   — monitoring and measurement results;

   — audit results;

d) impacts of security operations;

e) risk management criteria and controls;

f) opportunities for continual improvement.

The outputs of the management review shall include decisions related to continual improvement opportunities and any need for changes to the SOMS. The organization shall retain documented information as evidence of the results of management reviews.

9.3.2 Review input

The input to a management review shall include:

a) results of SOMS audits and reviews;

b) feedback from stakeholders;

c) techniques, products, or procedures that could be used in the organization to improve the SOMS performance and effectiveness;

d) status of preventive and corrective actions;

e) results of exercises and testing;

f) risks not adequately addressed in the previous risk assessment;

g) incident reports;

h) results from effectiveness measurements;

i) follow-up actions from previous management reviews;

j) any changes that could affect the SOMS;

k) adequacy of policy and objectives

l) recommendations for improvement.

9.3.3 Review output

The outputs from top management reviews shall include decisions and actions related to possible changes to policy, objectives, targets and other elements of the SOMS, with the aim of promoting continuous improvement, including:

a) improvement of the effectiveness of the SOMS;

b) update of the risk assessment and risk management plans;

c) modification of procedures and controls that effect risks, as necessary, to respond to internal or external events that may affect the SOMS;

d) resource needs;

e) improvement of how the effectiveness of controls is being measured.

10 Improvement

10.1 Nonconformity and corrective action

The organization shall establish, implement and maintain procedures for dealing with nonconformities and for taking corrective and preventive action.

The procedures shall define requirements for identifying and correcting nonconformities and taking actions to mitigate their consequences.

When a nonconformity occurs, the organization shall:

a) react to the nonconformity and, as applicable:

   — take action to control and correct it;

   — deal with the consequences;

b) evaluate the need for action to prevent nonconformities and eliminate the causes of the nonconformity, in order that it does not recur or occur elsewhere, by:

   — reviewing the nonconformity;

   — determining the root causes of the nonconformity;

   — determining if similar nonconformities exist, or could potentially occur;

c) investigate nonconformities, determining their causes and taking actions in order to avoid their recurrence;

d) implement any appropriate action needed and designed to avoid their occurrence;

e) review the effectiveness of any corrective and preventive action taken;

f) record the results of corrective and preventive actions taken;

g) make changes to the SOMS, if necessary.

Corrective actions shall be appropriate to the effects of the nonconformities encountered.

The organization shall ensure that proposed changes are made to the SOMS documentation and shall retain documented information as evidence of:

— the nature of the nonconformities and any subsequent actions taken;

— the results of any corrective action.

10.2 Continual improvement

10.2.1 General

The organization shall continually improve the suitability, adequacy and effectiveness of the SOMS through the use of the security operations management policy, objectives, audit results, analysis of monitored events, corrective and preventive actions and management review.

10.2.2 Change management

The organization shall establish a defined and documented security operations change management programme to ensure that any internal or external changes that impact the organization are reviewed in relation to the SOMS. It shall identify any new critical activities that need to be included in the SOMS change management programme.

10.2.3 Opportunities for improvement

The organization shall monitor, evaluate and exploit opportunities for improvement in SOMS performance and eliminate the causes of potential problems, including:

a) ongoing monitoring of the operational landscape to identify potential problems and opportunities for improvement;

b) determining and implementing action needed to improve security operations performance;

c) reviewing the effectiveness of the action taken to improve performance.

Actions taken shall be appropriate to the impact of the potential problems and the organization's obligations and resource realities.

Top management shall ensure that actions are taken without undue delay to exploit opportunities for improvement. Where existing arrangements are revised and new arrangements introduced that could impact on the quality management of operations and activities, the organization shall consider the associated risks before their implementation.

The results of the reviews and actions taken shall be clearly documented and records shall be maintained. Follow-up activities shall include the verification of the actions taken and the reporting of verification results.

Annex A
(informative)

Guidance on the use of this International Standard

A.1 General

The additional text given in this annex is provided to assist in understanding the requirements of this International Standard. While this guidance addresses and is consistent with the requirements, when implementing those requirements, the organization also needs to consider and implement the relevant clauses of this guidance that apply to its scope, legal and contractual obligations, and operating environment, based on its risk assessment and human rights risk analysis. Elements of this guidance not considered relevant to the organization's SOMS need to be justified in the Statement of Applicability.

Private security operations play an important role in protecting public, private and not-for-profit sector clients operating in circumstances where governance may be weak or rule of law undermined due to human or naturally caused events. Clients from the public, private and non-governmental organization (NGO) sectors engage a broad-range of services from organizations that conduct or contract security operations in support of commercial, humanitarian, diplomatic, development and military efforts, and to protect other activities, including rebuilding of infrastructure. The scope and scale of the activities of organizations that conduct or contract security operations include guarding and protection of persons and objects, such as convoys, facilities, designated sites, property or other places (whether armed or unarmed), as well as other activities for which the personnel of organizations are required to carry or operate a weapon in the performance of their duties. This International Standard provides auditable criteria for organizations and their clients in order to demonstrate accountability that human rights and fundamental freedoms are adhered to, and that untoward, illegal and excessive acts are prevented.

The primary role of organizations that conduct or contract security operations is to ensure that clients can operate safely and securely, while fully adhering to and supporting the fundamental and universal human right of people to be secure in their persons and property in conditions of weakened governance. In many parts of the world, this basic right is under attack. In many cases, these attacks are directed against people who are working to alleviate the suffering of affected populations, to restore critical infrastructure necessary for the well-being of individuals and society, or are engaged in other activities that will lead to long term stability and development of the population. These attacks may be for the purpose of immediate financial gain, politically motivated, or for reasons of hatred, bigotry and/or revenge. These attacks not only violate the basic rights of the individuals targeted by that violence, but also affect the broader population who are consequently denied food, water, medical treatment, electricity, employment and peace. Frequently, the perpetrators seek cover among the civilian population, using the innocent to shield themselves, often using intimidation and fear. Where the community or effective authority lacks the capacity to broadly defend lives, rights and property of their citizens – or is incapable of providing minimum security or bringing perpetrators of this violence to justice – individuals and organizations may seek recourse to commercial providers of security services to provide the capacity for self-defence to prevent the commission of a serious offenses involving grave threat to life or serious bodily harm.

This International Standard recognizes that organizations that conduct or contract security operations operate in circumstances that are inherently unstable and dangerous. This International Standard provides principles and requirements to manage risk associated with operating in circumstances of weakened governance or where the rule of law has been undermined by human or naturally caused events. The purpose of this International Standard is to improve and demonstrate high level of professionalism by organizations while maintaining the safety and security of their operations and clients within a framework that aims to ensure respect for human rights, laws and fundamental freedoms.

The challenge to organizations that conduct or contract security operations goes beyond response and reporting of incidents. Organizations should engage in a comprehensive and systematic process to pre-emptively manage the risks associated with their operations. This requires the creation of an on-going, dynamic and interactive management process that serves to promote a culture of respect for human rights, laws and fundamental freedoms, while providing clients with a level of service to support their mission.

Respect for life and human dignity is the paramount underlying principle of this International Standard. Organizations that conduct or contract security operations, and their clients, have an obligation to respect the lives and human dignity of both internal and external stakeholders (including the community at large). By using this International Standard, organizations can better understand the risks they face and pre-emptively develop strategies that will:

a) manage risk posed to the lives and property of those whom they are contractually obligated to protect;

b) 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 for Business and Human Rights; Implementing the United Nations "Protect, Respect and Remedy" Framework* 2011;

c) demonstrate commitment, conformance and accountability to respect human rights, laws and fundamental freedoms;

d) reduce risk and support the business and operational mission;

e) successfully manage an undesirable or disruptive event by developing a strategy and action plans to safeguard its interest and those of its clients and other stakeholders.

Adaptive and pre-emptive planning and preparation for potential undesirable and disruptive events will help reduce the likelihood and consequences of an event. The holistic management process can help avoid or minimize the interruption or suspension of mission critical services and operations.

This International Standard provides guidance or recommendations for any organization providing or contracting security operations to identify and develop best practices to assist and foster action in:

a) reducing risks throughout its operations and supply chain (including subcontractors);

b) providing top management driven vision and leadership for strategies to protect tangible and intangible assets while respecting human rights, laws and fundamental freedoms;

c) identifying and evaluating risks critical to its short- and long-term success;

d) minimizing the likelihood and consequences of a wide variety of hazards and threats;

e) understanding, providing and applying training in respect for human rights;

f) understanding the roles and responsibilities needed to protect assets and further the mission;

g) managing incident response measures and resources;

h) developing, testing and maintaining incident prevention and response plans, and associated operational procedures;

i) developing and conducting training and exercises to support and evaluate prevention, protection, preparedness, mitigation, response, recovery and operational procedures;

j) developing and conducting training programmes to support operations requiring the use of force;

k) developing internal and external communications procedures, including response to requests for information from the media or the public;

l) establishing metrics for measuring and demonstrating success;

m) documenting the key resources, infrastructure, tasks and responsibilities required to support critical operational functions;

n) establishing processes that ensure the information remains secure, current and relevant to the changing risk and operational environments.

The success of the management system depends on the commitment of all levels and functions in the organization, especially the organization's top management. Decision makers should be prepared to budget for and secure the necessary resources to make this happen. It is necessary that an appropriate administrative structure be put in place to effectively deal with prevention, mitigation and management. This will ensure that all parties concerned understand who makes decisions, how the decisions are implemented and what the roles and responsibilities of all persons working on behalf of the organization are. This International Standard drives a culture of security operations within the organization where all security activities are inextricably linked to respect for human rights, laws and fundamental freedoms.

Clients of organizations that conduct or contract security operations have an inherent interest to ensure that the organizations abide by the principles of this International Standard, given that the actions of an organization directly reflect on their clients, particularly when the client is a government entity. The consequences of untoward, illegal and excessive acts on the part of an organization conducting or contracting security operations can range from embarrassing the client, reputational risks and legal liabilities, disrupting critical diplomatic, aid and reconstruction efforts, and increasing the threat. Therefore, when contracting the services of organizations, clients also have an interest in making sure that the contracts reflect the transparent implementation of an SOMS.

A.2 Human rights and international law

A.2.1 General

The discussion of human rights and international law in this clause is a broad summary; legal advice should be sought before conducting security operations in any particular environment.

See Bibliography for citations to some of the applicable international instruments.

A.2.2 Human rights

A.2.2.1 General

Building on 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* of 21 March 2011, "human rights" where it appears in this International Standard refers to the rights and freedoms articulated in international human rights law to which all people are entitled to without discrimination. Human rights are universal and are interrelated, interdependent, inalienable and indivisible. They are articulated in both national and international law.

For the purposes of this International Standard, organizations that conduct or contract security operations should respect all human rights, including but not limited to, non-derogable human rights, such as:

— the right to life;

— freedom from genocide and crimes against humanity;

— freedom from torture, cruel, inhuman, or degrading treatment or punishment;

— freedom from slavery, slave trade and servitude;

— the rights to due process, equal treatment before the law and a fair trial;

— the right to be free from retroactive application of penal laws;

— the right to freedom of thought, conscience and religion;

— freedom from discrimination.

A.2.2.2 Self-defence and defence of others

The purpose of an organization conducting or contracting security operations is to enable the right to life in circumstances that are inherently unstable and dangerous, doing so in such a way that does not violate other human rights. This International Standard recognizes the fundamental importance of self-defence to protect the right to life. Self-defence allows an individual to use reasonable force in defence of oneself or others. Lethal force should only be used in self-defence or the defence of others, when it is reasonable and necessary to prevent death or serious bodily harm.

A.2.3 International humanitarian law

International humanitarian law (IHL) or the law of armed conflict (LOAC) refers to international treaty and customary rules that govern war or armed conflict (the laws and customs of war). For the purposes of this guidance, IHL and LOAC can be considered to have the same meaning. IHL defines the conduct and responsibilities of individuals and states during armed conflict. IHL aims to limit the suffering caused by war, by protecting people who are not or are no longer taking part in hostilities and restricting the methods and means of warfare. The essential rules of IHL include obligations to:

a) engage in limited methods and means of warfare;

b) distinguish between those directly participating in hostilities and the civilian population (non-combatants);

c) limit attacks solely to military objectives;

d) avoid unnecessary harm to the civilian population and property;

e) abstain from harming or killing an adversary who surrenders or who can no longer take part in the fighting;

f) treat humanely all persons taking no active part in hostilities (including adversaries who have surrendered, are wounded, or sick);

g) abstain from physical or mental torture or performing cruel punishments.

International legal obligations particularly applicable to PSCs are specified in the *Montreux Document,* Part 1, paragraphs 22-27.

During an armed conflict, security operations personnel are normally considered civilians under IHL. As civilians, security operations personnel may not be the object of a direct attack unless and for such time as they directly participate in hostilities. Under the conditions of this International Standard, organizations conducting or contracting security operations and their personnel are not privileged to either engage in combat or carry out any other act that is likely to directly harm the military operations or capacity of a party to the conflict. This restriction generally means that security operations personnel cannot, for example, attack enemy armed forces or defend a military objective against an attack by enemy armed forces without losing their protection as civilians. Direct participation in hostilities by security operations personnel is not prohibited by IHL. If captured, security operations personnel who are authorized to accompany the armed forces do not lose any existing entitlement to prisoner of war status as a result of their direct participation in hostilities. However, as civilians without combatant privileges, security operations personnel can be held accountable under criminal and tort law for any serious injury or death inflicted on others or destruction of property committed by them. Regardless

of prisoner of war status, captured security operations personnel are entitled to adequate and humane conditions of detention.

Self-defence and the defence of others against unlawful attack is an inherent right and is not direct participation in hostilities. This right to self-defence applies even if the attacker(s) is/are members of the armed forces of a state, if such attack is unlawful under IHL. Use of force by security operations personnel to resist unlawful attacks does not forfeit their protected status as civilians. However, defensive fire against or otherwise resisting a lawful attack (e.g. by a party to the armed conflict against an enemy party's military objective) could be considered direct participation in hostilities, which would result in the loss of protected status during that action.

Security operations personnel can be charged and convicted for serious violations of international law, such as war crimes and crimes against humanity. These crimes have extraterritorial jurisdiction, with varying degrees of application. Some states and international organizations promote a concept of universal jurisdiction for such crimes. Under this concept, it is possible for persons accused of such crimes to be brought to court in any country, before any judge. Directors, managers and supervisors of security operations personnel can also be held liable for such crimes committed by personnel under their effective authority, either because of orders or instructions they issue or the failure of security operations supervisors to exercise proper control over their personnel. Companies may also be found liable under evolving criminal or tort law.

Based on the risk assessment, it is recommended that the organization consult with appropriate legal counsel for interpretations and evolving law. Organizations operating in conditions of armed conflict should include more comprehensive training for persons working on its behalf that includes, but may not be limited to:

a) the difference between self-defence/defence of others and direct participation in hostilities;

b) specific individual crimes, such as torture and other inhumane treatment, that could be charged against them as war crimes or crimes against humanity;

c) specific considerations for the use of force in international and non-international armed conflicts, to include the differences between international armed conflict and armed conflict not of an international character and the status of various belligerents and non-state armed groups;

d) the difference between RU procedures and rules of engagement proper to armed forces;

e) the circumstances in which the organization and persons working on its behalf could be regarded as belligerents or incorporated into armed forces.

A.2.4 Customary international law

Customary international law refers to the rules of law derived from the consistent conduct of states acting out of the belief that the law required them to act that way. Elements of customary international law include widespread repetition by states of similar international acts over time (state practice), the acts occurring out of a sense of obligation, and the acts being accepted by a significant number of states.

Customary international law is binding on all states regardless of whether they are a party to a particular treaty or convention. A number of human rights listed above are today considered customary international law. With regard to IHL, significant elements of the laws covering international armed conflict remain customary, rather than treaty law. The application of much of IHL to non-international armed conflicts is a matter of customary international law. Issues relating to civilian status in armed conflict and direct participation in hostilities are still emerging as matters of customary law and directly affect the activities of the organization.

A.2.5 International human rights law

International human rights law refers to the body of international law that is designed to promote and protect human rights and consists of treaties and agreements between states. International human rights law is binding on states and their agents. International human rights standards are enforceable

through national law and various international and regional courts and tribunals, as well as the UN charter and treaty-based mechanisms. The principles described in the *ICoC* are intended to guide the organization in developing and implementing policies and procedures that are consistent with the objectives of international human rights law.

A.3 Management systems approach

A management system is a dynamic and multifaceted process, with each element interacting as a structured set of functional units. It provides a framework that is based on the premise that the component parts of a system can best be understood when viewed in the context of relationships with each other and with other systems, rather than in isolation. The only way to fully understand and implement the elements of a management system is to understand the parts in relation to the whole. This results in an iterative process where establishing the context and policy, risk assessment, implementation, operation, evaluation and review are not a series of consecutive steps, but rather a network of interacting functions.

The management systems approach is characterized by:

a) understanding the context and environment within which the system operates;

b) identifying the core elements of the system, as well as the system boundary;

c) understanding the role or function of each element in the system;

d) understanding the dynamic interaction between elements of the system.

The systems approach ensures that holistic strategies and policies are developed. It provides a sound analytical basis for developing strategies and policies that are to be implemented in the complex and changing environment in which the organization operates. Establishing a framework for assessing the risks and effectiveness of strategies and policies prior to and during implementation provides a feedback loop for decision-making throughout the process.

A.4 Context of the organization

A.4.1 Understanding the organization and its context

A.4.1.1 General

In order to manage risks and promote a culture of respect for human rights, the organization requires a knowledge and understanding of the internal and external factors that can influence its security operations and impact stakeholders.

The organization establishes the context of its SOMS by identifying and understanding the internal and external influences and environment in which it operates. By establishing the context, an organization can define the scope of its SOMS and design a fit-for-purpose framework for security operations management. This should help assure that the organization meets the objectives, needs and concerns of internal and external stakeholders. The context will determine the criteria for managing the risk to the organization, clients and impacted communities thereby providing a basis for setting risk criteria and parameters for the risk assessment and treatment processes.

During the process of establishing the internal and external context, the organization should identify the significant tangible and intangible assets of the organization. This includes identifying the relative importance of various types of assets to the viability and success of the organization.

A.4.1.2 Internal context

When establishing the internal context of the organization it is important to consider:

a) internal factors affecting the security operations and operating environment of the organization;

b) internal stakeholders who are risk makers and risk takers;

c) internal stakeholders that are impacted by risks;

d) factors that influence the acceptance of risk.

A.4.1.3 External context

When establishing the external context of the organization it is important to consider:

a) risks factors associated with the industry sector and operational environment;

b) external factors affecting the security operations and operating environment of the organization;

c) external stakeholders who are risk makers and risk takers;

d) external stakeholders that are impacted by risks related to security operations;

e) factors that influence the acceptance of risk by external stakeholders.

A.4.1.4 Supply chain and subcontractor mapping and analysis

Managing risks in the supply chain, including subcontractors and local forces under contract, requires an understanding of those entity's culture and environment as well as the end-to-end context of its supply chain. Each node of the organization's supply chain involves a set of risks and management processes that need to be managed.

Supply chains and the use of subcontractors are integral parts of security operations. While there is significant interdependence within a supply chain, each individual node of a supply chain is unique in certain respects; this uniqueness may require tailored approaches to the management of the risks involved. Therefore, to manage the risks within a supply chain, the organization needs to identify:

a) the role of organizations and individuals at each tier or level of its upstream and downstream supply chain or network;

b) understand the interdependencies and supporting infrastructure critical to mission success;

c) how each node plays a role in adding value to the performance of other members of the chain, directly or indirectly;

d) determine how each node has the potential to contribute to the risk profile of the organization, both positively and negatively;

e) evaluate how each node exerts some influence on the success of minimizing risk during implementation of the management system.

When conducting node analysis, the organization should recognize the decisions taken at individual nodes have potential chain-wide implications. Therefore, the risk factors throughout the supply chain need to be understood and controlled for successful implementation of the SOMS.

A.4.1.5 Defining risk criteria

The organization should understand and define its criteria to evaluate the significance of risk. The risk criteria should reflect the organization's values, objectives and resources, as well as the context of its security operations. The risk criteria will establish the benchmarks for measuring risk factors and the needs for risk treatments.

A.4.2 Understanding the needs and expectations of stakeholders

The organization should identify and maintain a register of the stakeholders that are relevant to the operations of the organization and the requirements under this International Standard and document

its engagement with stakeholders. The organization should consider the requirements, perceptions, values, needs, interests and risk tolerance of the relevant stakeholders.

Relevant stakeholders include, but are not limited to:

a) clients and customers;

b) end users;

c) supply chain and outsource partners;

d) competent legal authorities which are responsible for domestic security and the licensing or authorization and regulation of private security operations;

e) local communities within the scope of application of this International Standard (e.g. community where the security operations are being performed);

f) state of expatriate personnel employed by the organization or from which the organization purchases materiel and other assets;

g) non-governmental organizations and international organizations within the operating environment;

h) organization's personnel;

i) the media.

A.4.3 Determining the scope of the security operations managementsystem

The organization defines the boundaries for implementing its SOMS. It may choose to implement the SOMS across the entire organization, specific operating units, discrete geographic locations, or clearly defined supply chain flows. These scoping boundaries reflect top management objectives for the SOMS and the size, nature and complexity of the organization and its activities. Once top management defines the SOMS scope, all assets, activities, products and services within that scope become elements of concern within the SOMS.

The organization should justify any exclusions from the scope of the SOMS using the risk assessment in the justification. Exclusions may include the inability of an organization to control certain services or operations; however, exclusions do not negate the organization's responsibilities and obligations to respect human rights, laws and fundamental freedoms. The scope should ensure the integrity of the organization and its clients operations. The credibility of the SOMS depends on the choice of organizational boundaries defined in the scope.

Organizations conduct security operations in a wide range of environments where risk factors will differ. Based on the context of the security operations and risk assessment, the Statement of Applicability should document the relevant clauses of this annex that apply to the establishment and implementation of the SOMS within the defined scope.

Outsourced and subcontracted activities remain the organization's responsibility and should be within the SOMS. If an outsourced or subcontracted product, service, activity, or part of the organization's supply chain remains under the organization's risk accountability and management control, then top management should place it within the scope of the SOMS. The organization should make appropriate agreements and take appropriate measures to assure effective security operations management agreements are in place with its subcontractors and outsource partners.

The level of detail and complexity of the SOMS, the extent of documentation required and resources committed to the SOMS should guide the SOMS scope statement. When the organization implements this International Standard for a specific operating unit, then the organization may use applicable policies, plans and procedures developed by other parts of the organization to satisfy the requirements of this International Standard.

A.4.4 Security operations management system

The implementation of the SOMS specified by this International Standard is intended to result in:

a) improved security operations and service provision;

b) security and safety of internal and external stakeholders;

c) a culture of respect for human rights, laws and fundamental freedoms;

d) demonstration of implementation of the principles and commitments of the *ICoC*.

This International Standard is based on the premise that the organization will monitor, review and evaluate its SOMS to identify opportunities for continual improvement and the implementation of corrective and preventive measures. The rate, extent and timescale of this continual improvement process are determined by the organization in the light of the changing risk environment, economic and other circumstances. This International Standard requires an organization to:

a) establish an appropriate security operations management policy;

b) assess and manage the risks related to the organization's security operations;

c) identify applicable legal requirements and other requirements to which the organization subscribes;

d) identify priorities and set appropriate security operations management objectives and targets;

e) establish a structure and programmes to implement the policy and achieve objectives and meet targets;

f) facilitate planning, control, monitoring, preventive and corrective action, and auditing and review activities, to ensure both that the policy is complied with and that the SOMS remains appropriate;

g) be capable of adapting to changing circumstances.

A.5 Leadership

A.5.1 Leadership and commitment

A.5.1.1 General

The top management of the organization (such as the managing director or chief executive) should demonstrate commitment and resolve to implement the SOMS in the organization. Without top management commitment, no management system can succeed. Top management should demonstrate to its internal and external stakeholders a visible commitment to respect for human rights, laws and fundamental freedoms in the provision of security operations. To initiate and sustain the SOMS effort, top management should communicate to all persons working on behalf of the organization the importance of:

a) making organizational and individual competence in the conduct of security operations inherent in everything the organization does;

b) respect for human rights, laws and fundamental freedoms is an integral component of all security operations;

c) integrating security operations management throughout the organization;

d) looking at problems as opportunities for improvement.

The top management should provide evidence of its commitment to the development and implementation of the SOMS and continually improve its effectiveness by:

a) communicating throughout the organization the importance of meeting the requirements of this International Standard;

b) setting and communicating the policy and risk criteria;

c) ensuring that security operations objectives are established at all levels and functions;

d) ensuring that the responsibilities and authorities for relevant management system roles are assigned and communicated within the organization;

e) allocating appropriate resources for the management system;

f) ensuring the competence and training of persons working on behalf of the organization;

g) demonstrating commitment to the management system and risk minimization;

h) promoting awareness of risk and SOMS requirements throughout the organization;

i) leading by example;

j) participating in reviews and driving the continual improvement process.

It is essential that top management of the organization sponsors, provides the necessary resources and takes responsibility for creating, maintaining, testing and implementing a comprehensive SOMS. This will insure that management and staff at all levels within the organization understand that the SOMS is a critical top management priority. It is equally essential that top management engage a "top down" approach to the SOMS: so that management at all levels of the organization understand accountability for system maintenance as part of the overall governance priorities.

A.5.1.2 Statement of Conformance

The Statement of Conformance establishes and communicates the top management's commitment to conduct security operations consistent with the organization's responsibility to respect human rights by implementing the requirements of this International Standard 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 standards.

A.5.2 Policy

The security operations policy is the driver for implementing and improving an organization's SOMS. This policy should therefore reflect the commitment of top management to:

a) respect human life and dignity as a first priority;

b) avoid, prevent and reduce the likelihood and consequences of disruptive and undesirable events;

c) comply with applicable legal requirements and other requirements;

d) respect human rights;

e) continual improvement.

The security operations policy is the framework that forms the basis upon which the organization sets its objectives and targets. The security operations policy should be sufficiently clear to be capable of being understood by internal and external stakeholders and should be periodically reviewed and revised to reflect changing conditions and information. Its area of application (i.e. scope) should be clearly identifiable and should reflect the unique nature, scale and impacts of the risks of its activities, functions, products and services.

The security operations policy should be communicated to all persons who work for or on behalf of the organization, including its clients, supply chain partners, subcontractors and relevant members of the local community. Communication to subcontractors and other external parties can be in alternative forms to the policy statement itself, such as rules, directives and procedures. The organization's security operations policy should be defined and documented by its top management within the context of the security operations policy of any broader corporate body of which it is a part and with the endorsement of that body.

A.5.3 Organization roles, responsibilities and authorities

Managing risks is not just the responsibility of top management. For an SOMS to be effective, it needs to be implemented by every person working on behalf of the organization. It is a top-down, bottom-up approach. Protection of human rights and managing risk need to become an integral part of the organization's culture. Therefore, all risk-makers and risk-takers should be the risk-managers. Therefore, the roles, responsibilities, authorities of persons working on behalf of the organization within the scope of the SOMS should be clearly defined and communicated.

The management system is implemented by people within the organization. One or more qualified persons should be appointed and empowered to implement, test or exercise, and maintain the SOMS. Top management should conduct its own periodic reviews and audits of the overall SOMS. A security operations management planning team, including senior leaders from all major organizational functions and support groups may be appointed to ensure wide-spread acceptance of the SOMS.

A.6 Planning

A.6.1 Actions to address risks and opportunities

A.6.1.1 General

Organizations conducting or contracting security operations inherently operate in circumstances of uncertainty and risk. They need to manage risk to the client while also managing risk to the organization and impacted stakeholders and communities. The organization needs to achieve its tactical, operational and business objectives within the context of protecting life and property of its clients, people working on its behalf and local communities, while respecting human rights. Respecting rights creates value for the business and therefore is intrinsically a business objective requiring human rights due diligence to accomplish the operational mission, while respecting human rights and adhering to local, national and international law. The challenge is to assess, evaluate and treat risk in order to cost effectively manage the risk and uncertainty while meeting the organization's and the client's strategic and operational objectives. The risk assessment provides a clear understanding of the risk environment in order for the organization to identify risks and make informed decisions in prioritizing its risks treatment.

The risk assessment process provides an understanding of the risks to internal and external stakeholders that could affect the organization's achievement of its operational and business objectives. It is intended to create a systematic process for an organization to identify, analyse and evaluate risks to determine those that are significant to the organization and its stakeholders. The risk assessment provides a basis for evaluating the adequacy and effectiveness of current controls in place, as well as decisions on the most appropriate approaches to be used in managing and treating risks. It identifies those risks that should be addressed as a priority by the organization's SOMS. The risk assessment provides the foundation for setting objectives, targets and programmes within the management system, as well as measuring the efficacy of the SOMS.

A.6.1.2 Legal and other requirements

A.6.1.2.1 General

The organization should identify and understand legal, regulatory and contractual requirements that affect the achievement of its objectives. These may include local, national and international, and legal and regulatory requirements. Identifying and understanding these requirements help ensure legal compliance, prevent litigation, minimize liability, improve the organization's image and enhance the organization's capability to provide responsible protective services to its client.

The organization should establish, implement and incorporate into its processes, measures to identify, comply with and evaluate applicable legal and voluntary requirements, including (but not limited to):

a) applicable and relevant local, national and international legal, regulatory and other requirements related to its activities and operations and those of any subcontractors or joint ventures within the scope of application of this International Standard;

b) relevant international humanitarian law and human rights law, including but not limited to prohibition of torture or other cruel, inhumane or degrading treatment; awareness and prohibition of sexual exploitation and abuse or gender based violence, recognition and prevention of human trafficking and slavery;

c) applicable international and national employment and environmental laws and codes;

d) international and national measures against bribery, corruption and similar crimes;

e) processes for compliance with local, national and international laws as regards the procurement, licensing and transhipment of firearms (and other controlled goods such as body armour and explosives) for use in its security operations;

f) any voluntary codes or conventions to which the organization subscribes. These may include the *UN Guiding Principles on Business and Human Rights* (UNGPs), the *International Code of Conduct for Private Security Service Providers (ICOC)* and the *Voluntary Principles on Security and Human Rights* (VPs).

Examples of other requirements to which the organization may subscribe include, if applicable:

a) business and other contractual obligations;

b) agreements with public authorities, community groups, or non-governmental organizations;

c) agreements with clients;

d) non-regulatory guidelines;

e) voluntary principles or codes of practice;

f) product or service stewardship commitments (e.g. warranties);

g) requirements of trade associations;

h) public commitments of the organization or its parent organization;

i) non-binding protocols;

j) healthcare requirements;

k) financial obligations;

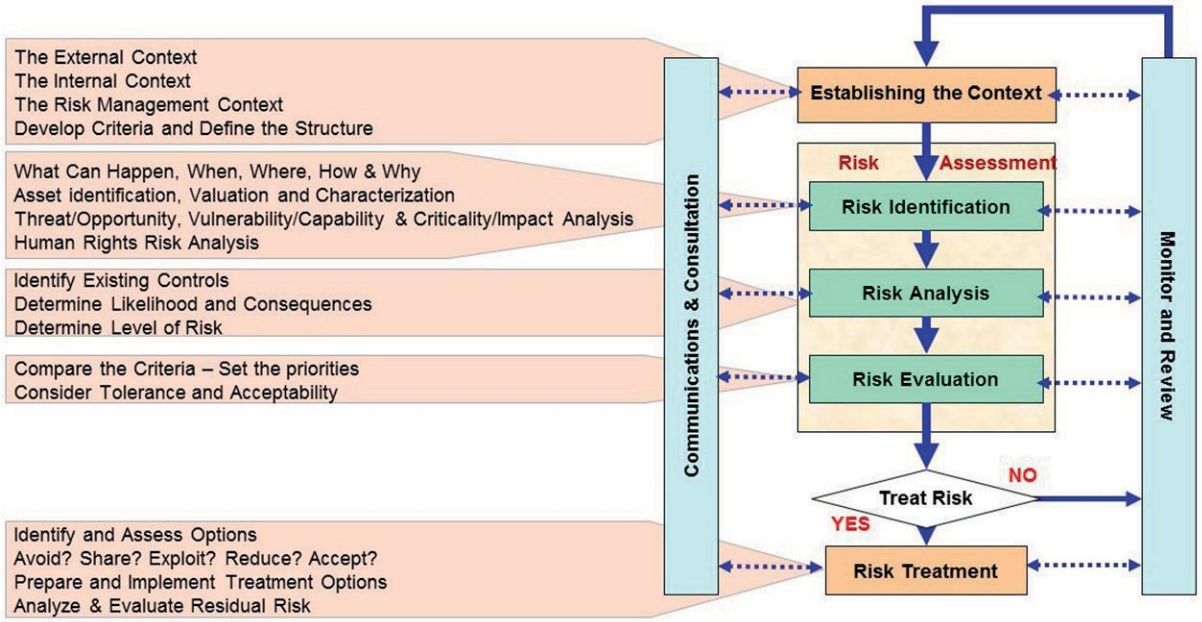
l) social responsibility and environmental commitments;

m) identity information, confidentiality and privacy requirements.

The *Montreux Document*, Section 1, Paragraph E, summarizes the pertinent international legal obligations applicable to organizations and their personnel conducting or contracting security operations. Specific legal obligations vary by jurisdiction, geographic location, the type and nature of operations, and the location, type and nature of the organization's customers. Therefore, it is important that the organization be aware of its obligations within the context of its operating environment. The organization should define and document specific operational controls as well as individual responsibilities to meet these requirements.

A.6.1.2.2 Risk assessment process as described in ISO 31000

An organization should apply the principles and guidelines on implementation in ISO 31000, as illustrated in Figure A.1.



NOTE Source: ASIS International.

Figure A.1 — Process for managing risk including the risk of adverse human rights impact

The risk assessment process is conducted within the internal and external context of the organization.

Risk assessment is the overall process of risk identification, risk analysis and risk evaluation, as described below.

a) Risk identification: The process of identifying, grading and documenting risks by means of threat analysis, criticality analysis, vulnerability analysis and human rights risk analysis. The process considers the causes and sources of risks, as well as events, situations and circumstances that could impact the organization and its stakeholders.

   The identification should include of all sources of risk that may deter the organization from achieving its business, tactical and operational objectives, including the rights, security and safety of clients, persons working on behalf of the organization as well as other internal and external stakeholders.

b) Risk analysis: The process of developing an understanding of risk and the level of risk. It provides the basis for determining which risks should be treated and the most appropriate method for treating them.

   It considers the causes and sources of risk, their consequences (including severity) and the likelihood that the incident and associated consequences can occur. An organization should determine what the consequences of an event upon stakeholders will be if a threat materializes. The level of risk is a function of the likelihood, severity and consequences and provides the basis for prioritizing the risks that need to be treated;

c) Risk evaluation: The process of comparing the estimated levels of risk with the risk criteria defined when the context was established. It determines the significance of the level and type of risk. The risk evaluation uses the understanding of the risk obtained in the risk analysis to make decisions about the strategies required for risk prioritization, control and treatment.

A.6.1.2.3 Human rights risk analysis

The human rights risk analysis is the process to identify, assess and document human rights-related risks and their impacts in order to manage risk and to mitigate or prevent adverse human rights impacts and legal infractions. It is also sometimes referred to as a "human rights risk assessment" or a "human rights impact assessment". The human rights risk analysis should assess both the negative and positive outcomes of risks. Negative impacts are graded and prioritized in terms of the severity of the consequences of a risk event. Assessing the positive outcomes of risk may provide opportunities to improve the risk environment of stakeholders. The human rights risk analysis is an integral part of the overall risk assessment process.

Conducting a thorough human rights risk analysis provides a basis to identify, evaluate, manage and document risk to prevent, mitigate and account for human rights abuses and legal infractions, and forms part of the necessary due diligence to avoid the organization's involvement in human rights abuses and legal infractions. Organizations should identify potential and actual human rights risks related to their activities or directly linked to their business relationships and their potential sources, and should analyse their likelihood, severity and consequences in order to prioritize risks and implement appropriate measures to prevent, mitigate and account for the risks.

Human rights risk analysis processes:

a) assess risks directly related to the organization's security operations activities and linked to their client, subcontractor, outsource partner, supply chain and other business relationships;

b) include communication and meaningful consultation with internal and external stakeholders impacted by the risk and associated activities;

c) identify and obtain the necessary human rights expertise and competences needed to conduct the human rights risk analysis and demonstrate the thoroughness of process to assess the human rights risks;

d) document the risk assessment process for purposes such as review, integrating and acting upon findings, tracking effectiveness of responses, external communications and reporting about how impacts are addressed, and litigation protection.

A.6.1.2.4 Risk assessment process considerations

The risk assessment provides an understanding of risks, their causes, likelihood, severity and consequences. Therefore, an organization should conduct a comprehensive risk assessment within the scope of its SOMS, taking into account the inputs and outputs (both intended and unintended) associated with:

a) its activities, products and services;

b) interactions with the environment and community;

c) relations with internal and external stakeholders;

d) infrastructure and interdependencies.

The risk assessment should include a detailed analysis and evaluation of the uncertainties associated with the successful achievement of the organization's mission and its responsibility to respect the rights of all stakeholders, for example (but not limited to) the following:

a) tactical risks related to the mission and operations;

b) risks related to the reputation of the organization and the client;

c) political, economic and social implications of the organization's activities;

d) threats and consequences to persons working on behalf and the organization;

e) threats and consequences to local communities and other stakeholders and the potential impact of operations on their human rights;

f) risks related to business relationships, such as the use of subcontractors, outsource partners and interactions with other organizations engaged in security operations;

g) the interrelationships between tactical and operational risks and the need to respect human life and rights.

Many methodologies exist for risk assessments. The organization should establish, implement and maintain a formal methodology that is documented and repeatable. Assumptions, scope, evaluation criteria and results should be clearly defined and reviewed by top management.

Since an organization might have many risks, it should establish and document criteria and a methodology to determine those that it will consider significant. There is no single method for determining significant risks. However, the method used should provide consistent results and include the establishment and application of evaluation criteria, such as those related to protection of life and human rights, the severity of adverse human rights impacts, its leverage to prevent or mitigate adverse impacts, criticality of activities and functions, legal issues and the concerns of internal and external stakeholders. An organization should analyse likelihood, severity and consequences of disruptive and undesirable events to its operations and stakeholders, and identify critical operations that are given high priority for developing response and recovery times and objectives.

When assessing consequences the organizations should consider the following.

a) Human cost: Physical and psychological harm to clients, persons working on its behalf, suppliers, local communities and other stakeholders.

b) Financial cost: Equipment and property replacement, downtime, overtime pay, stock devaluation, lost sales/business, lawsuits, regulatory fines/penalties, etc.

c) Image cost: Reputation, standing in the community, negative press, loss of clients, etc.

d) Human rights impacts: Actual and potential adverse human rights impacts on specific people and groups, in particular vulnerable or marginalized groups, within the specific context of operations.

e) Indirect impacts: On the regional economy and reduction in the regional net economy, etc.

f) Environmental impacts: Degradation to the quality of the environment or to endangered species.

The risk assessment is an inclusive process that draws on the requisite internal and external human rights expertise and involves meaningful consultation with internal and external stakeholders, including potentially adversely impacted stakeholders. The risk and impact identification, analysis and evaluation processes are framed within the operating environment of the organization; therefore, they should take into account the internal and external context and legal and other requirements.

To achieve results that accurately reflect the risk profile of the organization, data for the risk assessment should be gathered by a competently trained team, including suitably qualified and recognized human rights experts. The sampling techniques for the collection of administrative, financial, technical, social and physical data should be selected to assure representative samples. The risk assessment is not an exact science: therefore, assumptions and reliability of information should be documented. All operational units of the organization within scope of the SOMS should be directly consulted during the data-gathering process. Results of the risk assessment should be reported and reviewed by top management in order to establish the security operations management objectives, targets and strategies. The organization should define the scope of the risk assessment based on:

a) SOMS scope (products, services and activities);

b) client expectations and obligations;

c) legal, regulatory and contractual requirements;

d) responsibility to respect human rights;

e) impacted communities' and stakeholders' expectations;

f) risk appetite;

g) business relationships, interdependencies and infrastructure requirements;

h) data/information requirements.

The risk assessment process should consider normal and abnormal operating conditions, as well as reasonably foreseeable disruptive situations, in order to better control disruptive and undesirable events. However, it is not possible to foresee all disruptive and undesirable situations, so the organization should also consider the consequences of an event on critical assets, activities and functions, as well as impacted communities and stakeholders, regardless of the nature of an event in order to pre-emptively manage its risks.

The risk assessment should:

a) use a documented quantitative and/or qualitative methodology to estimate likelihood or probability of the identified potential risks and significance of their consequences if an event materializes;

b) be based on reasonable and defined criteria;

c) give due consideration to all potential risks it recognizes to its operations;

d) consider its dependencies on others and others dependencies on the organization, including client, community, business relationships and supply chain dependencies and obligations;

e) evaluate the consequences of legal and other obligations and voluntary commitments which govern the organization's activities;

f) consider risks associated with stakeholders, contractors, outsource partners, suppliers and other affected parties;

g) analyse information on risks and select those risks which may cause significant consequences and/or those risks whose consequence is hard to be determined in terms of significance;

h) analyse and evaluate the costs, benefits and resources needed to manage risks;

i) evaluate risks and impacts it can control and influence through its leverage.

NOTE It is the organization that determines the degree of control and its strategies for risk acceptance, avoidance, management, minimization, tolerance transfer and/or treatment.

In some locations, critical infrastructure, community assets and cultural heritage may be important elements of the surroundings in which an organization operates, and therefore should be taken into account in the understanding of its risks and impact on surroundings.

When developing information relating to its significant risks, the organization should consider the need to retain the information for historical purposes, and to design and implement its SOMS.

The process of identification and evaluation of risks should take into account the location of activities, the cost and time of undertaking the analysis, and the availability of reliable data. Information already developed for business planning, regulatory, or other purposes may be used in this process.

At regular intervals, the organization should revisit its reassessment throughout the life of an activity and to address changing organizational operations, operating environments, and in response to events. Changes that may elicit a revisit of the reassessment include changes in:

a) contractual and industry trends;

b) business relationships;

c) new activities and major changes in operations;

b) regulatory requirements;

c) political environment;

d) conditions due to an event;

e) performance based test/exercise results.

This process of identifying and evaluating risks is not intended to change or increase an organization's legal obligations.

A.6.1.3 Internal and external risk communication and consultation

The organization should establish a formal communication and consultation process with appropriate stakeholders both for the collection of risk assessment input information and for the controlled dissemination of the outcomes. Sensitivity and integrity of the information should be considered in the risk communication and consultation processes.

A.6.2 Security operations objectives and planning to achieve them

A.6.2.1 General

Objectives and targets are established to meet the goals and commitments of the organization's security operations policy. By setting the security operations objectives and targets, the organization can translate the policy into action plans it describes in the security operations strategies. The objectives and targets should be specific and measureable in order to track progress and ascertain how the SOMS is performing in improving overall organizational preparedness.

SOMS "objectives" are overriding considerations such as minimizing accidents. Security operations "targets" are specific metrics for measuring performance based on the key performance indicators. Objectives and targets should be appropriate for the organization, based on the risk assessment. The objectives and targets should reflect what the organization does, how well it is performing and what it wants to achieve. Appropriate levels of management should define the objectives and targets. Objectives and targets should be periodically reviewed and revised.

When the objectives and targets are set, the organization should consider establishing measurable security operations key performance indicators. These indicators can be used as the basis for a security operations performance evaluation system and can provide information on the SOMS and specific prevention, mitigation, response and recovery strategies.

In establishing its objectives and targets the organization should consider:

a) policy commitments;

b) alignment with strategic objectives;

c) outcomes of the risk assessment;

d) risk appetite and tolerance;

e) legal and other requirements;

f) internal and external context;

g) performance criteria;

h) infrastructure requirements and interdependencies;

i) interests of stakeholders;

j) technology options;

k) financial, operational and other organizational considerations;

l) actions, resources and timescales needed to achieve objectives.

When considering its technological options, an organization should consider the use of best available technologies where economically viable, cost-effective and judged appropriate.

The reference to the financial requirements of the organization is not intended to imply that organizations are obliged to use specific cost-accounting methodologies; however, the organization may choose to consider direct, indirect and hidden costs.

A.6.2.2 Achieving security operations and risk treatment objectives

The security operations strategies and action plans are documented approaches to achieve the organization's objectives and targets. Strategies should be coordinated or integrated with other organizational plans, strategies and budgets. Action plans may be subdivided to address specific elements of the organization's operations.

To successfully manage security operations, the strategies and action plans should define:

a) responsibilities for achieving goals (who will do it? where will it be done?);

b) means and resources for achieving goals (how to do it?);

c) timeframe for achieving those goals (when will it be done?).

The strategies may be subdivided to address specific elements of the organization's operations. The organization may use several action plans as long as the key responsibilities, tactical steps, resource needs and schedules are adequately defined in each of the documented plans.

The strategies should include – where appropriate and practical – consideration of all stages of an organization's activities related to planning, design, construction, commissioning, operation, retrofitting, production, marketing, outsourcing and decommissioning. Strategy development may be undertaken for current activities and new activities, products and/or services.

The organization's planning should take into account the priority of activities, contractual obligations, employee and neighbouring community necessities and operational continuity.

Strategies should be dynamic and monitored and modified when:

a) outcomes of the risk assessment change;

b) objectives and targets are modified or added;

c) relevant legal requirements are introduced or changed;

d) substantial progress in achieving the objectives and targets has been made (or has not been made);

e) activities, products, services, processes, or facilities change or other issues arise.

Determining security operations strategy enables the organization to evaluate a range of options. The organization may choose an appropriate approach for each activity, such that it can operate at an acceptable level. The most appropriate strategy or strategies should depend on a range of factors such as:

a) the results of the organization's risk assessment;

b) the costs of implementing a strategy or strategies;

c) the consequences of inaction.

Top management should approve documented strategies to confirm that the determination of security operations strategies has been properly undertaken, that they have addressed the likely causes and effects of an undesirable or disruptive event, and that the chosen strategies are appropriate to meet the organization's objectives within the organizations risk appetite.

The strategies should also consider the organization's relationships, interdependencies and obligations with external stakeholders. These stakeholders include clients, suppliers and outsource partners – as well as public authorities and others in the community. The organization should establish and maintain strategies that first and foremost protect life and safety of stakeholders while respecting human rights and preserving the integrity of its delivery of products and services. In addition, interactions and coordination with public authorities and others in the community should be determined and included in strategy development. These strategic arrangements with external stakeholders should support the achievement of security operations objectives and be clearly defined and documented.

A.7 Support

A7.1 Resources

A.7.1.1 General

The resources needed for the SOMS should be identified. These include human resources and specialized skills, equipment, internal infrastructure, technology, information, intelligence and financial resources. Top management should ensure the availability of resources essential for the establishment, implementation, control, testing and maintenance of the SOMS.

A.7.1.2 Structural requirements

A.7.1.2.1 General

A contract provides the principal legal basis for the relationship between the client and contractor. The organization entering into a contract should be a legal entity and signatures for the organization should be clearly authorized to enter into contracts on the organization's behalf.

A.7.1.2.2 Organizational structure

The organization should establish a management structure clearly defining the roles, responsibilities and accountabilities necessary to meeting its contractual obligations.

A.7.1.2.3 Insurance

The organization should seek insurance coverage sufficient to meet any liability for damages to any person with respect to personal injury, death, or damage to property consistent with its risk assessment. The limit of such coverage should at least be at the minimum level as prescribed by the client or recognized as best industry practice. Insurance should include employer's liability and public liability coverage. Foreign and local personnel should be provided with health and life insurance policies appropriate to their wage structure and the level of risk of their service as required by law.

When seeking insurance coverage the organization should consider:

a) the policies and limits to be held by the organization should be specified in the contract;

b) the jurisdiction of the policy and in the event of a dispute;

c) the territorial limitations;

d) limitations of indemnity;

e) coverage of all activities, including use of weapons;

f) medical coverage and treatment of persons working on behalf of the organization and impacted communities;

g) activities of subcontractors;

h) protection of the client.

Examples of the types of coverage to consider include (but are not limited to):

a) liability;

b) workers compensation;

c) accident;

d) property damage;

e) kidnapping, ransom and/or captive;

f) keyman.

A.7.1.2.4 Outsourcing and subcontracting

A contract should provide the legal basis for the relationship between the contractor and subcontractor. The organization is responsible for all activities outsourced to another entity. The contract should specify the responsibilities, terms and conditions under which the subcontractor is to perform.

A.7.1.2.5 Financial and administrative procedures and controls

An organization's financial and administrative procedures and controls to support the provision of effective security and risk management should also address salient financial risks.

A7.2 Competence

The organization should identify the awareness, knowledge, understanding and skills needed by any person with the responsibility and authority to perform tasks on its behalf including:

a) establishing training and awareness programmes for internal and external stakeholders who may be affected by an undesirable or disruptive event:

b) requiring that subcontractors working on its behalf are able to demonstrate that their employees have the requisite competence and/or appropriate training:

c) determining the level of experience, competence and training necessary to ensure the capability of personnel having documented responsibility for carrying out specialized SOMS management activities;

d) monitoring and reassessing the level of training should be conducted on an ongoing basis to identify opportunities for improvement.

It is the organization's responsibility that all persons working on behalf of the organization are sufficiently trained, both prior to any deployment and on an ongoing basis, in the performance of their functions and to respect relevant local, national and humanitarian and human rights laws. Defined training objectives should be based on the risk assessment and facilitate uniformity and standardization of training requirements. Training should specifically include human rights training on key subject matters such as:

a) prohibition of torture or other cruel, inhuman, or degrading treatment;

b) prohibition and awareness of sexual exploitation and abuse- or gender-based violence;

c) recognition and prevention of human trafficking and slavery.

The organization should identify and assess any differences between the competence needed to perform a security operations activity and that possessed by the individual required to perform the activity. This difference can be rectified through additional education, training, or skills development programme which may include the following steps:

a) identification of competence and training needs;

b) design and development of a training plan to address defined competence and training needs;

c) selection of suitable methods and materials;

d) verification of conformity with SOMS training requirements;

e) training of target groups;

f) documentation and monitoring of training received;

g) evaluation of training received against defined training needs and requirements;

h) improvement of the training programme, as needed.

Training may include general and task- and context-specific topics, preparing personnel for performance under the specific contract and in the specific circumstances. General topics include, but are not limited to:

a) use of force procedures and firearms;

b) humanitarian law and human rights law;

c) religious, gender and cultural issues, and respect for the local population;

d) handling complaints by the civilian population: in particular, by transmitting them to the appropriate authority;

e) measures against bribery, corruption and other related crimes.

Examples of task and context specific topics may include:

a) tactical driving;

b) interview techniques;

c) land navigation;

d) electronic communications

e) medical aid;

f) community liaison;

g) casualty evacuation;

h) other specified and implied tasks under the terms of the contract or services offered by the organization.

The organization should use practical, scenario-driven training that will require persons trained to make decisions in situations that reflect conditions that may be faced by security personnel in the performance of their missions, and that will require them to react to the consequences of those decisions. IHL training should be structured to meet the specific conditions faced by the organization's security operations in conditions of armed conflict. Training will focus on the civilian status of the organization, the consequences of activities that would result in a loss of that status, and individual liability for violations of the IHL or international human rights law.

A training and awareness programme may include:

a) a consultation process with staff throughout the organization concerning the implementation of the security operations management programme;

b) discussion of security operations management in the organization's newsletters, briefings, induction programme, or journals (including new employee orientation);

c) inclusion of security operations management on relevant web pages or intranets;

d) online training modules housed in the organization's learning management system;

e) learning from internal and external incidents through after action reports; f

) security operations management as an item at management team meetings;

g) conferences and classroom training;

h) first aid and other hands-on training.

All personnel should receive training to perform their individual SOMS-related responsibilities. They should receive briefs and training on the key components of the SOMS, as well as the human rights, humanitarian law and relevant criminal law that affect their activities directly. Such training could include procedures for prevention and mitigation measures, response, documentation and accountability requirements, the handling of local community, client and media inquiries.

Weapons training, including less lethal weapons, should be conducted to a written standard appropriate to the weapon and the expected conditions of use. Training should include instruction, scenario-based training and mechanical training – to include weapons malfunctions and live fire qualification. Initial training should be repeated at regular intervals, not less than annually, or more frequently if required by contract of statute.

Event response teams should receive education and training about their responsibilities and duties, including interactions with first responders and other internal and external stakeholders. Team members should be trained at regular intervals (at least annually). New members should be trained when they join the organization. These teams should also receive training on prevention of undesirable events. The organization should include relevant external stakeholders and resources in their competence, awareness and training programmes.

A.7.3 Awareness

The organization should build, promote and embed a security operations management culture within the organization that:

a) ensures the security operations management culture and respect for human rights becomes part of the organization's core values and governance;

b) makes stakeholders aware of the security operations management policy and their role in any plans;

c) benefits improved personal performance.

A.7.4 Communication

A.7.4.1 General

Arrangements should be made for communication and consultation, internally and externally, during normal and abnormal conditions. Effective communication is one of the most important ingredients in preventing, managing and reporting an undesirable or disruptive event. Proactive communications and consultation planning should be conducted with internal and external stakeholders in order to convey day-to-day, alert, disruptive event and organizational and community response information. To provide the best communications and suitable messages for various groups, it may be appropriate to segment the audiences. In this way, messages may be tailored that can be released to specific groups such as employees, clients, the local community, or the media.

The communication and consultation procedures and processes should consider:

a) internal communication between the various levels and activities of the organization and with subcontractors, clients and partner entities;

b) needs of stakeholders;

c) receiving, documenting and responding to relevant communications from external stakeholders (including local communities);

d) proactive planning of communications with external stakeholders (including the media);

e) pre-emptive communication of response and reporting plans to applicable stakeholders facilitating communication and assuring stakeholders that proper planning is in place;

f) facilitating structured communication with emergency responders;

g) availability of the communication channels during a disruptive situation;

h) sensitivity and level of detail of the information;

i) the operational environment.

The organization should implement a procedure for receiving, documenting and responding to relevant communications from internal and external stakeholders. This procedure can include a dialogue with stakeholders and consideration of their relevant concerns. In some circumstances, responses to concerns of stakeholders may include relevant information about the risks, impacts and control procedures associated with the organization's activities and operations. These procedures should also address necessary communications with public authorities regarding emergency planning and other relevant issues.

A.7.4.2 Operational communications

Operational communication plans are necessary to provide adequate control, coordination and visibility over ongoing security operations. Such plans should include a description of how relevant threat information will be shared between security operations personnel, military forces and law

enforcement authorities, and how appropriate assistance will be provided to security operations personnel who become engaged in hostile situations. Information should be exchanged in a way that can be understood at each level of performance, with the client or other people that are protected by the organization, and with military or other public security forces encountered by the organization's security teams.

A.7.4.3 Risk communications

The organization should also identify and establish relationships with the community, public sector agencies, organizations and officials responsible for intelligence, warnings, prevention, response and recovery related to potential undesirable and disruptive events. The organization should formally plan its prevention, mitigation and response communications strategy, taking into account the decisions made specific to relevant target groups, the appropriate messages and subjects, and the choice of means.

The organization should establish procedures to communicate and consult with internal and external stakeholders specific to its risks, their impacts and control procedures. These procedures should consider the specific stakeholder group, the type of information to be communicated, the type of disruptive event and its consequences, the availability of methods of communication and the individual circumstances of the organization. Methods for external communication can include:

a) news or press releases;

b) media;

c) financial reports;

d) newsletters;

e) websites;

f) social media;

g) phone calls, emails and text messages (manually delivered and/or via automated emergency notification systems);

h) voice mails;

i) community meetings.

The organization should conduct preplanning of communication for a disruptive event. Draft message templates, scripts and statements can be crafted in advance for threats identified in the risk assessment, for distribution to one or more stakeholder groups identified in the risk assessment. Procedures to ensure that communications can be distributed on short notice should also be established.

The organization should designate and publicize the name of a primary spokesperson (with back-ups identified) who should manage/disseminate crisis communications to the media and others. These individuals should receive training in media relations in preparation for a crisis, and on an ongoing basis. All information should be funnelled through a single team to assure the consistency of messages. Top management should stress that all organization personnel should be informed quickly regarding where to refer calls from the media and that only authorized company spokespeople may speak to the media. In some situations, an appropriately trained site spokesperson may also be necessary.

A.7.4.4 Communicating complaint and grievance procedures

The organization should establish and communicate to relevant stakeholders internal and external complaints and grievances procedures. The procedures should assure privacy and confidentiality and be tailored to the culture, language, education and technology requirements of the target audience. Procedures should be established for creating a reporting mechanism for anonymous and non-anonymous complaints and grievances.

A.7.4.5 Communicating whistle-blower policy

Whistleblowing occurs when a person working on behalf of the organization raises a concern about danger, unethical conduct, or illegality that affects others, internally or externally. Persons working on the organization's behalf may be fearful that raising the alarm will lead to retribution from their colleagues or employer. However, the organization should encourage persons working on its behalf to voice their concerns over malpractice and inappropriate acts against any internal or external stakeholder. A whistle-blower policy will help the organization deal with a concern in an appropriate manner. A whistle-blower policy can also serve as a deterrent to those who may be considering an illegal, improper, or unethical practice. A good whistle-blower policy will help the organization to reduce problems and improve working conditions and operational effectiveness.

Effective whistle-blower policies provide individuals with an alternative route other than their direct line management through which to raise their concerns. Therefore, organizations should establish and communicate a whistle-blower policy that provides for a clear internal mechanism for anonymously reporting non-conformances and concerns about danger, unethical conduct, or illegality that affects others, internally or externally. The policy should also designate circumstances and conditions where external disclosures are acceptable and protected, and where matters need to be referred to the appropriate authority. Whistle-blowers should receive protection for raising concerns so long as they have acted in good faith and have reasonable grounds for raising a concern.

A.7.5 Documented information

A.7.5.1 General

The level of detail of the documentation should be sufficient to describe the SOMS and how the parts work together. The documentation should also provide direction on where to obtain more detailed information on the operation of specific parts of the SOMS. This documentation may be integrated with documentation of other management systems implemented by the organization. It does not have to be in the form of a manual.

The extent of the SOMS documentation can differ from one organization to another due to:

a) the size and type of organization and its activities, products, or services;

b) the complexity of processes and their interactions.

Examples of documents include:

a) policy, objectives and targets;

b) Statement of Applicability, Statement of Conformance and Code of Ethics;

c) information on significant risks and impacts;

d) procedures;

e) process information;

f) organizational charts;

g) internal and external standards;

h) incident response, mitigation, emergency and crisis plans;

i) records.

Any decision to document procedures should be based on:

a) the consequences, including those to tangible and intangible assets, of not doing so;

b) the need to demonstrate compliance with legal and with other requirements to which the organization subscribes;

c) the need to ensure that the activity is undertaken consistently;

d) the requirements of this International Standard.

The advantages of effective documentation include:

a) easier implementation through communication and training;

b) easier maintenance and revision;

c) less risk of ambiguity and deviations;

d) demonstrability and visibility.

Documents originally created for purposes other than the SOMS may be used as part of this management system and (if so used) should be referenced in the system.

A.7.5.2 Creating and updating

A.7.5.2.1 General

Procedures should include control of the identification, accessibility, integrity and security of the documented information.

A.7.5.2.2 Records

In addition to the records required by this International Standard, records may also include (among others):

a) compliance records;

b) authorization to possess weapons;

c) accountability for serialized and sensitive equipment;

d) reports for fuel, ammunition and training materials;

e) tracking of weapons, explosives, vehicles and hazardous materials;

f) use of force reports (lethal and non-lethal);

g) contract compliance audit reports;

h) export/import compliance reports;

i) audit trail documentation;

j) licensing;

k) exercise and testing results;

l) access control records;

m) subcontractor documentation.

A.7.5.3 Control of documented information

The organization should create and maintain documents in a manner sufficient to implement the SOMS. However, the primary focus of the organization should be on the effective implementation of the SOMS and on security operations management performance and not on a complex document control system.

Proper account should be taken of confidential information. Procedures should be established, communicated and maintained for the handling of classified information. This information should be clearly graded and labelled to protect:

a) the sensitivity of the information;

b) the privacy, life and safety of individuals;

c) the image and reputation of the client.

The organization should consult with the appropriate legal authority within their organization to determine the appropriate period of time the documents should be retained and establish, implement and maintain the processes to effectively do so. Records should be retained for a minimum of seven years or as otherwise required or limited by law.

A.8 Operations

A.8.1 Operational planning and control

A.8.1.1 General

An organization should evaluate those of its operations that are associated with its identified significant risks, and should ensure that they are conducted in a way that will control or reduce the likelihood and adverse consequences associated with them in order to fulfil the requirements of its security operations management policy and meet its objectives and targets. This should include all parts of its operations including subcontractor, supply chain and maintenance activities.

As this part of the SOMS provides direction on how to take the system requirements into day-to-day operations, it requires the use of documented procedures to control situations where the absence of documented procedures could lead to deviations from the security operations management policy, objectives and targets.

To minimize the likelihood of an undesirable or disruptive event, these procedures should include administrative, operational and technological controls. Where existing arrangements are revised or new arrangements introduced that could impact on operations and activities, the organization should consider the associated minimization of threats and risks before their implementation.

A.8.1.2 Performance of security-related functions

A.8.1.2.1 General

Procedures should support the provision of security-related functions for the protection of people and tangible and intangible assets consistent with legal requirements, contractual obligations and respect for human rights.

A.8.1.2.2 First aid and casualty care

All personnel should receive initial and recurrent training in first aid and casualty care with special emphasis on immediate response to traumatic injury following an attack or accident. Training should be conducted to an accepted standard. Minimally, training should include maintaining or establishing appropriate security and safety of the treatment area, casualty stabilization, preparation and request for evacuation. This includes assuring that the individual being treated does not continue to pose a deliberate or unintentional threat to other persons in the vicinity. Training should also include prioritizing casualties for treatment based on severity of injury, without regard for friendly/enemy status, race, ethnic background, or other discrimination. The organization should ensure that individuals and security teams are equipped with the materials necessary to provide immediate treatment and stabilization of survivable traumatic injuries while awaiting casualty evacuation.

A.8.1.3 Respect for human rights

Organizations are obliged to respect and comply with IHL and human rights law imposed upon them by applicable national law, as well as international human rights standards. They should establish, implement and document procedures to protect the human dignity and treat all persons humanely. Procedures should be established and communicated to appropriate parties to report and remediate any non-compliances and non-conformances.

A.8.1.4 Prevention and management of undesirable or disruptive events

Procedures should emphasise the pre-emptive and proactive management of risks that may lead to undesirable and disruptive events, as well as address response, recovery and remediation measures should an event occur.

The organization should establish appropriate administrative and financial structures to effectively support the SOMS, before, during and after an undesirable or disruptive event. Procedures should be established and documented to ensure transparency with regard to authorizations, consistent with generally accepted accounting procedures and industry good practices. Therefore, a management structure, authorities and responsibility delegation for decision-making (including spending limitations, authorities and responsibility for implementation) should be clearly defined.

A.8.2 Establishing norms of behaviour and codes of ethical conduct

The organization should establish, implement and maintain a Code of Ethics for its employees, subcontractors and outsource partners. The Code of Ethics should clearly communicate respect for human rights and the dignity of human beings, as well as the prohibition of bribery, conflicts of interest, corruption and other crimes (e.g. use of legal or illegal substances which impact on performance). The Code of Ethics should ensure that all persons working on behalf of the organization understand their responsibilities to abide by human rights, local, national and international law, and to prevent and report any abuses of human rights including (but not limited to) prohibition of:

a) torture or other cruel, inhuman, or degrading treatment or punishment;

b) sexual exploitation and abuse or gender-based violence;

c) human trafficking;

d) slavery and forced labour;

e) the worst forms of child labour;

f) unlawful discrimination.

The organization should clearly communicate and provide training on the Code of Ethics to all persons working on behalf of the organization. The organization should document and maintain records of communication and training.

A.8.3 Use of force

A.8.3.1 General

The greatest risks presented by private security operations are associated with inappropriate use of force and firearms by the organization's personnel. This includes any use of force by the organization's personnel which exceeds what is necessary or reasonable under the circumstances presented to those personnel. Inappropriate use of force could result in death or serious injury to innocent parties which could result in damage to the organization's reputation and legal liability to the company and the party it protects. It could also lead to further insecurity and instability which will affect the organization, those it protects and other actors working in the area. Inappropriate use of force also includes the failure to use available force that is necessary to prevent loss of life of the organization's personnel, those people and resources it protects and others in the nearby vicinity.

The organization's use of force procedures are the critical tools for managing the risk of inappropriate use of force and therefore need to be:

a) clear and understood by all persons authorized to carry weapons and those who supervise them;

b) applicable in complex situations and ambiguous circumstances;

c) rigidly enforced by the organization, even when legal enforcement of the use of force is weak.

Clear procedures, effective training and unambiguous enforcement will facilitate the mission of the organization and any party it supports, and will promote adherence to the rule of law and long term stability of the area in which the organization operates.

A.8.3.2 Use of force policy

An organization may develop a use of force policy as an overarching statement about the allowable use of force across the organization's operational context. The policy should describe generally applicable principles to include:

a) the use of force only in self-defence, the defence of others, or to restrict access to or prevent destruction of specified property;

b) limiting the use of force to that which is necessary and reasonable to negate the threat;

c) the use of lethal force only in self-defence or the defence of others against an imminent threat of death or serious bodily injury and there is no other reasonable alternative available;

d) restriction from engaging in uniquely military functions such as combatant operations, combat- like operations, cordon and search operations, or offensive operations alone or in conjunction with armed forces of a state.

When developed, the organization's use of force policy forms the basis for the use of force procedures specific to scope of operations and the conditions or work for that location.

A.8.3.3 Use of force procedures

Use of force procedures:

— document the circumstances under which firearms and other force may be used in self-defence and the protection of specified persons (including other security operations personnel) or property against unlawful attack or some other injury attempted by another;

— guide personnel in the application of force, assuring that any use of force which is consistent with that policy is also consistent with local law or other controlling regulation as well as any codes of conduct to which the organization subscribes.

Wherever possible, these procedures should be developed in consultation with the party the organization protects. This assures a common understanding between those providing protection and those being protected and to promote procedures which support the mission and intent of the protected party.

A.8.3.4 General considerations for the use of force, firearms, or other weapons

The specific limitations on the use of force will vary from locality to locality and the specific operational environment. There are, however, certain broadly applicable principles which the organization should consider when developing its use of force procedures, including the following.

a) Lethal force is justified only under conditions of extreme necessity and as a last resort when all lesser means have failed, are likely to fail, or cannot reasonably be employed. Lethal force should only be used in self-defence or the defence of others against an imminent lethal threat, or when it is reasonable and necessary to prevent the commission of a serious offense involving grave threat to life or serious bodily harm.

b) Lesser degrees of force may be used in response to threats which do not pose an imminent threat of death or serious bodily harm or injury. These options range from physical presence to use of weapons such as batons and neural shock devices (e.g. Tasers), and measures in between. These measures are commonly referred to as "less-lethal" force as a reminder that regardless of intent, any use of force could result in unintentional serious injury or death. The risk of unintended lethal effects increases with the complexity and effectiveness of the device and decreases with the level of training and proficiency of the user and those directing use of force.

c) The authorization to use force in defence of property changes from locality to locality, sometimes changing between regional authorities under the same national government. Generally, lethal force is not authorized to protect property or to prevent unauthorized access to property. Common exceptions to this include:

   1) situations where the individual guarding the property perceives an imminent threat of death or serious injury in his (or her) attempt to block access to, or prevent the theft or destruction of, that property: in that situation, the use of force becomes that of self-defence;

   2) to prevent the actual theft or sabotage of inherently dangerous property, the loss or destruction of which would present an imminent threat of death or serious bodily harm (examples include firearms and other munitions, radiological materials and highly toxic chemicals or biological agents): reasonable and necessary use of force to protect these kinds of properties is generally considered defence of others.

d) Competent legal authority may also authorize the use of lethal force if it is reasonable and necessary to prevent the sabotage or destruction of critical infrastructure (e.g. essential public utilities and facilities), which are vital to public health or safety, and the damage to which would create an imminent threat of death or serious bodily harm or injury. In these situations, the authority would usually issue specific rules for the use of force to cover the protection of such infrastructure.

e) Use of force continuum. The organization's use of force procedures should describe the application of force along an operational continuum. Security operations personnel should attempt to resolve situations at the lowest levels of force or deescalate applied force if the situation and circumstances permit. Nonetheless, delay of force or sequential increase of force along a continuum is not required to resolve a situation or threat. In some cases sequential increase, or escalation of force, may increase risk to all parties. The objective of the use of force continuum is to use reasonable force when force is used to accomplish lawful objectives.

The organization's use of force procedures is not a legal document. It does not provide any protection to the organization or its personnel from prosecution arising from the use of force leading to serious injury or death. The use of force procedures can be cited in defence to charges of murder, manslaughter or other homicide, assault, or battery, demonstrating that the organization had clearly defined procedures for the use of force which were consistent with the applicable law at the time force was used. The procedures can also be used by the organization's personnel to demonstrate that the use of force was reasonable in degree and duration in the circumstances faced by the individual at that time and that it was not an ill-thought reaction, but disciplined and controlled, with due consideration for the safety of others.

The organization's use of force procedures may be more restrictive than what is permitted under applicable law. For example, the use of warning shots could be permitted under relevant law or regulation, but not required. The organization may determine that using warning shots presents an unnecessary risk of unintentional harm to bystanders by the un-aimed discharge of lethal weapons. Similarly, some legal regimes authorize broad use of force to protect others in the vicinity, even if they have no relation to the armed individual or his or her duties. The organization's use of force procedures, however, may restrict the use of force in defence of others in these circumstances. When considering such a restriction, the organization should consider that some legal regimes require the use of reasonable, necessary, and available force in the defence of others. In no circumstance, however, should the organization's use of force procedures restrict the inherent right of individual self-defence.

A.8.3.5 Rules for the use of force (RUF)

In some circumstances, the organization may be given RUF by a competent legal authority. Competent legal authorities include governments exercising control over the area the organization is operating in, governments contracting with the organization for security, or military commanders exercising authority equivalent to military occupation of an area.

RUF represent official authorizations for and limitations to the organization in its use of firearms and other force associated with its business operations. Typically, such RUF will include instructions regarding weapons authorization procedures, to include types of weapons, escalation of force to include requirements for warnings, clarifications and limitations on the use of force in self-defence, and communication and reporting requirements associated with the use of force.

The organization should conduct a comprehensive review of the RUF, this International Standard and other commitments to which the organization subscribes. The organization's use of force procedures should cover any elements in these sources which are missing from the RUF. The organization should also review the RUF to ensure it does not exceed the use of force permitted in this International Standard or restrict the use of reasonable and necessary force in self-defence. Should the published RUF exceed the use of force permitted by this International Standard or other applicable law, or unreasonably restrict the use of force in self-defence, the organization should seek modification of the RUF.

Wherever possible, the organization should seek approval by a competent legal authority of its use of force procedures to be issued as RUF.

A.8.3.6 Weapons authorization

The organization should develop procedures for identifying specific personnel who need to be armed to perform the organizations' security operations and the circumstances under which those personnel may carry weapons. Arming authorization should be limited to qualified personnel in accordance with the terms and conditions of a contract or if there is a reasonable expectation that life or assets will be jeopardized if weapons are not carried. The organization should document its due diligence procedures appropriate to the region where security operations are being performed against applicable and relevant national law of its personnel to assess whether an individual is prohibited from possessing or carrying a weapon. The organization should not issue weapons to its personnel until background investigations for that individual are complete. Arming authorization procedures should restrict personnel from carrying weapons on security operations until the individual has been trained and certified on the use of those specific weapons. The organization's procedures should specify the conditions under which weapons authorization may be suspended or revoked and the authority for such action.

The organization should also consider restricting access to weapons in the following circumstances:

a) when not performing security operations;

b) within eight or more hours after the consumption of alcoholic beverages;

c) while under prescription medication that may impair reaction or judgment;

d) immediately following report of an undesirable event;

e) upon receipt of allegations of noncompliance with established RUF or use of force procedures.

For all persons authorized to carry weapons on behalf of the organization, there should be a record of:

a) proof of authorization to carry weapons;

b) a current record of weapons training, qualification and competence specific to authorized type and model;

c) issuance and return of the specific weapon used in performance of duties;

d) weapons maintenance;

e) weapons usage (discharge of weapon outside of training.)

The organization should develop procedures to maintain and access these records for each person for as long as the individual is authorized to use or carry weapons or for a longer period as required by law.

A.8.3.7 Use of force training

RUF and use of force policy and procedures should be communicated to persons working on behalf of the organization at a level of detail appropriate to the target audience. Training should include all major elements of the organization's use of force procedures and authorized RUF appropriate to the level and expected tasks to be performed by the personnel being trained. Special attention should be paid to the following areas:

a) applicable laws of self-defence to particular security operations;

b) when and where organization personnel may be armed;

c) storage of weapons when not on duty;

d) the concepts of self-defence and the defence of others;

e) what is reasonable and necessary;

f) the consequences of non-conformance with either use of force procedures or authorized RUF;

g) the potential criminal and civil liabilities that may be faced by the individual or organization resulting from the use of force (this includes supervisory responsibility for action or inaction and individual responsibility regardless of supervisory orders or instructions given by to the individual);

h) the differences between rules of engagement (ROE) appropriate for armed forces and use of force procedures or RUF applicable to civilian self-defence. (In many cases, private security personnel will come from a military background where they learned use of force consistent with ROE. In addition, private security operations may be conducted in an environment where they are working alongside of, or with, military forces operating under ROE.) A clear understanding of the differences is critical for both the private security and military operations.

Training should include instruction on the application of force as part of a continuum of responses and evaluate the individual's understanding within that continuum. The goal is for the individual to understand and be able to apply only that amount of force reasonably necessary to stop a threat yet effective and sufficient to protect people and property from attack or other violence. At a minimum, the continuum, or the graduated use of force should include training in the following techniques and the appropriate indicators for their use and the success or failure of that technique.

a) Personnel presence: Presence as deterrence.

b) Verbalization: Force is not-physical; shouting of verbal warnings to desist activities.

c) Empty-hand control: Use of bodily force to gain control of a situation, physically restrain, block access or detain the adversary.

d) Less-lethal methods: Use less-lethal technologies to gain control of a situation.

e) Threat of lethal force: Showing a weapon and demonstrate the intent to use it.

f) Lethal force: Use of lethal weapons to gain control of a situation. Shoot to remove the threat only where necessary. Fire only aimed shots and with due regard for the safety of bystanders.

Use of force training should address:

a) the use of force continuum;

b) the role of supervisory authority in the control of that force (including the authority and limits on the authority to direct and escalation or de-escalation of force);

c) the roles and authority of the organization's supervisory personnel, the protected party and legal authorities such as police or military personnel in directing or restricting the use of force.

Training programmes should include academic (classroom), mechanical, live fire and scenario based training. Individuals should be presented with situations similar to those which they may face during their conduct of security operations. These situations should be appropriate to the individual tasks and require the individual to apply judgment and initiate appropriate responses in situations of increasing complexity and ambiguity. Live fire training should also be relevant to the requirements of the particular security operations. Examples include, but are not limited to, quick-fire at short ranges, disabling fire directed against moving vehicles, use of barricades and obstacles, or firing from moving vehicles. The organization should use realistic, measurable and objective standards for demonstrating proficiency. Standards in weapons qualification should be consistent with published military or industry standards appropriate to the security tasks expected of the individual and should be agreed by the entity being protected whenever possible.

A.8.4 Apprehension and search

A.8.4.1 Apprehension of persons

The organization should provide training for its personnel in the apprehension of persons. This is normally limited to persons apprehended following an attack against the organization's personnel, clients, or property under the organization's protection. It should also include actions taken when an individual attempts to leave an access control point without permission. Training should be theoretical, practical and emphasise the protection of persons and property from further attack, while treating apprehended persons humanely. Training should include measures for protecting the apprehended person from attack or violence, reporting the apprehension to the client and proper authorities, and transferring apprehended persons to the appropriate authority at the earliest opportunity. The organization should document the transfer of custody including the apprehended person's identity, alleged offense and to whom the individual was transferred.

A.8.4.2 Search

The organization should establish procedures for searching personnel that are consistent with the dignity and humane treatment of persons being searched while assuring the safety of clients, property under protection and the safety of organization personnel and bystanders. Organizations should document and safeguard personal effects retained following a search. Training will distinguish between minimally invasive searches of persons at static guard posts and the comprehensive searches required after apprehension.

Search of apprehended persons procedures should address:

a) the distinction between persons under apprehension as the result of attack or imminent threat and the voluntary search of persons at access control points;

b) the balance between rendering any first aid required to preserve life and the need to assure that the individual being searched does not present an imminent threat of death or serious bodily harm to those in the vicinity;

c) the actions regarding persons who refuse to be searched or those who attempt to leave the area after learning that they will be searched.

A.8.5 Operations in support of law enforcement

The organization should consult with competent legal counsel before entering into law enforcement or related activities.

A.8.6 Resources, roles, responsibility and authority

A.8.6.1 General

The successful implementation of an SOMS calls for a commitment from all persons working for the organization or on its behalf. The roles, responsibilities and authorities of individuals should be clearly defined to ensure implementation of the SOMS, prevent misunderstandings (particularly during an undesirable or disruptive event) and avoid missed tasks.

Roles, responsibilities and authorities should also be defined, documented and communicated for coordination with external stakeholders. This should include interactions with subcontractors, partners, suppliers, public authorities and local communities. The organization should define and communicate the responsibilities and authorities of all persons engaged in security operations management regardless of their other roles in the organization. The resources provided by top management should enable the fulfilment of the roles and responsibilities assigned. The roles, responsibilities and authorities should be reviewed when a change in the operational context of the organization occurs.

It is necessary that an appropriate administrative structure be put in place to effectively deal with incident management during an undesirable or disruptive event. Clear definitions should exist for a management structure, authority for decisions and responsibility for implementation. An organization should have an "incident management team" to lead event response under the clear direction of top management or its representatives. The team should be comprised of such functions as:

a) planning;

b) incident response and management;

c) human resource management;

d) health, safety and medical response;

e) information management;

f) security;

g) legal;

h) communications/media relations;

i) other critical support functions.

The incident management team may be supported by as many teams as appropriate taking into account such factors as organization size and type, number of employees, location, etc. Teams should develop response plans to address various aspects of potential crises – such as damage assessment and control, communications, human resources, information technology and administrative support. Incident response and management plans should be consistent with and included within the overall SOMS. Individuals should be recruited for membership on incident management teams based upon their skills, level of commitment and vested interest.

A.8.6.2 Personnel

A.8.6.2.1 General

Personnel, competence and training needs are an output of the context of the organization and its contractual requirements, as well as the risk assessment and definition of objectives.

Organizations should establish procedures for the welfare of persons working on their behalf, consistent with the protections provided by applicable labour and other laws including:

a) providing personnel a copy of any contract to which they are party to, in a language they understand;

b) providing personnel with adequate pay and remuneration arrangements commensurate to their responsibilities and working conditions;

c) adopting operational safety and health policies;

d) ensuring personnel unrestricted access to their own travel documents;

e) preventing unlawful discrimination in employment.

The privacy and confidentiality of information about individuals should be protected. Background and operational information about individuals can be highly sensitive. It is essential that the organization establish and maintain procedures to appropriately and strictly secure the confidentiality of information both internally and externally. The organization should retain relevant documents in a secure manner for a period of time that complies with applicable laws and regulations, contractual requirements and the organization's records policies.

At a minimum, the following information should be documented for all personnel:

a) name, address and contact information;

b) contact information for immediate family and persons to notify in event of injury or death;

c) personal identification information;

d) information required by legal and other requirements.

A.8.6.2.2 Selection, background screening and vetting of personnel

The organization should establish a documented procedure for pre-employment background checks and vetting of individuals working on behalf of the organization. The organization should establish, document, implement and maintain procedures that screen out personnel who do not meet minimum qualifications established for positions, and select appropriately qualified personnel based on their knowledge, skills, abilities and other attributes. The screening and selection procedures should be consistent with legal, contractual requirements and the principles of the *Montreux Document* and the *ICoC*. The screening and vetting process should be based on the nature of the job for which the candidate is being considered, the person's level of authority and the area of specialization. The screening and vetting should take place before the candidate is offered a position and commences work. Candidates should sign appropriate authorizations and consents prior to performing background screening. A decision to retain the services of an individual should be based on the totality of the candidate's qualifications and the results of the background screening and vetting.

Wherever possible, the screening and vetting process should include:

a) identity verification;

b) personal history verification;

c) experience, qualifications;

d) other credentials verification.

Exclusions should be documented when information is unavailable, unreliable, or unsuitable.

Identity verification should include verification of the validity of personal history and minimum age of the prospective employee. Personal history, validated by personal history searches when available, should consider (but not be limited to):

a) home addresses;

b) employment records;

c) electronic media;

d) criminal and civil record history;

e) records of human rights violations;

f) military or law enforcement service records;

g) motor vehicle records;

h) credit reports;

i) sexual offender indices;

j) government and industry sanctions lists;

k) industry specific licensing records.

In verifying the experience and qualifications that are presented by the candidate, the organization should look for unexplained gaps. This should provide information on, but is not limited to:

a) education verification;

b) employment verification;

c) licensure/certification/registration verification;

d) personal references;

e) supervisor and co-worker interviews;

f) military and law enforcement history verification.

The organization should also establish clearly defined criteria for the screening and vetting of individuals based on:

a) substance abuse;

b) physical and mental fitness for activities;

c) unsuitability to carry weapons;

d) ability to operate in stressful and adverse conditions.

The privacy and confidentiality of information about individuals should be protected. Personal documents, such as passports, licenses and original birth certificates, should be returned to personnel within a reasonable timeframe.

A.8.6.2.3 Selection, background screening and vetting of subcontractors

The organization should only retain the services, on a temporary or continuing basis, of competent subcontractors capable of operating in a manner consistent with this International Standard and the principles of the *Montreux Document* and the *ICoC*. The organization is responsible and liable for the subcontractor's work. The organization should establish, maintain and document clearly defined criteria for the screening and vetting of subcontractors to be used in contracting. Contractual agreements with subcontractors should be documented and retained in accordance with applicable laws and contractual obligations with the client.

Criteria for subcontracting should include the subcontractor's capacity to:

a) meet the requirements of this International Standard;

b) carry out its activities in compliance with relevant laws (local, national, humanitarian and human rights);

c) protect the image and reputation of the client;

d) provide adequate resources and expertise, including competent personnel, to meet operational objectives;

e) ensure transparency, accountability and appropriate supervision in the implementation of assigned duties;

f) take into account the financial and economic obligations (including appropriate remuneration of their personal and insurance coverage);

g) obtain requisite registrations, licenses, or authorizations;

h) maintain accurate and up to date personnel and property records;

i) acquire, use, return and dispose of weapons and ammunition in accordance with applicable laws and contractual obligations.

The organization should:

a) ensure appropriate written agreements with the subcontractor or outsource partner;

b) advise the client in writing of the arrangement and where appropriate obtain approval of the client;

c) be responsible for oversight of the training of personnel supplied by the subcontractor for use on the contract, including respect for human rights and avoidance of adverse impacts;

d) ensure that full insurance covering is provided for the activities of the subcontractor;

e) maintain a record of conformance with this International Standard for work subcontracted or outsourced.

A.8.6.3 Procurement and management of weapons, hazardous materials and munitions

The organization should establish and document its processes for compliance with national and international laws and regulations as regards the procurement, licensing and transhipment of firearms (and other controlled goods such as body armour and explosives) for use on operations. Therefore, the organization should establish, maintain and document procedures that ensure it:

a) acquires its munitions and equipment, in particular its weapons, lawfully (including "end user undertakings);

b) acquires and maintains legal authorization for the possession, transport, export and transhipment of firearms, ammunition and other controlled goods as required by applicable international and national law;

c) can identify and account for all ammunition and equipment, especially its weapons and hazardous materials (e.g. register of serial numbers, material safety data sheet (MSDS), safety data sheet (SDS), product safety data sheet (PSDS), or batch numbers);

d) uses munitions and equipment, in particular weapons that are not prohibited by international law;

e) sets criteria for the use of equipment, materials and weapons, appropriate for the task and operations, within the context of use for self-defence or the defence of others;

f) establishes a system of traceability for equipment, materials and weapons;

g) creates appropriate provision for the safe and secure storage, issue, maintenance, transport and use of equipment, materials and weapons;

h) carries out regular maintenance of firearms and security equipment to ensure that they remain fit and safe for purpose;

i) has complied with contractual provisions concerning return and/or disposition of weapons and ammunition.

Possession and use of weapons should be authorized by the organization and its subcontractors, as specified in the contract. For persons working on behalf of the organization, there should be a record of:

a) proof of authorization to carry weapons;

b) a current record of weapons training, qualification and competence;

c) weapons maintenance;

d) weapons usage.

A.8.6.4 Uniforms and markings

The organization should adopt and use uniforms and equipment markings that indicate the status of security operations team members and their company affiliation, using patterns, colours, or markings that are not easily confused with that of public security forces such as the military and police. Uniforms and markings selected by the organization or designated by the client may also be subject to approval by appropriate authorities in the country where the organization operates.

Standardized uniforms and marked vehicles provide an indication to the general public, police, military and other authorities that the security operations team members have authorization to carry and use weapons. Uniforms should include a badge number, name, or other means to distinguish individual organization personnel. Vehicle markings should include a company logo and unique number. Uniforms and other markings facilitate proper identification by the public in the event of a disruptive or undesirable event. This identification enables open and transparent reporting, and reduces the likelihood that one organization may be blamed for possible misconduct of another organization operating in the same area.

Uniforms can project a positive image about the organization and encourage professional and responsible behaviour by company personnel. In situations of armed conflict, distinguishable uniforms and markings can reduce the likelihood of security operations personnel being mistaken as combatants and targeted by hostile armed forces – where these forces are abiding by IHL. To be effective, information describing the uniforms, company logo, badges and unique vehicle markings should be made available to local authorities, to the public and – as applicable – to opposing armed forces.

There may be specific circumstances where a client may not wish security operations personnel to be readily identifiable as such. In other circumstances, the risk assessment may indicate that visible identification of armed security escorts will increase the threat of violence and danger to the client, the public and security personnel. In these situations, and when a more discreet approach is consistent with local law, security operations personnel may be directed to wear other functional clothing not easily distinguishable from civilian dress, will not carry arms openly, and vehicles will not stand out from other civilian traffic. Even in discreet or low-profile situations, security operations personnel should still maintain on their persons non-transferable means of personal identification.

A.8.7 Occupational health and safety

The organization should provide a safe and healthy working environment, recognizing the possible inherent dangers and limitations presented by the local environment. Reasonable precautions should be taken to protect all persons working on behalf of the organization – or those in their care – in high-risk or life-threatening situations.

A.8.8 Incident management

A.8.8.1 General

The organization should develop prevention, preparedness, mitigation, response, recovery and remediation procedures for undesirable and disruptive events. The organization should establish documented procedures that detail how the organization will manage a disruptive event and how it will

recover or maintain its activities to a predetermined level, based on management-approved recovery objectives. The procedures should:

a) be based on the risks identified and prioritized in the risk assessment;

b) use the risk assessment to identify the specifics of potential undesirable and disruptive events, including any precursors and warning signs;

c) manage risk based on the outputs of the risk assessment in a systematic and holistic process;

d) combine risk treatment options considering avoidance, elimination, reduction, spreading, transfer and acceptance strategies to provide the optimal solution;

e) include provisions for notification of appropriate authorities and stakeholders.

The organization should establish procedures to recognize when specific dangers are noticeable that necessitate the need for some level of reaction to avoid, prevent, mitigate, or respond to the potential of the undesirable event. A strong programme of detection and avoidance policies and procedures should support this process.

A potential disruptive incident, once recognized, should be immediately reported to the designated authorities, a member of management, or another individual tasked with the responsibility of crisis notification and management internally and with external stakeholders. Specific notification criteria should be established, documented and adhered to.

Problem assessment (an evaluative process of decision making that will determine the nature of the issue to be addressed) and severity assessment (the process of determining the severity of the disruption and any associated consequences) should be made at the outset of an undesirable event. Factors to be considered include the size of the problem, its potential for escalation and the possible impact of the situation on the organization and its stakeholders (e.g. local community and clients).

Prevention can include proactive steps to coordinate with internal and external stakeholders. Organizational culture, operational plans and management objectives should motivate individuals to feel personally responsible for prevention, avoidance, deterrence and detection. Cost-effective mitigation strategies should be employed to prevent or lessen the consequences of potential events. The various resources that would contribute to the mitigation process should be identified.

Preparedness and response plans should be developed around a realistic "worst case scenario," with the understanding that the response can be scaled appropriately to match the actual crisis. Considerations include:

a) people are the most important aspect of any preparedness and response plan;

b) how an organization's human resources are managed will impact the success or failure of incident management;

c) logistical decisions made in advance will impact the success or failure of a good preparedness and response plan;

d) existing funding and insurance policies should be examined.

A.8.8.2 Incident monitoring, reporting and investigations

The organization should establish procedures for incident reporting, documenting any incident involving persons working on its behalf that involves the use of any weapon under any circumstance (except authorized training), any escalation of force, damage to equipment, injury to persons, destruction of property, attacks, criminal acts, traffic accidents, incidents involving other security forces and any other such reporting as otherwise required by the client. The organization should establish procedures for an internal inquiry in order to determine the following:

a) time and location of the incident;

b) identity of any persons involved including their addresses and other contact details;

c) injuries/damage sustained;

d) circumstances leading up to the incident;

e) any measures taken by the organization in response to the incident;

f) causes of internal and external casualties;

g) notification of appropriate authorities;

h) identification of root causes;

i) corrective and preventive actions taken.

Upon completion of the inquiry, the organization should produce in writing an incident report including the above information, copies of which should be provided to appropriate stakeholders (e.g. clients and jurisdictional authorities). Incident reports should provide sufficient information to evaluate the adequacy of the response.

Persons working on behalf of the organization should be aware of the responsibilities and mechanisms for incident reporting, including evidence gathering and preservation. The incident reporting programme should be included in the organization's training programme.

A.8.8.3 Internal and external complaint and grievance procedures

The organization should establish a complaint and grievance procedure whereby any internal or external stakeholder who believes there are potential or actual non-conformances with this International Standard, or violations of international, national and local law, or human rights may file a grievance. The procedure should state that the organization, or persons working on its behalf, may not retaliate against anyone who files a grievance or cooperates in the investigation of a grievance.

Complaint and grievance procedures are not for merely documenting grievances; they should be designed to resolve disputes by identifying root causes, improving accountability, evaluating effectiveness criteria and driving a culture of continual improvement. Once a complaint or grievance has been verified, corrective and preventive actions should be implemented in an expedited fashion.

When developing complaint and grievance procedures, one or more individuals should be designated with the authority to coordinate the efforts to investigate and resolve any complaints that the organization receives alleging any actions that threaten human life, rights, or safety, or are not in conformance with the requirements of this International Standard, or as required by the client. The organization should adopt and publish its grievance procedures providing for prompt and equitable resolution of complaints.

The procedures should include, but are not limited to:

a) mechanisms for submission of the complaint or grievance;

b) information requirements of the submitter, including submission of corroborating information;

c) timeframes for submission, investigations and outcomes;

d) provisions for confidentiality and privacy;

e) hierarchical steps for the resolution process;

f) investigation procedures, both internal and external;

g) maintenance requirements of files and records related to the grievance and investigation;

h) disciplinary actions;

i) steps for resolution of complaint or grievance, including actions to prevent a recurrence;

j) documentation and communication of outcomes;

k) notification to appropriate authorities;

l) evaluation of effectiveness of complaint and grievance procedures.

A.8.8.4 Whistle-blower policy

A whistle-blower is a person working on behalf of the organization who exposes activities and actions not in conformance with this International Standard or inconsistent the organization's legal obligations and voluntary commitments. Whistle-blowers may make their allegations internally or externally (e.g. to regulators and law enforcement agencies, or to groups concerned with the issues). The organization should establish and communicate its whistle-blower policy to appropriate stakeholders.

A.9 Performance evaluation

A.9.1 Monitoring, measurement, analysis and evaluation

A.9.1.1 General

Performance evaluation involves the measurement, monitoring and evaluation of the organization's security operations, legal compliance and human rights performance. The organization should have a systematic approach for measuring and monitoring its security operations key performance indicators on a regular basis. Metrics assure the organizations policy, objectives and targets are achieved, as well as elucidate areas for improvement.

In order to measure and monitor the organization's security operations performance, a set of performance indicators should be developed to measure the management system and its outcomes (including the impacts of its security operations). Measurements can be either quantitative or qualitative, directly related to the risk assessment and security operations objectives and targets. Performance indicators can be management, operational, or economic indicators. Indicators should provide useful information to identify both successes and areas requiring correction or improvement.

The SOMS should provide procedures for defining metrics, collection of data and analysis of data collected. Metrics should be established to monitor and measure the effectiveness of the SOMS and identify areas for improvements to enhance performance to pre-emptively prevent potential undesirable and disruptive events. Knowledge gained from this information can be used to implement corrective and preventive action. Key characteristics are those that the organization needs to consider to determine how it is managing its significant risks, achieving objectives and targets and improving security operations performance.

When necessary to ensure valid results, measuring equipment should be calibrated or verified at specified intervals, or prior to use, against measurement standards traceable to international or national measurement standards. Where no such standards exist, the basis used for calibration should be recorded.

A.9.1.2 Evaluation of compliance

The organization should be able to demonstrate that it has evaluated compliance with the legal and human rights requirements identified, including applicable permits or licenses.

The organization should be able to demonstrate that it has evaluated compliance with the other identified requirements to which it has subscribed.

A.9.1.3 Exercises and testing

Exercising and testing scenarios should be designed using the events identified in the risk assessment. Exercising and testing can serve as an effective training tool and can be used to validate the assumptions and conclusions of the risk assessment.

Exercising ensures that technology resources function as planned, and that persons working on the organizations behalf are adequately trained in their use and operation. Exercising can keep persons working on the organizations behalf effective in their duties, clarify their roles and identify areas for improvement in the SOMS, its plans and its procedures. Exercising can reveal weaknesses in the SOMS that should be corrected. A commitment to exercising lends credibility and authority to the SOMS.

The first step in exercises and testing should be the setting of goals and expectations. A critical goal is to determine whether certain prevention and response processes work and how they can be improved. The organization should use exercises and the documented results of exercises to ensure the effectiveness and readiness of the SOMS – specifically, its security operations plans, team readiness and facilities – to perform and validate its security operations function.

Benefits of exercising and testing include:

a) validation of planning scope, assumptions and strategies;

b) examine and improve competence of persons working on behalf of the organization;

c) capacity testing (e.g. the capacity of a call-in or call-out phone system);

d) increase efficiency and reduce the time necessary for accomplishment of a process (e.g. using repeated drills to shorten response times);

e) awareness and knowledge for internal and external stakeholders about the SOMS and their roles.

The organization should design exercise scenarios to evaluate the security operations plans. An exercise schedule and timeline for periodically exercising the SOMS and its components should be established. Exercising and testing should be realistic, evaluate the capabilities and capacities of security operations management and assure the protection of people and assets involved. The scope and detail of the exercises should mature based on the organization's experience, resources and capabilities. Early tests may include checklists, simple exercises and small components of the SOMS. Examples of increasing maturity of exercises include:

a) Orientation: Introductory, overview, or education session;

b) Table top: Practical or simulated exercise presented in a narrative format;

c) Functional: Walk-through or specialized exercise simulating a scenario as realistically as possible in a controlled environment;

d) Full scale: Live or real-life exercise simulating a real-time, real-life scenario.

There are several roles that exercise participants may fill. All participants should understand their roles in the exercise. The exercise should involve all organizational participants defined by the scope of the exercise; where appropriate, external stakeholders may be included. As part of the exercise, a review should be scheduled with all participants to discuss issues and lessons learned. This information should be documented in a formal exercise report which should be reviewed by top management. Updates should be made to plans and procedures, and corrective and preventive measures expeditiously implemented.

Design of tests and exercise should be evaluated and modified as necessary. They should be dynamic, taking into account changes to the SOMS, personnel turnover, actual incidents and results from previous exercises. Lessons learned from exercises and tests, as well as actual incidents experienced, should be built into future exercises and test planning for the SOMS.

Exercise and test results should be documented and retained as records.

A.9.2 Internal audit

It is essential to conduct internal audits of the SOMS to ensure that the SOMS is achieving its objectives, that it conforms to its planned arrangements, that it has been properly implemented and maintained, and to identify opportunities for improvement. Internal audits of the SOMS should be conducted at planned intervals to determine and provide information to top management on appropriateness and effectiveness of the SOMS, as well as to provide a basis for setting objectives for continual improvement of SOMS performance.

The organization should establish an audit programme (see ISO 19011 for guidance) to direct the planning and conduct of audits, and to identify the audits needed to meet the programme objectives. The programme should be based on the nature of the organization's activities, its risk assessment, the results of past audits and other relevant factors.

An internal audit programme should be based on the full scope of the SOMS; however, each audit need not cover the entire system at once. Audits may be divided into smaller parts, so long as the audit programme ensures that all organizational units, activities and system elements – and the full scope of the SOMS – are audited in the audit programme within the auditing period designated by the organization.

The results of an internal SOMS audit can be provided in the form of a report and used to correct or prevent specific nonconformities and provide input to the conduct of the management review.

Internal audits of the SOMS can be performed by personnel from within the organization or by external persons selected by the organization, working on its behalf. In either case, the persons conducting the audit should be competent and in a position to do so impartially and objectively. In smaller organizations, auditor independence can be demonstrated by an auditor being free from responsibility for the activity being audited.

NOTE If an organization wishes to combine audits of its SOMS with security, resilience, safety or environmental audits, the intent and scope of each need to be clearly defined. Third-party conformity assessment, performed by a body that is independent of the organization, provides confidence to internal and external stakeholders that the requirements of this International Standard are being met. The value of certification is the degree of public confidence and trust that is established by an impartial and competent external assessment.

A.9.3 Management review

Management review provides top management with the opportunity to evaluate the continuing suitability, adequacy and effectiveness of the SOMS. The management review should cover the scope of the SOMS, although not all elements of the SOMS need to be reviewed at once, and the review process may take place over a period of time. The management review will enable top management to address need for changes to key SOMS elements, including:

a) policy;

b) resource allocations;

c) risk appetite and risk acceptance;

d) objectives and targets;

e) security operations strategies.

Review of the implementation and outcomes of the SOMS by top management should be regularly scheduled and evaluated. While ongoing system review is advisable, formal review should be structured, appropriately documented and scheduled on a suitable basis. Persons who are involved in implementing the SOMS and allocating its resources should be involved in the management review. In

addition to the regularly scheduled management system reviews, the following factors can trigger a review and should otherwise be examined once a review is scheduled.

a) Risk assessment: The SOMS should be reviewed every time a risk assessment is completed for the organization. The results of the risk assessment can be used to determine whether the SOMS continues to adequately address the risks facing the organization.

b) Sector/industry, contractual and political trends: Significant changes in sector/industry, contractual and political trends should initiate an SOMS review. General trends and best practices in the sector/industry and in security operations planning techniques can be used for benchmarking purposes.

c) Regulatory requirements: New regulatory requirements may require a review of the SOMS.

d) Event experience: A review should be performed following an undesirable or disruptive event, whether the prevention, mitigation, or response plans were activated or not. If the plans were activated, the review should take into account the history of the plan itself, how it worked, why it was activated, etc. If the plans were not activated, the review should examine why not and whether this was an appropriate decision.

e) Test and exercise results: Based on test and exercise results, the SOMS should be modified as necessary.

Continual improvement and SOMS maintenance should reflect changes in the risks, activities and operation of the organization that will affect the SOMS. The following are examples of procedures, systems, or processes that may affect the SOMS:

a) policy changes;

b) hazards and threat changes;

c) changes to the organization and its business processes;

d) changes in assumptions in risk assessment;

e) personnel changes (employees and contractors) and their contact information;

f) subcontractor and supply chain changes;

g) process and technology changes;

h) systems and application software changes;

i) lessons learned from exercising and testing;

j) lessons learned from external organizations' undesirable and disruptive events;

k) issues discovered during actual invocation of the plan;

l) changes to external environment (new client needs, political changes, relations with local communities, etc.);

m) other items noted during review of the plan and identified during the risk assessment.

A.10 Improvement

A.10.1 Nonconformity and corrective action

The organization should establish effective procedures to ensure that non-fulfilment of a requirement, inadequacies in planning approach, incidents, near misses and weaknesses associated with the SOMS (its plans and procedures) are identified and communicated in a timely manner to prevent further

occurrence of the situation, as well as to identify and address root causes. The procedures should enable ongoing detection, analysis and elimination of actual and potential causes of nonconformities.

An investigation should be conducted of the root cause(s) of any identified nonconformity in order to develop a corrective action plan for immediately addressing the problem to mitigate any consequences, make changes needed to correct the situation and to restore normal operations, and take steps to prevent the problem from recurring by eliminating cause(s). The nature and timing of actions should be appropriate to the scale and nature of the nonconformity and its potential consequences.

Sometimes, a potential problem may be identified, but no actual nonconformity exists. In this case, a preventive action should be taken using a similar approach. Potential problems can be extrapolated from corrective actions for actual nonconformities, identified during the internal SOMS audit process, analysis of industry trends and events, or identified during exercise and testing. Identification of potential nonconformities can also be made part of routine responsibilities of persons aware of the importance of noting and communicating potential or actual problems.

Establishing procedures for addressing actual and potential nonconformities and for taking corrective and preventive actions on an ongoing basis helps to ensure reliability and effectiveness of the SOMS. The procedures should define responsibilities, authority and steps to be taken in planning and carrying out corrective and preventive action. Top management should ensure that corrective and preventive actions have been implemented and that there is systematic follow-up to evaluate their effectiveness.

Corrective and preventive actions that result in changes to the SOMS should be reflected in the documentation, as well as trigger a revisit of the risk assessment related to the changes to the system to evaluate the effect on plans, procedures and training needs. Changes should be communicated to affected stakeholders.

The organization should take action to eliminate the cause of nonconformities associated with the implementation and operation of the SOMS to prevent their recurrence. The documented procedures for corrective action should define requirements for:

a) identifying any nonconformities;

b) determining the causes of nonconformities;

c) evaluating the need for actions to ensure that nonconformities do not recur;

d) determining and implementing the corrective action needed;

e) recording the results of action taken;

f) reviewing the corrective action taken and the results of that action.

A.10.2 Preventive action

The organization should take action to prevent potential nonconformities from occurring. Preventive actions taken should be appropriate to the potential impact of nonconformities.

The documented procedure for preventive action should define requirements for:

a) identifying potential nonconformities and their causes;

b) determining and implementing preventive action needed;

c) recording results of action taken;

d) reviewing preventive action taken;

e) identifying changed risks and ensuring that attention is focused on significantly changed risks;

f) ensuring that all those who need to know are informed of the non-conformity and preventive action put in place;

g) the priority of preventive actions based on results of risk assessments.

A.1 Maturity model for the phased implementation

Implementation of a management system standard can be a daunting task, especially for small to medium sized enterprises. All organizations face the challenge of managing their risks within the bounds of organizational objectives and available resources. Only through the full implementation with conformance to all requirements of this International Standard, ongoing maintenance and continual improvement of the SOMS can an organization reach its ultimate goal of assuring the professionalism of security operations consistent with respect for human rights. Building the SOMS in a phased approach and achieving benchmarks of maturity, provides the organization a link between objectives and its resources.

By using a maturity model for the phased implementation of the SOMS, the organization defines a series of steps designed to help it evaluate where they currently are with regard to security operations and respect for human rights, to set goals for where they want to go, to benchmark where they are relative to those goals, and to plot a business-sensible path to get to full implementation of the SOMS. (ANSI/ASIS PSC.3-2013 provides more information on using a maturity model.)

Annex B
(informative)

General principles

B.1 General

The goal of an SOMS is to manage an organization's security operations in a manner that enhances human safety and security as well as the protection of assets (both tangible and intangible) consistent with respect for international, national and local laws and human rights. This is particularly important in circumstances where governance may be weak or rule of law undermined due to human or naturally caused events. Organizations need to conduct operations – and achieve clients' objectives – by managing risks to all stakeholders, including persons working on its behalf, affected communities and their clients. This is accomplished by integrating legal, social, cultural environmental concerns into business operations and interactions with stakeholders when developing appropriate pre-emptive measures to protect the human and physical assets entrusted to their care. The intent is to minimize the likelihood and consequences of a disruptive or undesirable event by:

— prevention, when possible;

— mitigating the impact of an event;

— effectively and efficiently responding when an event occurs, maintaining an agreed level of performance;

— assuring accountability after the event;

— taking measures to prevent a recurrence.

An SOMS will promote a culture in the organization that ensures security operations consistent with respect for international, national and local laws and human rights.

A consistent agreed upon level of performance is achieved by developing, designing, documenting, deploying and evaluating fit-for-purpose SOMS. The elements of the management system for conducting security operations consistent with respect for human rights are detailed in Clauses 4 to 10 and the annexes of this International Standard. In developing, implementing and improving an SOMS, top management/decision-makers should apply the following general principles.

The organization should integrate all the principles described below into the design and implementation of its SOMS. The goal is to achieve the organization's and client's objectives and protect assets (both tangible and intangible) while assuring human safety and security coupled with respect for human rights. Security operations management will depend on the effectiveness of integrating these principles into the organization's management framework, which drives a security operations culture consistent with respect for human rights throughout all levels of the organization. Use of these principles should establish an environment where information is adequately reported and used as a basis for decision-making and accountability at all relevant organizational levels.

B.2 Outcomes oriented

A management system is more than a set of management processes; it is a tool to achieve desired outcomes. An SOMS is used to achieve the outcome of security operations consistent with respect for human rights and contractual and legal obligations. Key performance indicators (KPIs) are defined to support achievement of objectives. KPIs drive a culture of management by measurement for continual

monitoring and performance improvement. The outcome of any SOMS is the effective management of risk related to:

— security operations and management;

— protection of the client, assets and persons being protected;

— human rights;

— impacted communities;

— security and safety of the security providers;

— reputation and information

B.3 Leadership and vision

Top management (which refers to the person or persons responsible for decision making, that have authorization for the implementation of the decisions) establishes the vision, sets objectives and provides direction for the organization. They promote a culture of ownership within the organization where everyone views respect for human rights and managing the risks of undesirable and disruptive events as part of their contribution to achieving the organization's goals and objectives. Top management demonstrates a commitment to promote a culture of security operations coupled with a respect of international, national and local laws and human rights, and effective leadership in the implementation and maintenance of this International Standard.

B.4 Governance

The assurance of professional security operations is viewed as part of an overall good governance strategy and an enterprise-wide responsibility. Conducting security operations in line with respecting international, national and local laws and human rights is part of the organization's ethos and values. The protection of human life and safety in the course of achieving the mission's objectives is the primary concern of managing the risks of undesirable and disruptive events.

B.5 Needs oriented

Assessing and understanding the organization's assets, needs and expectations is critical to the success of private security operations management. Security operations management needs to be responsive to the needs and expectations of the client while also considering the needs and expectations of other stakeholders – such as affected communities, whose active or passive support is necessary for the success of the organization and its client. Objectives of the organization are linked to internal and external stakeholder needs and expectations. Stakeholder relationships are systematically managed using a balanced approach between the needs of the organization, clients and other stakeholders (such as affected communities).

B.6 Overall organizational risk management strategy

Managing security operations consistent with respect for human rights is part of an organization's overall risk management strategy. Unless risk is managed effectively, organizations cannot maximize opportunities and minimize risk. Risk is the effect of uncertainty on the achievement of objectives, emphasising human safety and security and the protection of assets (both tangible and intangible), while maintaining respect for international, national and local laws and human rights. The risk management process requires a clear understanding of the organization's internal and external contexts to proactively identify opportunities and minimize risk. Assessing and understanding an organization's acceptable level of risk is critical for the organization to develop a pre-emptive and effective risk management strategy that matches the needs and expectations of its internal and external stakeholders within the context of the operating environment's level of risk.

B.7 Systems approach

An SOMS requires a multi-dimensional, iterative approach. Identifying, understanding and managing interrelated processes and elements contribute to the organization's effective and efficient control of its risks. The systems approach examines the linkages and interactions between the elements that compose the entirety of the system. Component parts of a system can best be understood in the context of their interrelationships,rather than in isolation, and need to be treated as a whole.

B.8 Adaptability and flexibility

Most organizations, especially those conducting or contracting security operations, operate in situations where the internal and external environments are subject to change. Organizations need to conduct on-going operational monitoring to identify changes and implement effective change control strategies. Organizations need to be adaptable: able and willing to evolve – constantly adapting to reflect the changing operating environment. The SOMS should be seen as a management framework, rather than a set of activities. As missions, budgets, priorities and staff continue to change, the structure of the framework will remain predictable when particular applications change.

B.9 Managing uncertainty

Security operations management is not always based on predictable threats and quantifiable risks. Organizations conducting or contracting security operations often work in circumstances where governance may be weak or the rule of law undermined due to human or naturally caused events. Estimates and assumptions need to be made in analysing the likelihood and consequences of threats, both known and unknown, and the vulnerability of the organization and stakeholders within a changing environment. The management of risks of undesirable and disruptive events explicitly takes account of uncertainty, the nature of that uncertainty and how it should be addressed.

B.10 Cultural change and communication

It is essential for top management to establish a well-defined strategy, communications, training and awareness programmes to ensure all levels of management and employees understand the goals of the management system. The SOMS supports cultural and perceptual change in the organization, thereby protecting the image and reputation of the organization and its clients. The SOMS needs to be fully understood and supported at the top level in the enterprise and communicated to all persons who work on behalf of the organization as part of the core culture of the organization.

B.11 Factual basis for decision making

Assessing managing the business and risk-related issues of security operations drives decision making and dictates the actions that will be taken based on factual analysis – balanced with experience and accepted industry best practices. The SOMS increases the ability to review, challenge and change opinions and decisions, enhances problem-solving capacity, increases the ability to demonstrate effectiveness of past decisions through reference to factual records, and ensures that data and information are accurate, reliable and timely – in line with company policy.

B.12 Continual improvement

Managers improve their SOMS through the monitoring, measurement, review and subsequent modification of SOMS processes, procedures, capabilities and information within a continual improvement cycle. Formal, documented reviews are conducted regularly. The findings of such reviews should be considered by top management and acted upon as appropriate.

Annex C
(informative)

Getting started – Gap analysis

An organization should establish its current position with regard to managing potential risk scenarios by means of a gap analysis. A gap analysis will enable the organization to compare its actual performance with the potential performance needed to meet its objectives. The analysis should consider the organization's risks (including potential impacts) as a basis for establishing the SOMS.

The gap analysis should cover five key areas:

a) identification of risks, including those associated with operating conditions, emergency situations, accidents and potential undesirable and disruptive events;

b) human rights risk analysis to determine the severity of the impacts of the organization's security operations and to identify opportunities for improvement;

c) identification of applicable legal requirements and other requirements to which the organization subscribes;

d) evaluation of existing risk management practices and procedures, including those associated with subcontracting activities;

e) evaluation of previous emergency situations and accidents, as well as previous measures taken to prevent and respond to undesirable and disruptive events.

In all cases, consideration should be given to operations and functions within the organization, its relationships with its relevant stakeholders, and to potentially disruptive and emergency conditions. Tools and methods for undertaking a gap analysis may include checklists, conducting interviews, direct inspection and measurement, or results of previous audits or other reviews, depending on the nature of the activities.

Annex D
(informative)

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.

The management systems approach considers how local policies, culture, actions, or changes influence the state of the organization as a whole and its environment. The component parts of a system can best be understood in the context of relationships with each other, rather than in isolation. Therefore, a management system examines the linkages and interactions between the elements that compose the entirety of the system. The management systems approach systematically defines activities necessary to obtain desired results and establishes clear responsibility and accountability for managing key activities. This management systems standard provides requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's management system for security operations consistent with respect for human rights. An organization needs to identify and manage many activities in order to function effectively. Any activity which enables the transformation of inputs into outputs, that uses resources and is formally managed, can be considered to be a process. Often the output from one process directly forms the input to the next process.

The management systems approach for security operations management presented in this International Standard encourages its users to emphasise the importance of:

a) understanding an organization's risk, security and human rights protection requirements;

b) defining outcomes for security operations consistent with respect for human rights, contractual and legal obligations;

c) establishing a policy and objectives, processes, systems and culture to manage risks;

d) implementing and operating controls to manage an organization's risk and security requirements, and respect for human rights;

e) monitoring and reviewing the performance and effectiveness of the SOMS, administratively and operationally;

f) continual improvement based on objective measurement.

This International Standard adopts the "Plan-Do-Check-Act" (PDCA) model, which is applied to structure the security operations processes. Figure D.1 illustrates how an SOMS takes as input the security operations management requirements and expectations of stakeholders and through the necessary actions and processes produces security operations and risk management outcomes that meet those requirements and expectations. Figure D.1 also illustrates the links in the processes presented in this International Standard.

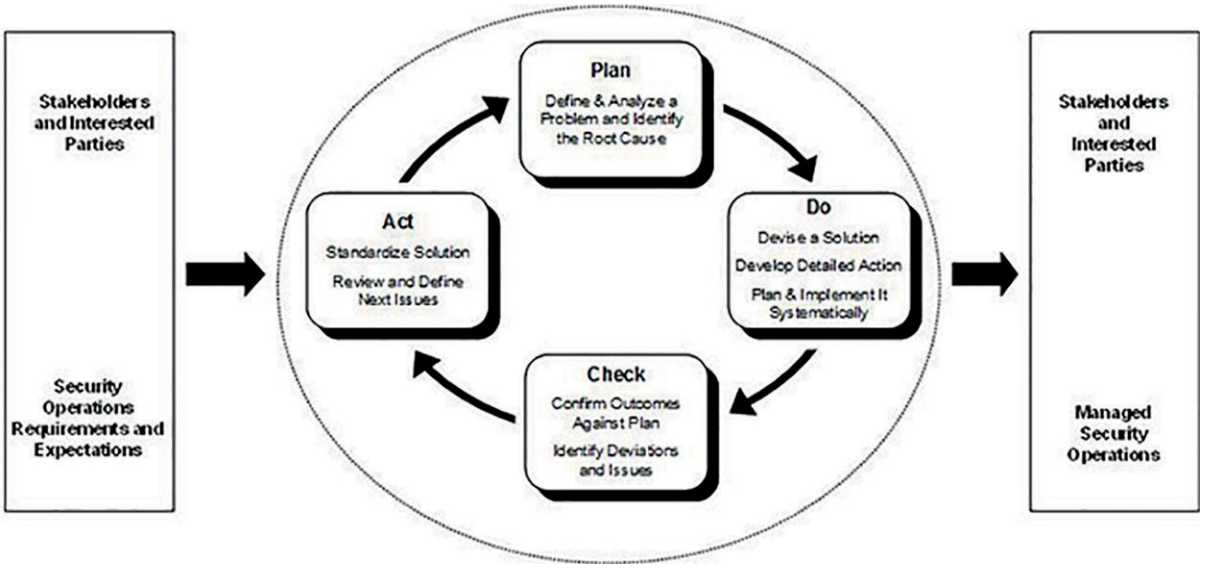


Figure D.1 — Plan-Do-Check-Act model

The PDCA cycle can be briefly described as follows:

— Plan (establish the management system): Establish management system policy, objectives, processes and procedures relevant to managing operations and improving risk management to deliver results in accordance with an organization's overall policies and objectives.

— Do (implement and operate the management system): Implement and operate the management system policy, controls, processes and procedures.

— Check (monitor and review the management system): Assess and measure process performance against management system policy, objectives and practical experience and report the results to management for review.

— Act (maintain and improve the management system): Take corrective and preventive actions, based on the results of the internal management system audit and management review, to achieve continual improvement of the management system.

The PDCA model is a clear, systematic and documented approach to:

a) set measurable objectives and targets;

b) monitor, measure and evaluate progress;

c) identify, prevent or remedy problems as they occur;

d) assess competence requirements and train persons working on the organizations behalf;

e) provide top management with a feedback loop to assess progress and make appropriate changes to the management system.

Furthermore, it contributes to information management within the organization, thereby improving operational efficiency.

This International Standard is designed so that it can be integrated with quality, safety, environmental, information security, resilience, risk, security and other management systems within an organization. A suitably designed management system can thus satisfy the requirements of all these standards. Organizations that have adopted a management systems approach (e.g. according to ISO 9001, ISO 14001, ISO/IEC 27001, ISO 28000, OHSAS 18001, ANSI/ASIS PSC.1-2012, ANSI/ASIS SPC.1-2009) may be able to use their existing management system as a foundation for the SOMS as prescribed in this

International Standard. Conformance with this International Standard can be verified by an auditing process that is compatible and consistent with the methodology of ISO/IEC 17021-1.

Annex E
(informative)

Qualifiers to application

The adoption and implementation of a range of security operations management techniques in a systematic manner can contribute to optimal outcomes for all stakeholders and affected parties. However, adoption of this International Standard will not by itself guarantee optimal security operations outcomes. In order to achieve its objectives, the SOMS should incorporate the best available practices, techniques and technologies, where appropriate and where economically viable. The cost- effectiveness of such practices, techniques and technologies should be taken fully into account.

This International Standard does not establish absolute requirements for security operations performance beyond commitments in the organization's policy to:

a) comply with applicable legal requirements and with other requirements to which the organization subscribes;

b) support prevention of undesirable and disruptive events and risk minimization;

c) promote continual improvement.

The main body of this International Standard contains generic criteria that may be objectively audited. Guidance on supporting security operations management techniques is contained in the other annexes.

For organizations that so wish, an external or internal auditing process may verify compliance of their SOMS to this International Standard. Verification may be by an acceptable first-, second-, or third-party mechanism. Verification does not require third-party certification.

This International Standard does not include requirements specific to other management systems, such as those for quality, occupational health and safety, or resilience management – though its elements can be aligned or integrated with those of other management systems. It is possible for an organization to adapt its existing management system(s) in order to establish an SOMS that conforms to the criteria of this International Standard. However, the application of various elements of the management system might differ depending on the intended purpose and the stakeholders involved.

The level of detail and complexity of the SOMS, the extent of documentation and the resources devoted to it will be dependent on a number of factors, such as the scope of the system, the size of an organization and the nature of its activities, products, services and supply chain. This may be the case in particular for small and medium-sized enterprises.

This International Standard provides a common set of criteria for security operations management programmes. Terminology used in this International Standard emphasises commonality of concepts, while acknowledging nuances in term usage in the various disciplines. For consistency with ISO 31000, risk assessment is the process of risk identification, analysis and evaluation.

Bibliography

[1] ISO 9000:2015, *Quality management systems — Fundamentals and vocabulary*

[2] ISO 9001, *Quality management systems — Requirements*

[3] ISO 14001, *Environmental management systems — Requirements with guidance for use*

[4] ISO/IEC 17021-1, *Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 1: Requirements*

[5] ISO 19011:2011, *Guidelines for auditing management systems*

[6] ISO/IEC 27000:2014, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

[7] ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*

[8] ISO/IEC 27035, *Information technology — Security techniques — Information security incident management*

[9] ISO 28000, *Specification for security management systems for the supply chain*

[10] ISO 31000, *Risk management — Principles and guidelines*

[11] OHSAS 18001, *Occupational health and safety management*

[12] ASIS International (2008), *ASIS International glossary of security terms*. [Online]. Available at: < https://www.asisonline.org/Membership/Library/Security-Glossary/Pages/Security-Glossary-A.aspx >

[13] ASIS International[4] (2012), ANSI/ASIS PSC.1-2012, *Management Systems for Quality of Private Security Company Operations – Requirements with Guidance Standard*

[14] ASIS International (2012), ANSI/ASIS PSC.2-2012, *Conformity Assessment and Auditing Management Systems for Quality of Private Security Company Operations Standard*

[15] ASIS International (2013), ANSI/ASIS PSC.3-2013, *Maturity Model for the Phased Implementation of a Quality Assurance Management System for Private Security Service Providers*

[16] ASIS International (2013), ANSI/ASIS PSC.4-2013, *Quality Assurance and Security Management for Private Security Company's Operating at Sea – Guidance*

[17] ASIS International (2009), ANSI/ASIS SPC.1-2009, *Organizational Resilience: Security Preparedness, and Continuity Management Systems – Requirements with Guidance for Use*

[18] ASIS International (2012), ANSI/ASIS SPC.4-2012, *Maturity Model for the Phased Implementation of the Organizational Resilience Management System*

[19] *Convention Relative to the Protection of Civilian Persons in Time of War* (Geneva Convention IV), August 12, 1949; < http://www.icrc.org/ihl.nsf/INTRO/380 >

[20] *Convention Respecting the Laws and Customs of War on Land* (Hague IV); October 18, 1907; < http://avalon.law.yale.edu/20th_century/hague04.asp >

[21] International Committee of the Red Cross, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law*, Geneva, ICRC, May 2009

4) ASIS documents are available at < http://www.asisonline.org >.

[22] Parks W.H. Evolution of Policy and Law Concerning the Role of Civilians and Civilian Contractors Accompanying the Armed Forces, Washington, DC, (c). Hays Parks, W., 2005

[23] *Protocol Additional to the Geneva Conventions of 12 August* 1949, *and relating to the Protection of Victims of Non-International Armed Conflicts* (Protocol II), 8 June 1977, < http://www.icrc.org/ihl.nsf/INTRO/475?OpenDocument >

[24] United Nations. *Basic Principles on the Use of Force and Firearms by Law Enforcement Officials*, 1990, < http://www.ohchr.org/EN/ProfessionalInterest/Pages/UseOfForceAndFirearms.aspx >

[25] United Nations. *The Convention against Torture and Other Cruel, Inhuman or Other Degrading Treatment of Punishment* (CAT) 1984. < http://www2.ohchr.org >

[26] United Nations. *The Convention of the Elimination of All Forms of Discrimination against Women* (CEDAW) 1979, < http://www.un.org >

[27] United Nations. *The Convention on the Prevention and Punishment of the Crime ofGenocide* 1948, < http://www.un.org >

[28] United Nations. *The Convention on the Rights of the Child* (CRC) 1989, <http://www2.ohchr.org>

[29] United Nations. *Global Compact Principles*, < http://www.unglobalcompact.org/AboutTheGC/TheTenPrinciples/index.html>

[30] United Nations. *ILO Declaration on Fundamental Principles and Rights at Work.* International Labour Conference, Eighty-sixth Session, Geneva, 18 June 1998 (Annex revised 15 June 2010), < http://www.ilo.org/declaration/thedeclaration/textdeclaration/lang--en/index.htm >

[31] United Nations. *The International Covenant on Civil and Political Rights* (ICCPR) 1966, < http://www2.ohchr.org >

[32] United Nations. *The International Covenant on Economic, Social and Cultural Rights* (ICESCR) 1966, < http://www2.ohchr.org >

[33] United Nations. *The International Convention on the Elimination of All Forms of Racial Discrimination* (ICERD) 1966, < http://www2.ohchr.org>

[34] United Nations. *The Universal Declaration of Human Rights* 1948, < http://www.un.org >

[35] United Nations. *Protect, Respect, and Remedy: a Framework for Business and Human Rights* UN A/HRC/8/5 7 April 2008, < http://www.reports-and-materials.org/Ruggie-repor t-7- Apr-2008.pdf >

[36] U.S. Department of Defense, Department of Defense Directive 5210.56, *Carrying of Firearms and the Use of Force by DoD Personnel Engaged in Security, Law and Order, or Counterintelligence Activities*, Washington DC, USGPO, 1 April 2011

[37] *Voluntary Principles on Security and Human Rights*, < http:// www.voluntaryprinciples.org/files/voluntary_principles_english.pdf >

ICS 03.080.20; 13.310
Price based on 98 pages

This page deliberately left blank

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

bsi.

...making excellence a habit.™