国际标准

ISO 18788 标准

第一版2015年9月15日

私人保安业务管理制度-使用指南要求

私人安全运营管理系统—使用要求与指南

参考编号ISO 18788：2015(E)

受版权保护的文档

ISO版权办公室
Ch. de Blandonnet 8?邮编：401
瑞士日内瓦CH-1214 Vernier
电话：+41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

目录

前言

国际标准化组织（ISO）是全球各国标准机构(ISO成员机构）的联合体。国际标准的准备工作通常由ISO技术委员会承担。每个对已成立技术委员会的主题感兴趣的成员机构都有权派代表参与该委员会的工作。国际组织，无论是政府还是非政府机构，在与ISO联络的情况下，也会参与这项工作。ISO在所有电工标准化事务上与国际电工委员会（IEC）密切合作。

用于编制本文件以及进一步维护该文件的程序已在ISO/IEC指令第1部分中描述。特别是，不同类型的ISO文件所需的不同审批标准应予以注意。本文件是根据ISO/IEC指令第2部分（见www.iso.org/directives)的编辑规则起草的。

请注意，本文件的一些要素可能成为专利权的主题。ISO不负责识别任何或所有此类专利权。在文件开发过程中识别的任何专利权的详细信息将出现在引言和/或ISO收到的专利声明列表中（参见www.iso.org/patents)。

本文件中使用的任何商品名称都是为了方便用户而提供的信息，不构成认可。

有关与符合性评估相关的ISO特定术语和表达的含义的解释，以及关于ISO在技术性贸易壁垒（TBT）方面遵守世界贸易组织（WTO）原则的信息，请参见以下URL：<?1>.html。

负责本文件的委员会是ISO/TC 292安全和弹性技术委员会。

介绍

0.1 将军

本国际标准规定了进行或委托安全运营的组织所需的要求，并提供了指导。它为有效开展安全运营提供了一个业务和风险管理框架。该标准特别适用于在治理可能薄弱或因人为或自然灾害导致法治受到破坏的情况下运营的任何组织。采用计划-执行-检查-行动的方法，本国际标准为进行或委托安全运营的组织提供了一种手段，以证明：

a) 具备充分的业务和风险管理能力，以满足客户和其他利益相关者的专业要求；

b) 评估和管理其活动对当地社区的影响；

c) 对法律负责和尊重人权；

d) 与组织自愿承诺的一致性。

注1：本国际标准不打算在这些特定情况之外对一般防护服务造成额外负担。

本国际标准借鉴了以下文件的相关原则、法律义务、自愿承诺和良好实践的规定，并提供了一种证明符合这些规定的机制：

-蒙特勒关于相关国际法律义务和各国良好做法的文件

武装冲突期间私营军事和安保公司业务（2008年9月）；国际私营保安服务提供者行为守则（ICoC）（2010年11月）；

-《工商业与人权指导原则》；实施联合国“保护、尊重和补救”框架（2011年）。

注2：国际行为准则反映了1）《蒙特勒文件》的法律义务和良好实践（包括详细说明适用于安全提供者的权利法和人道主义法的规定），以及2）“保护、尊重和补救”框架的相关原则，这些原则在《工商企业与人权指导原则》中得到了具体化。

注3虽然《蒙特勒文件》是专门针对国家和武装冲突，但它对类似情况和其他实体也有指导意义。

私人安保行动在保护参与救援、恢复和重建工作的国家和非国家客户；商业运营；发展活动；外交；以及军事活动方面发挥着重要作用。本国际标准适用于任何类型组织进行或承包安保业务的情况，特别是在治理可能薄弱或因人为或自然灾害导致法治受到破坏的环境中。组织需与合法客户和国家行为体密切协调，采用并实施必要的标准，以确保遵守人权和基本自由，从而保护生命和财产，并防止不当、非法和过度的行为。这意味着从事安保业务的组织在使用战术、技术、程序和设备，包括武器时，应以实现操作和风险管理目标的方式进行管理。本国际标准的目的是改进和证明一致和可预测的安全操作，维护其客户的安全和安保，在一个旨在确保尊重人权、国家和国际法律以及基本自由的框架内。

注4：为了本国际标准的目的，国家法律可以包括组织所在国、其人员所在国、运营所在国和客户所在国的法律。

本国际标准以国际人权法和国际人道主义法（IHL）中的原则为基础。它提供了可审计的标准和指导，支持《蒙特勒文件》关于武装冲突期间私营军事和安保公司运营相关的国际法律义务和良好实践的目标。
17 *2008年9月；国际私人保安服务提供者行为守则（ICoC）*
9 *2010年11月；《工商企业和人权指导原则》；《实施联合国“保护、尊重和补救”框架》2011。*

本国际标准为组织及其客户提供了实施《蒙特勒文件》中的法律义务和推荐良好实践的手段，并提供可证明的承诺、合规性和问责制，以尊重《国际商业行为准则》中概述的原则，以及其他与人权和自愿承诺相关的国际文件，如《工商企业与人权指导原则》；《联合国“保护、尊重和补救”框架2011》和《安全与人权自愿原则（2000）》。

鉴于开展和订约执行安保业务的组织已成为支持和平、稳定、发展和商业努力的重要因素，而社会机构的能力已因人为和自然造成的破坏性事件而不堪重负，这些组织的业务面临一定的风险。挑战在于如何在保护内部和外部利益相关者，包括客户和受影响社区的安全、安保和人权的前提下，以成本效益的方式管理风险，同时满足组织的战略和运营目标。组织需要以尊重人权和法律的方式开展业务并提供服务。因此，他们及其客户有义务进行尽职调查，识别风险，预防事件发生，减轻和补救事件后果，在事件发生时报告，并采取纠正和预防措施以防止再次发生。本国际标准为客户提供了一个基础，以便区分哪些组织能够按照与利益相关者需求和权利相一致的最高专业标准提供服务。

保护有形资产和无形资产是任何类型组织（公共、私人或非营利）生存、盈利和可持续发展的关键任务。这不仅限于保护物理、人力和信息资产；还包括保护公司及其客户的形象和声誉。保护资产需要战略思维、问题解决、流程管理和实施与组织运营及其风险相适应的计划和举措的能力相结合。

实施这一国际标准成功的核心在于将蒙特勒文件和ICoC的价值观融入组织的文化和活动范围中。将这些原则整合到整个企业的管理中，需要高层管理团队长期致力于文化变革，包括领导力、时间、关注和资源——无论是资金还是物质上的。通过采用这一国际标准，组织可以展示其将蒙特勒文件和ICoC的原则融入管理体系及日常运营的决心。本国际标准旨在与组织内的其他管理系统（例如：质量、安全、组织弹性、环境、信息安全和风险标准）。一个设计得当的管理系统可以满足所有这些标准的要求。

在本国际标准中，使用以下语言形式（更多细节可参见ISO/IEC指令第2部分）：

— “shall”表示可稽查要求：用于表示严格遵循的要求，以符合文件要求，不允许偏离；

— “应”表示建议：用于表明在几种可能性中，某一种被推荐为特别合适，但不提及或排除其他可能性，或者某种行动方案更受青睐但并非强制要求，或者（在否定形式中）某种可能性或行动方案虽不被推荐但并未禁止；

— “may”表示许可：用于指示在文档范围内允许的行动；

— “ can ”表示一种可能性或能力：用于表示可能性和能力的陈述，无论是物质的、物理的还是因果的。

标记为“ 注释 ”的信息用于指导理解或澄清相关要求。

除非另有说明，列表中列出的项目并非详尽无遗，且列表顺序并不指定任何顺序或优先级。本国际标准的通用性质允许组织根据其特定的操作条件和情况，增加额外项目并指定顺序或优先级。

0.2 人权保护

虽然国家及其实体需要尊重、维护和保护人权，但社会各阶层（公共、私营和非营利部门）都有共同的责任，以尊重人权和基本自由的方式行事，不对其产生负面影响（见A.2条）。

开展和签订安全业务的客户和组织有共同的责任，制定政策和控制措施，确保符合《蒙特勒文件》和《国际行为准则》的原则。通过实施本国际标准，组织可以：

a) 建立和维持透明的治理和管理框架，以阻止、发现、监测、处理和防止对人权和基本自由产生不利影响的事件的发生和再次发生；

b) 根据适用的国际、国家和地方法律法规进行识别和操作；

c) 进行与安全、安保和人权风险相关的全面内部和外部风险评估；

d) 实施支持法治、尊重利益相关者人权、保护组织及其客户利益并提供专业服务的风险控制措施；

e) 确保根据已确定的风险实施和管理适当和充分的操作控制，以提高职业健康和安全以及代表组织工作的人员的福利；

f) 与公共和私人利益相关者有效沟通和协商；

g) 对代表本组织工作的人员进行有效的甄选和培训；

h) 确保使用武力是合理必要的、相称的和合法的；

i) 对所提供的服务和目标的实现情况进行业绩评估；

j) 制定和实施报告和调查违反国际法、地方法律或人权的指控以及减轻和补救不良或破坏性事件后果的制度。

0.3 管理体系方法

管理系统方法鼓励组织分析自身及利益相关者的需求，并定义有助于成功的流程。它为制定政策和目标、建立实现预期结果的程序以及衡量和监控目标与成果的达成提供了基础。管理系统为持续改进提供了框架，以提高提升安全运营专业性的可能性，同时确保人权和基本自由得到保护。这不仅增强了组织及其客户对其管理合同、安全和法律义务的信心，也体现了对人权的尊重。关于管理系统标准的更多信息，请参见附录D。

图1说明了本国际标准中使用的管理系统方法。

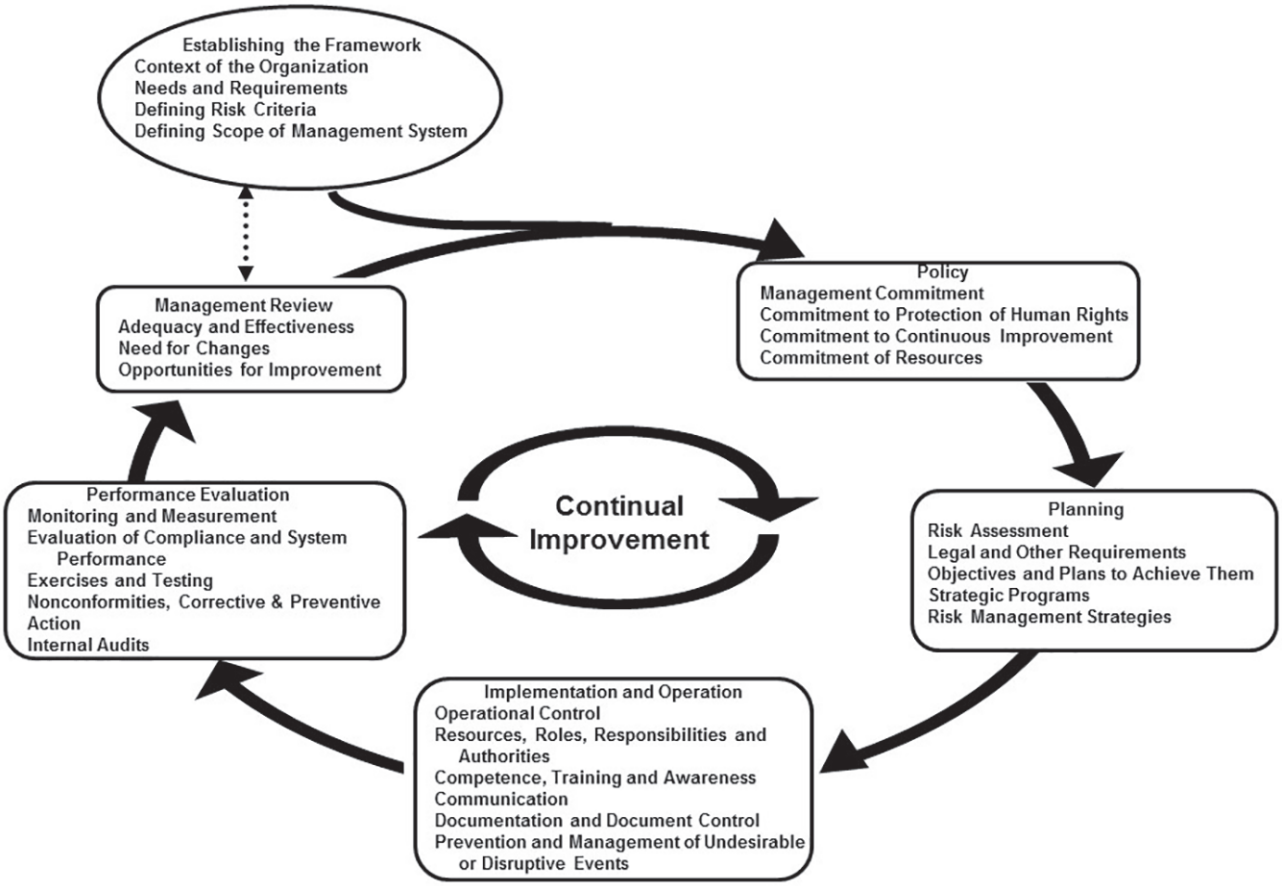


图1-安全运营管理系统（SOMS）流程图

私人保安业务管理制度-使用指南要求

1 范围

本国际标准提供了一个框架，用于建立、实施、运行、监控、审查、维护和改进安全操作的管理。

它提供了安全运营管理系统（SOMS）的原则和要求。本国际标准为开展或承包安全运营及相关活动和职能的组织提供业务和风险管理框架，同时证明：

a) 开展专业安保业务，满足客户和其他利益相关者的要求；

b) 对法律负责和尊重人权；

c) 与它所签署的自愿承诺保持一致。

本国际标准还为组织和使用安全服务的人员提供了一种方式，以证明其对相关法律义务的承诺，以及对《蒙特勒文件》中关于武装冲突期间私营军事和安保公司运营相关的国际法律义务和良好实践的规定的遵守，同时符合《国际私营保安服务提供商行为准则》（ICoC）中概述的原则和承诺。本国际标准特别针对在治理可能薄弱、法治因人为或自然灾害而受到破坏的情况下运营的任何组织。

注1：本国际标准不打算在这些特定情况之外对一般防护服务造成额外负担。

适用法律可以包括各种法律，包括但不限于国家、地区、国际或习惯法。本国际标准的使用者有责任确定适用法律并遵守。本国际标准未提供任何关于适用法律、法律冲突或其中提及的法律、法规、条约或文件的解释方面的建议或指导。

本国际标准适用于需要以下内容的任何组织：

a) 建立、实施、维护和改进SOMS；

b) 评估其是否符合其声明的安全运营管理政策；

c) 证明其持续提供满足客户需求并符合适用的国际、国家和地方法律及人权要求的服务的能力。

本国际标准的通用原则和要求旨在融入基于计划-执行-检查-行动（PDCA）模型的任何组织的综合管理体系中；并非旨在推广适用于所有行业所有组织的统一方法。安全运营计划、程序和实践的设计与实施应考虑

考虑每个组织的特殊要求：其目标、环境、文化、结构、资源、运营、流程、产品和服务。

注2：为了与公共和私营组织遵守所有适用法律并尊重人权的目标保持一致，客户在聘请私人保安服务时应参考本国际标准。组织应使用本国际标准的管理体系原则和要求来开展自身的尽职调查和服务管理，并构建其合同签订和合同管理流程，以支持符合本国际标准。

2 规范性引用文件

下列文件全部或部分地在本文件中作为规范性引用文件，对于其应用而言不可或缺。对于有日期的引用文件，仅适用所引用的版本。对于没有日期的引用文件，适用所引用文件的最新版本（包括任何修正案）。

ISO指南73：2009，风险管理-词汇

蒙特勒关于武装冲突期间私营军事和安保公司运作相关的国际法律义务和良好做法的文件（2008年9月）1)

《私营保安服务提供商国际行为准则》（ICoC）（2010年11月）2)

《工商业与人权指导原则》；《联合国“保护、尊重和补救”框架》20113)

3 术语和定义

为本文件的目的，ISO指南73：2009中给出的术语和定义以及以下内容适用。

3.1
资产
对组织具有有形或无形价值的任何东西（3.34）

条目注释1：有形资产包括人力（在本国际标准中被视为最有价值的）、实物和环境资产。

注2：无形资产包括信息、品牌和声誉。

3.2
审计
获取审计证据并客观评价以确定满足审计标准程度的系统、独立和有文件记录的过程（3.43）

条目注释1：审计可以是内部审计（第一方）或外部审计（第二方或第三方），也可以是综合审计（结合两个或多个学科）。

条目注释2：内部审计由组织（3.34）本身或其代表的外部方进行。

注3：条目中的“审计证据”和“审计准则”在ISO 19011中定义。

3.3
审计员
进行审计的人员（3.2）

[来源：ISO 19011：2011,3.8]

1) 可从以下网址获得：http://www.un.org/ga/search/view_doc.asp？symbol=A/63/467

2) 可从以下网址获得：http://icoca.ch/

3) 可从以下网址获得：http://www.ohchr.org/documents/issues/business/A.HRC.17.31.pdf

3.4
客户
雇佣、曾经雇佣或打算雇佣一个组织（3.34）代表其执行安全行动（3.63），包括在适当情况下，该组织与另一家公司或当地部队签订分包合同

示例消费者；承包商；最终用户；零售商；受益人；购买者。

条目注释1：客户可以是内部（例如，其他部门）或外部的。

3.5
能力
将知识和技能应用于实现预期结果的能力

3.6
沟通和协商
组织（3.34）为提供、共享或获取信息以及与利益相关者（3.24）和其他人就风险管理（3.50）进行对话而开展的持续和迭代过程（3.43）

条目注释1：信息可涉及风险和安保业务管理（3.64）的管理的存在、性质、形式、可能性（3.27）、严重性、评估、可接受性、处理或其他方面。

条目注释2：协商是组织与其利益相关者或其他人之间在做出决定或确定该问题的方向之前，就某一问题进行的双向知情沟通。协商是：

-通过影响力而非权力影响决策的过程；以及-决策的输入，而非共同决

策。

[来源：ISO指南73：2009,3.2.1，修改]

3.7
社会
相关组织（3.34）群体、具有共同利益的个人和团体

条目注释1：受影响社区是指受提供安保服务、项目或行动影响的人群和相关组织。

3.8
遵从
满足要求（3.45）

3.9
持续改进
经常性活动以提高业绩（3.36）

3.10
结果
影响目标（3.33）的事件结局（3.19）

条目注释1：事件可能导致一系列的后果。

条目注释2：结果可以是确定的或不确定的，可以对目标产生积极或消极的影响。

条目注释3：后果可以用定性或定量的方式表达。

条目注释4：初始后果可能通过一个事件引发一系列事件的累积效应而升级。

条目注释5：后果根据影响的大小或严重程度进行分级。

[来源：ISO指南73：2009,3.6.1.3，修改]

3.11
批改
消除检测到的不合格项的措施（3.32）

3.12
校正动作
消除不合格的原因（3.32）并防止再次发生

3.13
危害度分析
流程（3.43）旨在系统地识别和评估组织、（3.34）资产（3.1），依据其使命或职能的重要性、面临风险的群体（3.50）或对组织满足期望的能力造成不利影响（3.75）或破坏性事件（3.15）的重要性

3.14
关键控制点
CCP
可应用控制措施并可防止、消除或降低威胁或危害至可接受水平的点、步骤或过程（3.43）

3.15
破坏性事件
发生或改变，中断计划的活动、操作或功能，无论是预期的还是非预期的

3.16
记录的信息
组织需要控制和维护的信息（3.34）及其所包含的媒介

条目注释1：记录的信息可以是任何格式和媒体，来自任何来源。

条目注释2：记录的信息可参考：

-管理体系（3.29），包括相关过程（3.43）；

——为组织运营而创建的信息（文档）；

-成果证明（记录（3.44））。

3.17
有效
计划活动的实现程度和计划结果的达成

3.18
练习
评估安保业务管理（3.64）方案、演练团队成员和工作人员的角色以及测试组织的（3.34）系统（例如技术、报告协议、行政管理），以证明安保业务管理、能力和能力（3.5）

条目注释1：训练包括为组织工作人员进行适当反应的训练和调节活动，目的是实现最佳表现（3.36）。

3.19
事件
特定情况的发生或变化

条目注释1：事件的性质、可能性（3.27）和后果（3.10）无法完全知晓。

条目注释2：事件可以是一个或多个事件，并且可以有多个原因。

条目注释3：可确定与事件相关的可能性。

条目注释4：事件可以由一个或多个情况的不发生组成。

注释5：有时，具有后果的事件被称为“ 事故（3.21） ”。[来源：ISO指南

73：2009,3.5.1.3，修改]

3.20
人权风险分析
人力资源研究组织
（3.43）程序，以查明、分析、评价和记录与人权有关的风险（3.50）及其影响，以便管理风险并减轻或防止不利的人权影响和违法行为

注1：HRRA是组织（3.34）要求（3.45）的一部分，即开展人权尽职调查，以识别、预防、减轻和说明如何处理对人权的影响。

注释2：HRRA以相关国际人权原则和公约为框架，是组织整体风险评估（3.54）的基本组成部分。

条目注释3：HRRA包括对组织通过其安全行动（3.63）可能造成或促成的实际和潜在人权影响的严重程度的分析，或者可能通过其业务关系与组织的行动、项目或服务直接联系起来的严重程度的分析。HRRA进程应包括考虑业务环境，利用必要的人权专业知识，并与那些权利可能受到威胁的利益攸关方（3.24）进行直接、有意义的接触。

条目注释4：对人权受到不利影响的后果（3.10）进行分析，根据影响的严重程度衡量和确定优先次序。

条目注释5：应定期开展人权风险评估，同时认识到人权风险可能会随时间而变化。

条目注释6：人权风险评估的复杂程度将因组织规模、严重侵犯人权的风险以及其业务性质和背景而有所不同。

注7：HRRA有时被称为“ 人权风险评估 ”、“ 人权影响评估 ”或“ 人权风险和影响评估 ”。本国际标准中使用的语言与ISO标准中使用的风险词汇一致。

3.21
事件
事件（3.19）具有后果（3.10），能够导致生命损失、资产损害（3.1）或对内部或外部利益相关者的人权和基本自由产生负面影响（3.24）

3.22
固有危险财产
如果被未经授权的个人使用，会造成死亡或严重身体伤害的紧迫威胁的财产

致命武器、弹药、炸药、化学剂、生物剂和毒素、核材料或放射性材料。

3.23
正直
确保资产的准确性和完整性（3.1）

[来源：ISO/IEC 27000：2014,2.40，修改]

3.24
有关的当事人
股东
能够影响、受决策或活动影响或认为自己受到决策或活动影响的个人或组织（3.34）

条目注释1：决策者可以是利益相关者。

条目注释2：受影响社区和当地居民被视为外部利益相关者。

注3：本标准中“利益相关者”一词的使用与安全操作（3.63）中的用法一致。

3.25
关键绩效指标
关键业绩指标
组织（3.34）用来衡量或比较绩效（3.36）以满足其战略和运营目标（3.33）的可量化措施

3.26
非致命性武力
所使用的武力程度，较少可能导致死亡或严重伤害，以克服暴力冲突并适当应对遇到的抵抗水平

3.27
似然
发生某事的机率

条目注1：在风险管理(3.58)术语中，“可能性”一词用来指某事发生的几率，无论其定义、测量或确定是客观的还是主观的，定性的还是定量的，并用一般术语或数学方法（如概率或在给定时间段内的频率）来描述。

注释2：英文术语“likelihood”在某些语言中没有直接对应的词汇；相反，通常使用“probability”的等效词。然而，在英语中，“probability”常被狭义地解释为一个数学术语。因此，在风险管理术语中，“likelihood”被使用时，其意图是希望它能像“probability”在许多其他语言中的广泛解释一样。

[来源：ISO指南73：2009,3.6.1.1]

3.28
管理计划
明确且有文件记录的行动计划，通常涵盖实施事件（3.19）管理过程（3.43）所需的关键人员、资源（3.48）、服务和行动

3.29
管理系统
组织（3.34）的一组相互关联或相互作用的要素，用于制定政策（3.38）、目标（3.33）和过程（3.43），以实现这些目标

条目注释1：管理体系可以涉及单一学科或多个学科。

条目注2：系统要素包括组织结构、角色和职责、规划（3.37）、运行。

条目注释3：管理体系的范围可以包括整个组织、组织的具体和已确定职能、组织的具体和已确定部门，或一组组织的一个或多个职能。

条目注释4：组织使用管理系统制定政策，并通过目标和指标（3.72）将其付诸实施，使用：

-组织结构，其中定义了人员的角色、职责、权限等；

-系统过程和相关资源（3.48）以实现目标和指标；

-评估（3.30）和评价方法，以根据目标和指标评估绩效（3.36），并将结果反馈用于规划系统改进；

-审查（3.49）过程，确保纠正问题并识别和实施改进机会，如果合理的话。

3.30
量度
过程（3.43）以确定一个值

3.31
监视
确定系统、过程（3.43）或活动的状态

条目注释1：为了确定状态，可能需要检查、监督或严格观察。

3.32
新教教徒
未满足要求（3.45）

3.33
客观的
要达到的结果

条目注释1：目标可以是战略目标、战术目标或操作目标。

条目注释2：目标可以涉及不同的学科（如财务、健康和安全以及环境目标），并且可以在不同层次上应用（如战略、组织范围、项目、产品和过程（3.43））。

条目注释3：目标可以用其他方式表达，例如。作为预期结果、目的、操作标准、安全操作目标（3.65）或使用其他含义相似的词语（例如，目标、目的或目标（3.72））。

条目注释4：在安全操作管理（3.64）系统中，组织（3.34）根据安全操作政策（3.66）设定安全操作目标，以实现特定结果。

3.34
组织
具有自身职能、责任、权限和关系以实现其目标的个人或群体（3.33）

条目注释1：组织的概念包括但不限于独资商人、公司、企业、公司、企业、当局、合伙、慈善或机构、政府或公共实体，或其部分或组合，无论是否成立，公共或私人。

3.35
外包（动词）
安排由外部组织（3.34）执行组织的部分职能或过程（3.43）

条目注1：外部组织不在管理体系范围（3.29）内，但外包的职能或过程在范围内。

3.36
表演
可测量结果

条目注释1：性能可以与定量或定性结果相关。

条目注释2：绩效可涉及活动、过程（3.43）、产品（包括服务）、系统或组织（3.34）的管理。

3.37

计划
管理层部分工作重点是设定安全运营目标（3.65）和规定必要的操作流程（3.43）以及相关资源（3.48），以实现安全运营目标

3.38

政策
组织的意图和方向（3.34），由其最高管理层正式表达（3.74）

3.39

预防；阻止
使组织（3.34）能够避免、排除或限制不良（3.75）或潜在破坏性事件（3.15）的影响的措施

3.40

预防性措施

消除潜在不合格（3.32）或其他不良潜在情况的原因的措施。注1：一个潜在不合格可能有多个原因。

条目注释2：采取预防措施以防止发生，而采取纠正措施（3.12）以防止再次发生。

[来源：ISO 9000：2015,3.12.1]

3.41

私人保安服务提供商
私营保安公司

指南针

开展或承包安保业务（3.63）的组织（3.34），及其业务活动
包括以自身名义或代表其他方提供安保（3.62）服务

条目注释1：私营保安公司和私营保安服务提供商统称为钙钛矿太阳能电池。条目注释2：钙钛矿太阳能电池向客户（3.4）提供服务，目的是确保其自身和他人的安全。

条目注释3：钙钛矿太阳能电池通常在治理可能薄弱或法治因人为或自然事件（3.19）而受到破坏的情况下开展工作，并根据合同条款提供人员可能需要携带武器执行（3.36）其职责的服务。

条目注释4：钙钛矿太阳能电池提供的安保服务示例包括：警卫；严密保护；物理保护措施；安全意识和培训；风险、安全和威胁评估；为个人、院落、外交和住宅边界提供防护和防御措施；运输护送；以及政策分析。

注5：就本国际标准而言，合资企业视为组织的一部分。

注6：就本国际标准而言，PSC业务属于私人保安业务的法律范围。

3.42

程序
执行活动或过程的特定方式（3.43）

条目注释1：程序可以记录也可以不记录。

[来源：ISO 9000：2015,3.4.5]

3.43

过程

将输入转化为输出的一系列相互关联或相互作用的活动

3.44
记录
记录所取得的结果或提供所执行活动的证据

条目注释1：记录可用于，例如，记录可追溯性并提供验证、预防措施（3.40）和纠正措施（3.12）的证据。

条目注释2：一般情况下，记录不需要在修订控制下。

[来源：ISO 9000：2015,3.8.10]

3.45
要求
陈述的、通常隐含的或强制性的需要或期望

注1：“通常隐含”意味着组织（3.34）和利益相关者（3.24）习惯或通常做法是，考虑中的需求或期望是隐含的。

条目注释2：特定要求是指在文件化信息（3.16）中声明的要求。

3.46
剩余风险

风险处理后剩余风险（3.50）（3.61）

条目注释1：剩余风险可能包含未识别的风险。

条目注释2：剩余风险也可称为“保留风险”。

[来源：ISO指南73：2009,3.8.1.6]

3.47
弹性

组织在复杂多变环境中的适应能力（3.34）[来源：ISO指南73：2009,3.8.1.7]

3.48
资源

资产(3。1）、具有潜在价值且可使用的设施、设备、材料、产品或废物[来源：ANSI/ASIS SPC.1-2009]

3.49
评审
为确定管理体系（3.29）及其组成部分元素（3.17）的适宜性、充分性和有效性（3.33）以及实现既定目标（3.33）而开展的活动

3.50
风险

不确定性对目标的影响（3.33）

条目注释1：影响是指与预期的偏差——正向或负向。

条目注释2：不确定性是指与某一事件（3.19）、其后果（3.10）或可能性（3.27）有关的信息、理解或知识的不足状态，即使是部分不足。

注3：风险通常通过参考潜在的“事件”（如ISO指南73：2009,3.5.1.3中所定义）和“后果”（如ISO指南73：2009,3.6.1.3中所定义），或这些因素的组合来描述。

注4：风险通常以事件后果（包括环境变化）和相关“发生可能性”（如ISO指南73：2009,3.6.1.1中所定义）的组合来表示。

条目注释5：目标可以有不同的方面（如保护人权、安全管理、法律遵守、财务、健康和安全以及环境目标），并且可以在不同的层次上适用（如战略、全组织、项目、产品和过程（3.43））。

条目注释6：风险可能是有意、无意和自然来源造成的。

3.51
风险接受

做出承担特定风险的知情决定（3.50）

条目注释1：风险接受可以在没有风险处理（3.61）或在风险处理过程中（3.43）进行。

条目注释2：已接受的风险需进行监测（3.31）和审查（3.49）。

[来源：ISO指南73：2009,3.7.1.6]

3.52
风险分析

过程（3.43）以了解风险的性质（3.50）并确定风险水平

条目注1：风险分析为风险评价（3.56）和关于风险处理的决策（3.61）提供了依据。

条目注释2：风险分析包括风险估计。

[来源：ISO指南73：2009,3.6.1]

3.53
风险偏好

组织（3.34）准备追求、保留或采取的风险量和类型（3.50）[来源：ISO指南73：2009,3.7.1.2，修改]

3.54
风险评估

风险识别（3.57）、风险分析（3.52）和风险评价（3.56）的总体过程（3.43）[来源：ISO指南73：2009,3.4.1]

3.55
风险标准

用于评估风险重要性的参考条款（3.50）

条目注释1：风险标准基于组织目标（3.33）以及外部和内部环境。

条目注2：风险标准可从标准、法律、政策和其他要求（3.45）中得出。[来源：ISO指南73：2009,3.3.1.3]

3.56
危害度评价

通过将风险分析（3.52）的结果与风险标准（3.55）进行比较，确定过程（3.43）

风险（3.50）和/或其严重程度是否可接受或可容忍：注1：风险评价有助

于决定风险处理（3.61）。

[来源：ISO指南73：2009,3.7.1]

3.57
风险辨认

风险发现、识别和描述过程（3.43）（3.50）

条目注1：风险识别包括识别风险源、事件（3.19）、其原因及其潜在后果（3.10）。

条目注释2：风险识别可涉及历史数据、理论分析、知情和专家意见以及利益相关者（3.24）需求。

[来源：ISO指南73：2009,3.5.1]

3.58
风险管理

协调活动，以指导和控制组织（3.34）的风险（3.50）[来源：ISO指南73：2009,2.1]

3.59
风险登记册

已识别风险信息记录（3.44）（3.50）

注1：对风险评估（3.54）过程中识别、分析和评价的所有风险进行汇编（3.43），包括风险登记册中的信息，包括可能性（3.27）、后果（3.10）、处理和风险负责人。

3.60
风险容忍

组织（3.34）或利益相关者（3.24）在风险处理（3.61）后，为实现其目标（3.33）而愿意承担风险（3.50）

注1：风险承受能力可能受客户（3.4）、利益相关者、法律或监管要求（3.45）的影响。[来源：ISO指南73：2009,3.7.1.3，修改]

3.61
风险处理

过程（3.43）以修改风险（3.50）

条目注释1：风险处理可包括：

-通过决定不开始或继续从事引起风险的活动来避免风险；

-为了追求机会而承担或增加风险；

-消除风险源；

-改变可能性（3.27）；

-改变后果（3.10）；

-与另一方或多方共同承担风险（包括合同和风险融资）；以及-在知情的情况下保留风险。

注2：处理负面后果的风险处理有时被称为“风险缓解”、“风险消除”、“风险预防”和“风险降低”。

条目注释3：风险处理可能会产生新的风险或修改现有风险。

[来源：ISO指南73：2009,3.8.1]

3.62
保护措施

免受危险、威胁、风险（3.50）或损失的保护状态

条目注1：从一般意义上讲，安全是一个与安全概念相似的概念。两者之间的区别在于强调保护免受来自外部的危险。

注2：术语“安全”表示某物不仅安全，而且已经得到保护。[来源：ANSI/ASIS SPC.1-2009]

3.63
安全运行
与保护人员、有形资产和无形资产有关的活动和职能（3.1）

条目注释1：安保行动可能需要在执行任务（3.36）时携带和使用武器。

条目注释2：该概念包括《国际刑事法院罗马规约》对安全服务的定义：保卫和保护人员和物品，如车队、设施、指定地点、财产或其他地方（无论是否携带武器）或公司人员在履行职责时需要携带或使用武器的任何其他活动。

3.64
安全操作管理
协调活动，以指导和控制组织（3.34）的安全运作（3.63）

条目注释1：安全运营管理的指导和控制一般包括制定政策（3.38）、规划（3.37）和目标（3.33），指导操作过程（3.43）和持续改进（3.9）。

3.65
安全操作目标
与安全操作（3.63）相关的目标或目的

条目注释1：安全操作目标通常基于组织的安全操作策略（3.34）（3.66）

条目注释2：安全操作目标通常针对组织中的相关职能和级别进行规定。

3.66
安全操作策略
组织与安全操作（3.63）相关的总体意图和方向（3.34），由最高管理层正式表达（3.74）

条目注释1：通常，安全操作策略与组织的总体策略（3.38）一致，并为设置安全操作目标（3.65）提供框架。

注2：本国际标准中提出的安保业务管理（3.64）原则可作为制定符合ICoC和蒙特勒文件所述原则和义务的安保业务政策的基础。

3.67
安保业务方案
由最高管理层（3.74）支持的持续管理和治理过程（3.43），并提供资源以确保采取必要步骤协调努力，实现安全运营管理系统（3.64）的目标（3.33）

3.68
安保人员
代表组织工作的人员（3.34），直接或间接从事安全行动的人员（3.63）

3.69
自卫
保护个人或财产免受他人企图造成的伤害

[来源：布莱克法律词典]

3.70
分包
与外部方签订合同，以履行现有合同产生的义务

条目注释1：当一方被合同要求提供一系列服务时，可以将其中一项或多项服务分包给“分包商”或当地部队。

注2：母公司子公司可视为分包组织（3.34）。

3.71
供应链
组织（3.34）、人员、流程（3.43）、物流、信息、技术和资源（3.48）之间的双向关系，从采购材料到交付产品或服务，参与活动并创造价值

条目注释1：供应链可能包括供应商、分包商、制造设施、物流供应商、内部配送中心、分销商、批发商和其它导致最终用户的实体。

3.72
目标
详细性能（3.36）要求（3.45）适用于组织（3.34）（或其部分），该要求源于目标（3.33），并且需要设定和满足这些目标

3.73
威胁分析
识别、鉴定和量化不良事件潜在原因的过程（3.43）（3.19），这可能会对个人、资产（3.1）、系统或组织（3.34）、环境或社区（3.7）造成损害

3.74
高管理层
在最高层指导和控制一个组织（3.34）的个人或团体

条目注释1：最高管理层有权在组织内授权并提供资源（3.48）。

条目注2：如果管理体系范围（3.29）仅涵盖组织的一部分，则最高管理者是指对组织的这一部分进行指导和控制的人员。

条目注释3：最高管理者可称为组织的领导。

3.75
不良事件
可能造成生命损失、有形或无形资产损害（3.1）或对内部或外部利益相关者的人权和基本自由产生负面影响的事件或变化（3.24）

3.76
武力使用连续体
根据对手的反应，连续地增加或减少施加的力的水平，使用合理和必要的力量

注1：所用的力应是消除威胁所需的最小合理量，从而将风险（3.50）和可能发生的任何伤害的严重程度降至最低。

条目注释2：应根据当前情况适当升级或降级武力反应，承认反应可能在几秒钟内从连续体的一个部分移动到另一个部分。

3.77
弱点分析
识别和量化导致易受风险源（3.50）影响的某事物的过程（3.43），该风险源可能导致后果（3.10）

4 组织背景

4.1 了解组织及其背景

4.1.1 将军

组织应确定与其目的相关并影响其实现SOMS预期结果(s)能力的外部和内部问题。

管理体系框架的设计与实施基于对组织及其内外部运营环境的理解。因此，组织应定义并记录其内部和外部环境，包括供应链和分包商。在建立、实施和维护组织的SOMS时，以及分配优先级时，应考虑这些因素。

组织应评估可能影响组织风险管理方式的内部和外部因素。

4.1.2 内部上下文

组织应识别、评价并记录其内部环境，包括：

a) 组织的目标、战略和业务使命；

b) 实现目标的政策、计划和指导方针；

c) 治理、职责和责任以及问责制；

d) 总体风险管理策略；

e) 内部利益相关者；

f) 价值观、精神和文化；

g) 信息流和决策过程；

h) 能力、资源和资产；

i) 程序、流程和实践；

j) 活动、功能、服务和产品；

k) 品牌和声誉。

4.1.3 外部环境

组织应定义并记录其外部环境，包括：

a) 文化和政治背景；

b) 法律、监管、技术、经济、自然和竞争环境；

c) 合同协议，包括合同范围内的其他组织；

d) 基础设施依赖性和操作相互依赖性；

e) 供应链和承包商关系及承诺；

f) 可能影响组织流程和/或目标的关键问题和趋势；

g) 外部利益相关者（包括运营区域内的当地社区）的看法、价值观、需求和利益；

h) 作战部队和权力线。

在确定外部环境时，组织应确保在制定安保业务管理标准时考虑到外部利益相关者的宗旨和关注。

4.1.4 供应链和分包商映射和分析

组织应识别并记录其上下游供应链，特别是可能影响风险的分包商使用情况，以及可能导致不良或破坏性事件的可能性。管理供应链风险应纳入组织的整体安全运营计划中，当已识别出重大风险且有可能导致不良或破坏性事件时。组织应定义并记录其供应链和分包商的安全运营计划中的层级。

4.1.5 定义风险标准

组织应定义和记录评价风险重要性的标准。风险标准应反映组织的价值、目标和资源。在定义风险标准时，组织应考虑：

a) 关键活动、职能、服务、产品和利益相关者关系；

b) 在治理或法治薄弱的环境中运营的经营环境和固有的不确定性；

c) 与破坏性或不良事件相关的潜在影响；

d) 组织遵守的法律和法规要求以及其他要求（例如合同义务、人权承诺）；

e) 组织的总体风险管理政策；

f) 可能对其资产、业务和运营造成的威胁的性质和类型以及后果；

g) 如何确定可能性、后果和风险水平；

h) 利益相关者的需求和影响，特别是生命、安全和人权（见A.6.1.2.3）；

i) 声誉和感知风险；

j) 组织及其客户的风险承受能力或风险规避水平；

k) 将考虑多种风险的组合和顺序。

虽然风险标准是在风险评估过程开始时确定的，但它们是动态的，应持续监测和审查其适当性。

4.2 了解利益相关方的需求和期望

组织应确定

-与SOMS相关的利益相关者；

——这些利益相关者的相关要求。

最高管理层应确保识别、评估和记录内部和外部利益相关者的利益，以实现合同目标并最大限度地降低风险。

在确定内部和外部利益相关者的需求和要求时，组织应考虑其：

a) 利益相关者风险偏好；

b) 客户规定的合同义务；

c) 法律和监管要求以及自愿承诺；

d) 与所提供的服务有关的人权责任和影响；

e) 对外部利益相关者（如当地社区、客户和其他安全提供商）的影响和互动；

f) 服务交付和不合格品的记录和文件要求。

4.3 确定安全运营管理体系的范围

组织应确定SOMS的范围和适用性，以确立其范围（即整个组织或其一个或多个组成部分或职能）。组织应根据其规模、性质和复杂性，从持续改进的角度定义SOMS的范围。

在确定该范围时，组织应考虑：

-组织目标，4.1.2中提到的外部和内部问题；

-4.1.3中提到的要求；

-在潜在可能性和后果的背景下，可能对组织的运营和活动产生不利影响的风险因素。

范围应以文件化信息的形式提供。组织应确定其运营中适用SOMS的所有要素，以及适用的排除情况。

组织应界定范围，符合尊重适用的国际、国家和地方法律和人权的需要，同时保护和维护组织的完整性，包括与利益相关者的关系。

适用性声明应根据组织的风险评估和人权影响分析（见6.1），定义适用于组织范围、法律和合同义务以及运营环境的附录A的相关条款。如果风险评估和人权分析确定附件A中的特定条款与组织的范围、法律和合同义务以及经营环境相关且适用，组织应解决并实施这些条款。具体排除条款及其理由应予以记录。

4.4 安保业务管理系统

组织应根据本国际标准的要求建立、实施、保持并持续改进SOMS，包括所需的过程及其相互作用。组织应为其管理体系建立文件化的期望结果，并根据本国际标准中规定的要求持续改进其有效性。

SOMS应执行ICoC的原则和承诺。

当组织将任何属于本国际标准适用范围的流程或活动进行合同、分包或外包时，组织应确保在SOMS内识别和管理此类分包或外包流程或活动的控制。

5 领导

5.1 领导和承诺

5.1.1 将军

最高管理者应通过以下方式在SOMS的制定和实施以及持续改进其有效性方面展现领导力和承诺：

-确保制定安全运营政策和安全运营目标，并与组织的战略方向相一致；

—确保将SOMS要求整合到组织的业务流程中；

-确保SOMS所需的资源可用于建立、实施、运营、监控、审查、维护和改进SOMS；

-传达有效安全管理的重要性以及遵守的重要性
SOMS要求及其法律责任；

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

-指导和支持人员为提高SOMS的效率做出贡献；

-促进持续改进；

-支持其他相关管理角色，以展示其在责任领域的领导力；

-按计划的时间间隔进行SOMS的管理审查。

注：本国际标准中“业务”一词的含义可以广泛解释为指组织存在的目的的核心活动。

最高管理层应通过监督SOMS的建立和实施，以及激励个人将安全行动与尊重人权作为组织使命和文化的一个组成部分相结合，为SOMS提供积极领导的证据。

5.1.2 符合性声明

最高管理者应制定、记录并发布一份符合性声明，表明组织承诺遵守其SOMS中所体现的尊重人权的责任，并且：

a) *《私营保安服务提供者国际行为守则》；*

b) *蒙特勒关于武装冲突期间私营军事和安保公司运作相关的国际法律义务和良好做法的文件；*

c) *《工商业与人权指导原则》；《2011年联合国“保护、尊重和补救”框架》；*

d) 任何其他适用的国际公认的人权承诺（例如《安全与人权自愿原则》）。

符合性声明还规定了组织对其利益相关者的人权期望，这些期望直接与其运营相关。

符合性声明应：

a) 记录、维护和实施；

b) 公开发布，并在内部和外部向所有相关利益相关者传达；

c) 得到高层管理的明显认可。

5.2 政策

最高管理层应制定安全操作政策，该政策应：

-与组织的目的相适应；

—提供了设置安全操作目标的框架

-包括承诺满足适用的法律和其他要求，包括组织自愿承诺；

-包括对SOMS持续改进的承诺；

-承诺尊重人权；

-承诺避免、预防和减少破坏性或不良事件的可能性和后果。

安全操作政策应：

-可以作为文件化信息提供；

—在组织内部进行沟通；

-通知所有为本组织工作或代表本组织工作的相关人员；

-适当时，向利益相关者提供；

-得到高层管理的明显支持；

-在计划的时间间隔和发生重大变化时进行审查。

5.3 组织机构、职责和权限

最高管理者应确保相关角色的职责和权限在组织内分配和传达。

最高管理者应指定组织内部的一名或多名人员，无论其其他职责如何，都应具有明确的胜任能力、角色、责任和权限，以：

a) 确保SOMS符合本国际标准的要求；

b) 向最高管理层报告SOMS的绩效；

c) 确保按照本国际标准的要求建立、传达、实施和维护SOMS；

d) 识别、监测和管理第4.2条中规定的利益相关者的需求和期望；

e) 确保提供充足的资源；

f) 在整个组织内提高对SOMS要求的认识；

g) 向高层管理人员报告SOMS的绩效，供其审查，并作为持续改进的基础。

最高管理者应确保负责实施和维护SOMS的人员具有必要的权限和能力，并对其操作负责。

6 规划

6.1 应对风险和机遇的行动

6.1.1 将军

在规划SOMS时，组织应考虑4.1.2中提到的问题以及4.1.3中提到的要求，并确定需要解决的风险和机会，以：

-保证SOMS能够实现其预期结果(s)；

-防止或减少不良影响；

—实现持续改进。

组织应为其安全运营建立、实施和维护正式且有文件记录的风险评估流程，包括其相关供应链合作伙伴和分包商活动。风险评估流程应包括：

a) 风险识别-识别并评估威胁、漏洞、后果和人权风险，以确定因有意、无意或自然事件而可能对组织活动、资产、运营、职能及受影响的利益相关者产生直接或间接影响的战略、战术和操作风险，以及其遵守人权原则的能力；

b) 风险分析-系统地分析风险（可能性和后果分析，包括人权风险分析），以确定对活动、职能、服务、产品、供应链、分包商、利益相关者关系、当地人口和环境有重大影响的风险；

c) 风险评估-系统地评估和确定风险控制和治疗措施及其相关成本的优先级，以确定如何将风险控制在符合风险标准的可接受水平。

组织应：

a) 记录并保持此信息的最新和安全；

b) 定期审查安全运营的管理范围、政策、风险标准和风险评估是否仍然适合于组织的内部和外部环境；

c) 在组织内部发生变更或对组织的经营环境、程序、职能、服务、合作伙伴和供应链进行变更的情况下，重新评估风险；

d) 评估风险管理方案的直接和间接收益和成本，以提高可靠性和恢复能力；

e) 评估事件发生后和演习后的风险处理方案的实际有效性；

f) 确保在制定、实施和运行SOMS时考虑优先风险和影响；

g) 监控和评估风险控制和治疗的有效性。

风险评估应确定需要管理的活动、操作和过程，输出应包括：

a) 优先风险登记册，确定管理风险的措施；

b) 风险可接受的依据；

c) 关键控制点（立方最密堆积）的识别；

d) 外包和分包商控制要求。

与安全操作一致，组织应建立一个过程来监控和评估，
评估并应对风险环境的变化。

组织应计划：

a) 应对这些风险和机遇的行动；

b) 如何：

-将这些行动整合并实施到其SOMS流程中；

-评估这些行动的有效性。

6.1.2 法律和其他要求

组织应确保在建立、实施和维护SOMS时考虑并纳入适用的法律和其他要求。

组织应：

a) 确定与其业务和安全运营相关的适用的法律、法规、合同、许可和其他要求和承诺；

b) 除法律要求的外，确定与业务和安全行动相关的适用人权责任；

c) 确定这些要求如何适用于其操作以及本国际标准适用范围内的任何分包商或合资企业的操作。

组织应记录这些信息并保持其最新状态。组织应向代表其工作的人和其他相关第三方，包括分包商传达有关法律和其他要求的相关信息。组织及其客户有遵守这些义务的法律和道德责任。

注：为了本国际标准的目的，国家法律可以包括组织所在国、其人员所在国、运营所在国和客户所在国的法律。

6.1.3 内部和外部风险沟通和协商

组织应在风险评估过程中与内部和外部利益相关方建立、实施并维护正式的书面沟通和协商流程，以确保：

a) 理解客户（包括受保护的人员、组织、社区和/或活动）的运营目标和利益；

b) 风险得到充分识别和沟通；

c) 了解其他内部和外部利益相关者的利益；

d) 与相关利益相关者沟通风险及其处理；

e) 了解与分包商和供应链内的相关方之间的依赖关系和联系；

f) 安全运营风险评估流程与其他管理学科相衔接；

g) 风险评估在适当的内部和外部背景下进行，与组织及其分包商和供应链相关。

6.2 安全运营目标和实现这些目标的计划

6.2.1 将军

组织应在相关职能和级别上建立安全运营目标。

安全操作目标应：

a) 与安全操作策略保持一致；

b) 可测量（如可行）；

c) 考虑适用要求；

d) 应受监控；

e) 应予以通报；

f) 根据需要进行更新。

组织应保留有关安全运营目标的文件化信息。在规划如何实现其安全运营目标时，

组织应确定：将要做什么；

-需要什么资源；

——谁将负责；

-完成时间；

-如何评估结果。

组织应建立、实施和维护文件化的目标和指标，以管理风险，以便预测、避免、预防、阻止、减轻、应对并从破坏性或不良事件中恢复。记录的目标和指标应为组织、其分包商和供应链建立内部和外部期望，这些期望对于任务完成、产品和服务交付以及功能操作至关重要。

目标应根据安全运营政策和风险评估制定，并与之保持一致，包括承诺：

a) 通过降低可能性和后果来最小化风险；

b) 遵守国际、国家和地方法律和人权；

c) 财务、运营和业务要求（包括分包商和供应链承诺）；

d) 持续改进

在确定和审查其目标和指标时，组织应考虑其财务、运营和业务需求、法律、法规和其他要求、人权影响、重大风险、技术选择以及利益相关者的观点。

与关键绩效指标相关的目标应可定性和/或定量地衡量。目标应来源于安全运营目标，并且应符合以下要求：

a) 达到适当的详细程度；

b) 与风险评估相称；

c) 具体、可衡量、可实现、相关和基于时间（在可行的情况下）；

d) 通知所有相关员工和第三方，包括分包商和供应链合作伙伴，目的是让这些人了解他们的个人义务；

e) 定期审查，以确保其与安全运营目标保持相关性和一致性，并相应修改。

6.2.2 实现安全操作和风险处理目标

组织应建立、实施和维护实现其安全运营和风险处理目标的方案。这些方案应经过优化和优先排序，以便控制和处理与运营、分包商和供应链相关的风险。组织应建立、实施和维护正式且有文件记录的风险处理流程，该流程应考虑：

a) 在可能的情况下消除风险源；

b) 消除或降低事件及其后果的可能性；

c) 消除、减少或减轻有害后果；

d) 与其他方分担风险，包括风险保险；

e) 将风险分散到资产和功能上；

f) 通过知情决策接受风险或追求机会；

g) 避免或暂时停止产生风险的活动。

最高管理者应：

a) 评估消除、降低或保留风险的备选方案的收益和成本；

b) 评估其安保业务方案，以确定这些措施是否引入了新的风险；

c) 定期评审风险处理，以反映外部环境的变化，包括法律、法规和其他要求，以及组织的政策、设施、信息管理系统（系统）、活动、职能、产品、服务和供应链的变化。

7 支助

7.1 资源

7.1.1 将军

组织应确定并提供建立、实施、保持和持续改进SOMS所需的资源。

组织应考虑：

a) 现有的和可能增加的内部资源、能力和限制；

b) 哪些服务和商品将从外部采购。

可利用的资源包括相关信息、管理工具、人力资源，包括具有相关经验和专门技能和知识的人、技术和防护设备以及后勤支助，无论是内部还是外部承包。

7.1.2 结构要求

7.1.2.1 将军

组织应是法人或法人的一部分，应有明确的管理结构，显示组织各层级（包括其范围内的子公司）的控制和责任。

7.1.2.2 组织结构

明确的管理结构应确定其运营和服务的角色、职责、权限和责任。组织应：

a) 载明组织机构设置，明确管理层的职责、权限；

b) 定义并记录组织是否为某一法人实体的明确组成部分，以及与同一法人实体其他部分的关系；

c) 定义SOMS范围内的任何合资或合作安排。

7.1.2.3 保险

组织应证明其拥有保险，以覆盖与其风险评估一致的运营和活动产生的风险和相关责任。当外包或分包服务、运营或职能时，组织应确保分包活动有适当的保险覆盖。

7.1.2.4 外包和分包

组织应有明确的分包或外包活动、职能和业务流程。组织应建立、记录、传达并监督其分包商和外包合作伙伴遵守安全业务和尊重人权的具体职权范围和行为准则。

组织应有书面协议，涵盖分包或外包安排，包括：

a) 分包商承诺遵守与本组织相同的法律、道德和人权承诺及义务，如本国际标准所述；

b) 风险报告流程，以及不良和破坏性事件的发生和应对；

c) 保密和利益冲突协议；

d) 明确界定和记录将要提供的服务；

e) 指挥控制范围和限制；

f) 承包商与分包商之间的支持关系的定义；

g) 符合本国际标准的适用条款。

7.1.2.5 财务和行政程序

组织应制定财务和行政程序和控制措施，以支持在所有计划和运营中提供有效的安全和风险管理，以预测和应对破坏性或不良事件。程序应：

a) 设立的目的是确保财政决策能够加快；

b) 按照既定的权限级别和会计原则；

c) 与客户协商和协调后建立。

7.2 能力

7.2.1 将军

组织应：

-确定在其控制下从事影响其安全运营绩效工作的人员（或人员）的必要能力；

确保这些人具备适当的教育、培训或经验；

-在适用的情况下，采取行动获得必要的能力，并评估所采取行动的有效性；

-保留适当的书面信息作为胜任能力的证据。

注：适用的行动可以包括，例如，向目前受雇人员提供培训、指导或重新分配工作，或者聘用或与有能力的人签订合同。

7.2.2 能力鉴定

本组织应确定与其安保业务有关的能力、能力水平和培训需求，特别是与履行个人职能有关的能力、能力水平和培训需求，同时应遵守法律和合同义务并尊重人权。

组织应建立、实施和维护程序，以确保代表其执行任务的人员在以下各领域表现出适当水平的能力：

a) 安全功能的性能；

b) 评估风险；

c) 管理风险评估中发现的风险以及与工作相关的潜在人权影响；

d) 适用的当地和国际法律，包括刑法、人权法和国际人道主义法，包括但不限于：

   1) 禁止酷刑和其他残忍、不人道或有辱人格的待遇；

   2) 禁止和提高认识性剥削和性虐待或基于性别的暴力；

   3) 承认和防止人口贩运和奴役；

   4) 打击贿赂、腐败和类似犯罪的措施；

e) 他们所处环境的文化，如风俗和宗教；

f) 减少破坏性或不良事件的可能性和/或后果的程序，包括应对和缓解程序，以应对和报告事件；

g) 事故报告和记录程序；

h) 急救、健康和安全程序；

i) 使用武器，包括机械操作和实弹射击资格测试，使用经组织授权并针对具体安全相关任务规定的特定武器（或多种武器）；

j) 与安全行动有关的使用武力的限制；

k) 通信协议、手段和程序；

l) 针对内部和外部利益相关者的投诉程序。

7.2.3 培训和能力评估

组织应提供基于能力的培训，并建立衡量熟练程度或能力水平的方法。代表组织工作的人员应接受培训，以证明其具备所需的能力和熟练程度。

组织应：

a) 为培训方案制定基于能力的衡量标准；

b) 提供培训，使人们了解尊重人权是本组织的核心价值观和治理的一部分；

c) 为所有被授权在执行职务时携带致命性、非致命性或非杀伤性武器的人员提供初始和定期的课堂、体能、机械和实弹训练和评估；

d) 提供武器和使用武力的再培训，以满足法律、合同要求或更频繁地保持组织确定的能力水平；

e) 确定需要定期进修培训的其他能力，以保持所需的工作水平或纳入新的要求；

f) 提供培训，说明遵守SOMS政策和程序以及SOMS要求的重要性，以及偏离SOMS和安全操作规定程序的潜在后果。

7.2.4 文件

组织应保留以下记录：

a) 确定能力及衡量标准；

b) 培训方案；

c) 代表其工作的人员的培训和评估的相关记录。

7.3 意识

在组织控制下工作的人员应了解：

—安全业务政策；

-对SOMS有效性的贡献，包括改善安全运营绩效带来的好处；

-不符合SOMS要求的后果。

7.4 通信

7.4.1 将军

组织应确定与SOMS相关的内部和外部沟通的需要，包括：

——关于它将传达什么信息；

-何时沟通；

-与谁交流；

-如何沟通。

组织应建立、实施和维护以下程序：

a) 与内部和外部利益相关者沟通；

b) 接收、记录和回复来自内部和外部利益相关者的通信；

c) 在非典型情况和中断期间，确定并确保通信手段的可用性；

d) 对通信系统进行正常和异常情况下的定期测试。

沟通程序应考虑操作信息的敏感性质和信息共享的法律限制。

7.4.2 业务通信

组织应制定沟通程序，以分享有关安全团队活动、位置、运营和后勤状态、相关威胁信息以及向公司管理层、客户、其他私人安全团队和相关民用或军事当局报告事件的信息。这应包括请求立即从军事或民用当局、其他安全团队和紧急医疗支持提供援助的程序。

组织应确保所有级别和操作员能够接收和理解口头和书面沟通，并且所有级别能够使用适当的内部和外部利益相关者能够理解的语言或方式做出回应。

安全团队应能够以受保护方理解的形式向其保护的方传达与安全相关的信息。

7.4.3 风险沟通

组织应根据保障生命为首要任务，并与利益相关者协商，决定是否对外沟通重大风险、其影响及应对措施，并记录其决定。如果决定对外沟通，组织应建立并实施(a)外部沟通的方法、警报和警告（包括媒体）。

7.4.4 投诉和申诉程序

应向内部和外部利益相关者传达投诉和申诉程序。程序应在网站上公开，并尽量减少因语言、教育水平或害怕报复而造成的访问障碍，同时考虑保密和隐私的需求。

7.4.5 传达举报人政策

组织应告知代表其工作的人员，如果他们有合理理由相信发生了不符合本国际标准的情况，他们有权在内部匿名报告不符合情况，并向适当的主管部门报告。

7.5 记录的信息

7.5.1 将军

组织的SOMS应包括：

-本国际标准要求的文件化信息，包括记录；

-安全操作策略、符合性声明、目标和指标的文档；SOMS范围的描述；

-适用性声明；

-对SOMS主要元素及其相互作用的描述，以及相关文件的参考；

-有效实施和运行SOMS所需记录的信息；

-组织确定的、对SOMS有效性必要的文件化信息。

注：由于以下原因，不同组织的SOMS记录信息范围可能有所不同：

-组织的规模及其活动、流程、产品和服务的类型；

——过程及其相互作用的复杂性；

-人员的能力。

7.5.2 创建和更新

7.5.2.1 将军

在创建和更新记录信息时，组织应确保适当：

-识别和描述（例如标题、日期、作者或参考编号）；

—格式（例如。语言、软件版本、图形）和媒体（如纸张、电子）；

-审查和批准适用性和充分性。

7.5.2.2 记录

组织应建立并保持记录，以证明符合其SOMS的要求。

记录包括：

a) 本国际标准要求的记录；

b) 许可证和经营许可；

c) 人员筛查；

d) 培训记录；

e) 过程监控记录；

f) 检验、维护和校准记录；

g) 相关的分包商和供应商记录；

h) 事故报告；
i) 事故调查记录及其处理情况；
j) 审计结果；
k) 管理评审结果；
l) 外部沟通决策；
m) 适用法律要求的记录；
n) 重大风险和影响记录；
o) 武器库存和武器发放收据；
p) 管理体系会议记录；
q) 安全、安保行动和人权执行情况信息；
r) 与利益相关者的沟通。

7.5.3 文件化信息的控制

应控制SOMS和本国际标准要求的文件化信息，以确保：

a) 在需要的时间和地点，它可用且适合使用；
b) 得到充分保护（例如，防止机密性丧失、不当使用或完整性丧失）。

对于记录信息的控制，组织应酌情处理以下活动：

-分发、访问、检索和使用；
-存储和保存，包括保持清晰度；
-控制变更（例如版本控制）；
-保留和处置。

组织应建立、实施和维护以下程序：

a) 在发布前批准文件的充分性；
b) 保护信息的敏感性和保密性；
c) 审查、必要时更新并重新批准文件；
d) 对文件进行修订；
e) 随时提供更新和批准的文件；
f) 确保文件清晰易辨；
g) 确保识别外部来源的文件并控制其分发；
h) 防止过时文件的非预期使用；
i) 确保对过时文件进行适当、合法和透明的销毁。

应酌情识别并控制组织确定的、对SOMS的规划和运行而言必要的外部来源文件化信息。

注：访问权限可能意味着仅查看记录信息的权限决定，或者查看和更改记录信息的权限和授权。

组织应建立、实施并维护程序，以保护记录的敏感性、保密性和完整性，包括访问、识别、存储、保护、检索、保留和处置记录。记录应根据合同和适用法律的要求进行保存。雇用和服务记录应至少保存七年或按适用法律要求保存。组织应确保文件的完整性，通过安全备份、仅授权人员可访问以及防止未经授权的披露、修改、删除、损坏、退化或丢失来实现。

8 操作

8.1 业务规划和控制

8.1.1 将军

组织应通过以下方式计划、实施和控制为满足要求和执行6.1中确定的措施所需的流程：

-制定流程标准；

-按照标准实施对过程的控制；

-保留必要的文件信息，以确保流程按计划执行。

组织应确定与已识别的重大风险相关的活动，并符合其安全管理操作政策、风险评估、目标和指标，以确保在特定条件下执行这些活动，从而使其能够：

a) 遵守法律和其他监管要求，包括其运营的许可和执照；

b) 完成任务的同时保护客户的声誉；

c) 遵守当地和适用的国际法，包括国际人道主义法、人权法和习惯法，以及本国际标准中描述的其他义务；

d) 确保代表本组织工作的人员的安全、福祉和权利；

e) 尊重当地社区的权利；

f) 实施风险管理控制，以尽量减少破坏性或不良事件的可能性和后果；

g) 实现其安全操作目标和目标。

组织应建立、实施和维护文件化程序，以控制其缺失可能导致偏离SOMS政策、目标和指标的情况。

组织应控制计划变更，并审查非预期变更的后果，必要时采取措施减轻任何不利影响。

组织应确保外包过程得到控制。

8.1.2 安全相关功能的性能

组织应建立、实施和维护程序，以支持保护人员、有形资产和无形资产以及其他安全相关职能，包括但不限于：

a) 管理风险评估中发现的风险；

b) 客户或主管机构要求的特定功能；

c) 其他任务和特定上下文功能。

8.1.3 尊重人权

组织应建立、实施并维护程序，以尊严和尊重人权对待所有人，并报告任何不符合情况。组织应制定并传达给所有代表其工作的人员，与其行为一致的程序，这些程序应符合尊重人权的原则；以及适用于组织安全运营的任何合同、法律和监管要求。

8.1.4 不良或破坏性事件的预防和管理

组织应制定、实施和维护程序，记录组织将如何预防、缓解和应对不良和破坏性事件，考虑以下内容：

a) 安全功能的性能；

b) 保护生命，促进人员和内部及外部利益相关者的安全；

c) 尊重生命和人的尊严；

d) 将不良事件的预测和预防作为首要任务；

e) 应对和缓解措施，以防止破坏性事件升级；

f) 尽量减少对运营和服务的干扰；

g) 尽量减少对当地社区的任何不利影响；

h) 通知有关当局；

i) 吸取的经验教训和纠正预防措施，以避免再次发生。

8.2 制定行为规范和道德操守准则

组织应制定、实施并维护一套行为准则，适用于所有代表其工作的人员，包括员工、分包商和外包合作伙伴。该行为准则应形成文件，明确专业操守在安全运营中的重要性，并清晰传达对人权和人类尊严的尊重。行为准则应确保所有代表其工作的人员了解其防止和报告任何侵犯人权行为的责任。

组织应向代表其工作的所有人员以及客户传达并记录其《道德规范》。

8.3 使用武力

8.3.1 将军

组织应制定并记录代表其工作的人员使用武力的程序。如适用，此类程序应遵循由以下机构发布的武力使用规则（RUF）：

符合本国际标准要求的用于安全操作的合格法律机构。

注：主管法律当局包括但不限于组织注册地或主要管理地所在州（或）政府、对组织运营区域行使控制权的政府、与组织签订安全合同的政府，或行使相当于军事占领区域权力的军事指挥官。

在没有授权的RUF的情况下，组织应根据已发布的国际武力使用指导原则（例如1990年联合国《执法人员使用武力和火器的基本原则》和蒙特勒文件）制定程序。武力使用的程序应与相关法律一致，并在采纳前接受适当的法律审查。

本组织应制定保安业务人员自卫时使用的武力程序，包括保护本组织保护下的人员的自卫程序，这些程序应包括：

a) 授权其人员使用和携带武器；

b) 武力使用连续体；

c) 使用非致命武力；

d) 使用致命武力；

e) 为支持执法而使用武力（如适用）；

f) 训练

组织应建立并记录与其业务范围和每个地点所执行工作的条件相关的程序。组织使用武力的程序应与适用法律和合同要求一致，并且应与提供私人安保业务的任何其他实体达成协议。

8.3.2 武器授权

组织应制定并记录授权其人员在执行安保作业时携带武器的程序。授权应：

a) 只能授予组织认定适合执行任务的人员，且这些人员已经接受了与所执行任务相适应的背景调查；

b) 应针对某种武器类型和型号，且只有在个人按照使用武力程序中确定的、适用于该武器和预期职责的已发布标准对该类型和型号进行资格鉴定后才能发放。

在向个人发放武器之前，所有武装授权都应以书面形式并由相应的授权官员（或）签字（例如：墨水或数字签名）。组织应保留个人资格结果的文件，直至个人获得武装授权为止。

8.3.3 使用武力连续体

组织应建立并记录描述使用武力连续体的程序，应用合理必要的适当武力进行安保行动。连续体的要素应包括：

a) 使用武力的强度、持续时间和程度应当根据当时的情况合理；

b) 警告相关人员，并在情况或环境允许时提供撤回或停止威胁行动的机会；

c) 在情况和环境允许的情况下，降低使用武力的强度；

d) 对使用武力的启动、升级和降级以及对该权力的限制进行监督控制。

使用武力连续程序应符合自卫的固有权利。

8.3.4 非致命性武力

组织使用武力的程序应涵盖使用非致命武力，即那些不太可能导致死亡或严重身体伤害的武力程度，以及其人员在执行安全行动时被授权和可用的非致命武力类型。组织应根据适用的相关自卫法律记录非致命武力使用的程序，包括但不限于以下情况：

a) 在使用武力的其他方法失败或不可用时，防止他人攻击他人或自己，以避免受伤或继续攻击；

b) 当使用武力的其他办法已经失败或不可行时，对反抗合法逮捕的人；

c) 防止在本组织保护下的财产损失或毁坏。

8.3.5 致命武力

只有在必要的情况下才可使用致命武力，而且只能在无法合理使用或使用较轻手段无效时才能使用。本组织的武力使用程序应确定其每一项安保行动适用的自卫法律，并且应说明与下列方面有关的使用致命武力：

a) 固有的自卫权；

b) 保卫他人；

c) 对财产的防御，包括固有危险的财产或关键基础设施，如果丢失或被毁，将造成死亡或严重人身伤害的直接威胁。

只有在有合理理由相信存在以下情况时，才可使用致命武力：

a) 某人或多人对个人或附近其他人构成迫在眉睫的死亡或严重身体伤害威胁；

b) 在必要时防止对固有危险财产的实际盗窃或破坏；

c) 防止破坏或摧毁关键基础设施，主管法律当局确定的对关键基础设施的损害将造成死亡或严重身体伤害或伤害的紧迫威胁。

8.3.6 使用武力支持执法

当国家授权支持执法行动时，该组织应向相关国家的执法机构或控制军事机构申请RUF以履行此职能。若无法获得RUF，该组织的使用武力程序还应包括以下源自联合国《执法人员使用武力和火器的基本原则》的内容：

-有意使用致命枪支仅在严格不可避免的情况下，为了保护生命而使用；注：这并不改变自卫时使用合理和必要武力的固有权利。

-使用武力的连续过程应包括对组织人员的视觉或听觉识别，以表明其为执法人员，并明确警告使用枪支的意图

8.3.7 使用武力训练

组织使用武力程序应描述初次和反复培训的要求。获授权携带枪支的安全操作人员应圆满完成包括枪械熟悉（课堂学习）、实弹资格认证和使用武力训练在内的培训。此类培训应每12个月完成一次，或根据法律或合同要求，或组织风险评估的结果更频繁地进行。培训记录和能力展示应保存至相关人员与组织关系终止为止。

组织的武力使用培训应包括以下要素：

a) 将自卫的适用法律适用于特定的安全行动；

b) 审查该组织的武器授权、储存和运输政策；

c) 审查安全行动中使用武力与军事部队的交战规则之间的差异；

d) 审查使用导致人员死亡或严重受伤的武力和火器可能产生的法律责任；

e) 在可以合理确定使用武力的指示明显违法的情况下，服从上级命令作为辩护是不可用的；

f) 武力连续体的应用。

组织应制定培训辅助材料，供其人员携带，以帮助他们理解、记忆和应用特定的武力使用程序或适用的RUF。

8.4 拘捕和搜查

8.4.1 对人员的拘捕

组织的运营程序应包括逮捕涉嫌对受安全行动保护的人身或财产实施攻击的人。程序应描述在何种法律背景下可以强制扣留人员，使用武力的限制，以及组织何时及向谁移交被扣留人员的程序。

8.4.2 搜索

本组织的业务程序将说明在何种情况下可对第三方进行武器或其他违禁品搜查。在出入检查点对人员的搜查应说明按照基本人权、文化考虑和个人尊严对待这些人的要求。

8.5 支助执法行动

8.5.1 执法支助

该组织只能根据相关国家执法或控制军事当局的授权，按照适用的相关法律执行此类执法行动。该组织应制定额外的程序以支持执法行动中的安全行动，包括：

a) 按照有关执法或控制军事当局的指示，穿着制服和车辆标识；

b) 记录向任何受伤或受影响的人提供援助和医疗救助的程序；

c) 向执法机关和本组织的监督人员及时报告在执法活动中使用武力和火器造成的伤亡事件；

d) 如果已知，应将受组织执法活动伤害或受影响的人员姓名通知支持执法机构。

8.5.2 拘留行动

保护、运送或讯问被执法机关逮捕、拘留或监禁的人不在本国际标准的范围之内。

8.6 资源、角色、职责和权限

8.6.1 将军

最高管理者应提供必要的资源，以建立、实施、保持和改进SOMS。资源应包括信息、管理工具和人力资源（包括具有专门技能和知识的人员）以及财政支持。

应定义、记录和传达角色、职责和权限，以便于有效安全管理，包括控制、协调和监督责任，并确定继承顺序。

为有效应对破坏性事件和不良事件，组织应建立规划、安全、事件管理、响应和/或恢复团队（），并规定其职责、适当权限、充足资源，包括有效且安全的设备，并制定演练操作计划和程序。

如果组织选择分包或外包任何影响符合本国际标准要求的过程，组织应确保对这些过程进行控制。

8.6.2 人员

8.6.2.1 将军

组织应保留具有适当能力的足够人员（雇员、承包商或分包商），以履行其合同义务。应向人员提供与其职责和环境相称的适当薪酬和报酬安排，包括保险。组织应酌情保护该信息的机密性，并向相关人员提供所有各方都能理解的相关文件。

组织应保存所有人员的文件化信息：

a) 符合法律和合同义务的要求；

b) 与个人及其直系亲属保持联系；

c) 协助人员在发生事故时进行恢复；

d) 需要通知家人受伤或死亡。

8.6.2.2 人员甄选、背景审查和审查

组织应建立、记录、实施和维护所有层级代表其工作的人员的背景审查和审查程序，以确保他们适合并适当

针对他们将要开展的任务（即分包商、外包合作伙伴和子公司）。在可能的情况下，并且符合数据保护法，筛选应包括：

a) 符合法律和合同要求；

b) 身份、最低年龄和个人历史验证；

c) 教育和就业历史审查；

d) 军事、警察和安全部门记录检查；

e) 审查可能的犯罪记录；

f) 审查侵犯人权的报告；

g) 药物滥用评估；

h) 对指定活动的体能和精神评估；

i) 评估是否适合携带武器作为其职责的一部分。

当地法律、组织所在地适用的法律或客户要求的最低年龄要求可以设定。但是，在任何情况下，不得雇用未满18岁的人从事需要使用枪支或其他武器的工作。

筛选应包括人员的证明，即其当前或过去的任何行为都不会违背组织的《道德规范》、《符合性声明》或遵守本国际标准的条款。应要求工作人员通知组织任何可能导致审查其筛选状态的情况变化。

背景审查涉及高度敏感信息的披露，因此，组织应制定程序，以适当和严格地保护信息的内部和外部保密性。记录应与相关时效法规保持一致。

合格人员的选择应基于规定的胜任能力，包括知识、技能、能力和属性，筛选和选择措施应符合法律和合同要求，并与本国际标准的规范性引用文件一致。

8.6.2.3 分包商的选择、背景审查和审查

组织应制定明确的程序，用于选择、背景审查和审查分包商。组织负责分包商的工作，并且在适用法律的范围内，对分包商的行为负责。组织应：

a) 确保与分包商签订适当的书面合同协议；

b) 以书面形式向客户说明安排，并在适当情况下获得客户的批准；

c) 维护其使用的所有分包商的登记册；

d) 向分包商传达本国际标准的责任；

e) 保留分包工程符合或不符合本国际标准的证据记录。

8.6.3 武器、危险材料和弹药的采购和管理

使用武器、危险材料、爆炸物和弹药的组织应建立有关武器采购、管理、清点和可追溯性的书面程序和记录，包括：

a) 遵守适用的和相关的国家和国际法律（例如联合国制裁）；

b) 遵守进出口管制、注册、认证、许可和运输要求；

c) 收购

d) 安全存储；

e) 对其识别、发放、使用、维护、返还和损失进行控制；

f) 关于武器发放给谁、何时发放的记录；

g) 所有弹药和武器的识别和清点；

h) 妥善处置并进行验证。

8.6.4 制服和标志

该组织在履行合同开展活动时，应按照其客户的安全、其他平民的安全以及法律的要求，使用制服和标识来识别其人员和交通工具是否属于该组织。这种标识应能在远处看见，并且与军警使用的标识有区别。组织应制定和记录制服和标记的使用程序，以及确定和记录何时这种标识不符合本条款要求的程序。

8.7 职业健康和安全

组织应建立、实施和维护程序，以促进安全和健康的工作环境，包括合理的预防措施，以保护在其代表下从事高风险或危及生命操作的人员，符合法律、法规和合同义务。程序应包括：

a) 评估代表其工作的人员的职业健康和安全风险以及外部方的风险；

b) 敌对环境训练；

c) 提供个人防护装备、适当的武器和弹药；

d) 医疗和心理健康意识培训、护理和支持；

e) 识别和处理工作场所暴力、不当行为、酗酒和吸毒、性骚扰和其他不当行为的准则。

8.8 突发事件管理

8.8.1 将军

组织应建立、实施和维护程序，以识别可能影响组织、其活动、服务、利益相关者、人权和环境的不良和破坏性事件。程序应记录组织如何主动预防、缓解和应对事件。

在制定、实施和维护快速准备、缓解和应对破坏性事件的程序时，组织应考虑以下各项行动：

a) 保障生命安全，确保内部和外部利益相关者的安全；

b) 尊重人权和人的尊严；

c) 防止破坏性事件进一步升级；

d) 尽量减少对运营的干扰；

e) 通知有关当局；

f) 保护形象和声誉（组织及其客户）；

g) 纠正和预防措施。

8.8.2 事件监测、报告和调查

组织应建立、实施并维护事件监控报告、调查、纪律安排和补救措施的程序。涉及使用武力或武器、任何伤亡、身体伤害、虐待指控、敏感信息或设备丢失、药物滥用或不符合《蒙特勒文件》和《国际刑事法院罗马规约》原则以及适用法律法规的事件，应进行报告并采取以下步骤进行调查：

a) 事件的文档记录；

b) 通知有关当局；

c) 为调查事件而采取的步骤；

d) 识别根本原因；

e) 采取的纠正和预防措施；

f) 给予受影响方的任何赔偿和补救。

组织应确保代表其工作的所有人员都了解其职责以及监测和报告不符合项和事件的机制。

应保存并保留不符合项和事件记录，保存期限至少为7年或法律或法规要求。

8.8.3 内部和外部投诉和申诉程序

组织应建立程序，以记录和处理来自内部和外部利益相关者（包括客户和其他受影响方）的投诉。应制定并记录投诉程序的有效性标准。这些程序应传达给内部和外部利益相关者，以便个人报告潜在和实际不符合本国际标准的情况，或违反国际、国家和地方法律或人权的行为。组织应迅速、公正地调查指控，并适当考虑保密性和当地法律规定的限制。组织应制定并记录以下程序：

a) 受理和处理投诉和申诉；

b) 为解决过程建立分层步骤；

c) 对申诉的调查，包括以下程序：

    1) 配合官方外部调查机制；

2) 防止恐吓证人或妨碍收集证据；

3) 保护善意提出申诉或申诉的人免遭报复；

d) 识别根本原因；

e) 采取的纠正和预防措施，包括与任何违规行为相称的纪律措施；

f) 与有关当局的沟通。

对于指控犯罪行为、侵犯人权或对个人构成迫在眉睫的危险的申诉，组织和其他当局应酌情立即予以处理。

8.8.4 举报人政策

组织应为代表其工作的人员制定举报政策，这些人员有合理理由相信发生了不符合本国际标准的情况，并尊重他们内部匿名报告不合规行为的权利，以及向适当当局外部报告的权利。组织不得因任何个人出于善意进行举报而采取任何不利行动。组织应告知客户所报告的法律违规或人权侵犯行为。

9 业绩评价

9.1 监测、测量、分析和评价

9.1.1 将军

组织应通过定期评估、测试、事件后报告、经验教训、绩效评估和演习来评估安全运营管理和计划、程序和能力。这些因素的重大变化应立即反映在程序中。

组织应保留定期评价结果的记录。

组织应确定：

-需要监测和测量的内容；

-监测、测量、分析和评价的方法，如适用，以确保有效结果；

—应当进行监测和测量的时间；

-应分析和评价监测和测量的结果。

组织应保留适当的文件化信息，作为结果的证据。

组织应评估安全操作绩效和SOMS的有效性。

组织应建立、实施和维护绩效指标和程序，以定期监控和衡量其运营中对绩效有重大影响的特性（包括合作伙伴关系、分包合同和供应链关系）。这些程序应包括记录用于监控绩效的信息、适用的操作控制措施以及与组织安全运营管理目标和指标的一致性。

组织应评估并记录保护其资产（人力和物力）以及通信和信息系统性能。

9.1.2 依从性评价

为符合其遵守承诺，组织应建立、实施和维护定期评估遵守适用法律、法规和人权要求的程序。

组织应保留定期评价结果的记录。

9.1.3 练习和测试

组织应使用演练和其他手段测试其SOMS计划、流程和程序的适当性和有效性，包括利益相关者关系和分包商之间的相互依赖。运营和事件管理情景的演练应解决风险评估中发现的问题，并对风险管理程序进行压力测试，以识别潜在问题或弱点。演练的设计和实施方式应尽量减少对运营的干扰，并将人员、资产和信息暴露于最小的风险之中。

应定期（至少每年）进行演习，或在组织的使命和/或结构发生重大变化后，或外部环境发生重大变化后进行演习。每次演习后应编写正式报告。报告应评估组织的SOMS计划、过程和程序的适当性和有效性，包括不符合项，并提出纠正和预防措施。

运动后报告应成为最高管理层审查的一部分。

9.2 内部审计

9.2.1 组织应建立、实施和维护安全运营管理工作审核计划，并按计划的时间间隔进行内部审核，以提供有关SOMS是否：

a) 符合：

-组织自身对SOMS的要求；

-相关法律、法规、人权和合同义务；

—本国际标准的要求；

b) 得到有效和适当的实施和维护；

c) 表现符合预期；

d) 在实现组织的SOMS政策、目标和指标方面卓有成效。

9.2.2 组织应：

a) 制定、实施和维护审计计划（或多个计划），包括频率、方法、职责、规划要求和报告，应考虑相关流程和领域的现状和重要性以及以往审计的结果；

b) 定义审计标准、范围、频率、方法、职责、规划要求和每项审计的报告；

c) 选择审计员并进行审计，以确保审计过程的客观性和公正性（例如，审计员不应审计自己的工作）；

d) 确保将审计结果报告给相关管理层，以便对被审计领域进行管理；

e) 保留记录信息，作为审计计划和审计结果实施的证据。

负责审核区域的管理人员应确保采取行动，消除发现的不符合项及其原因，不应拖延。后续活动应包括对所采取行动的验证和验证结果的报告。

9.3 管理评审

9.3.1 将军

最高管理者应按计划的时间间隔审查组织的SOMS，以确保其持续的适宜性、充分性和有效性。此审查应包括评估改进机会以及对SOMS，包括SOMS政策和目标进行变更的需要。审查结果应明确记录，并保存记录。

管理评审应包括考虑：

a) 以往管理评审中采取的措施的状态；

b) 与SOMS相关的外部和内部问题的变化；

c) 安全运营绩效信息，包括以下方面的趋势：

-不符合项和纠正措施；

-监测和测量结果；

—审计结果；

d) 安全行动的影响；

e) 风险管理标准和控制；

f) 持续改进的机会。

管理评审的输出应包括与持续改进机会和SOMS变更需求相关的决定。组织应保留文件化信息，作为管理评审结果的证据。

9.3.2 评论输入

管理评审的输入应包括：

a) SOMS审计和审查的结果；

b) 利益相关方反馈；

c) 可用于组织以提高SOMS绩效和效率的技术、产品或程序；

d) 预防和纠正措施的状态；

e) 演习和测试的结果；

f) 在先前的风险评估中未充分解决的风险；

g) 事故报告；

h) 有效性测量结果；

i) 以往管理审查的后续行动；

j) 任何可能影响SOMS的改变；

k) 政策和目标的适当性

l） 改进建议。

9.3.3 评价输出

最高管理层评审的输出应包括与SOMS政策、目标、指标和其他要素可能变更相关的决策和行动，旨在促进持续改进，包括：

a） 提高SOMS的有效性；

b） 更新风险评估和风险管理计划；

c） 必要时修改影响风险的程序和控制，以应对可能影响SOMS的内部或外部事件；

d） 资源需求；

e） 改进控制有效性衡量方法。

10 改进

10.1 不合格和纠正措施

组织应建立、实施和保持处理不符合项以及采取纠正和预防措施的程序。

程序应规定识别和纠正不合格项以及采取措施减轻其后果的要求。

当出现不符合项时，组织应：

a） 对不符合项作出反应，并在适用的情况下：

-采取行动加以控制和纠正；

-处理后果；

b） 通过以下方式评估是否需要采取行动，以防止出现不符合项并消除不符合项的原因，从而避免不符合项再次出现或在其他地方出现：

-审查不合格情况；

-确定不合格的根本原因；

-确定是否存在类似的不合格情况，或可能发生此类情况；

c） 调查不合格项，确定其原因并采取措施避免再次发生；

d） 采取任何必要的适当行动，以避免其发生；

e） 审查所采取的任何纠正和预防措施的有效性；

f） 记录所采取的纠正和预防措施的结果；

g） 如有必要，对SOMS进行更改。

纠正措施应与遇到的不合格项的影响相适应。

组织应确保对SOMS文件进行拟议变更，并保留文件化信息作为以下证据：

-不符合项的性质以及随后采取的任何行动；

-任何纠正措施的结果。

10.2 持续改进

10.2.1 将军

组织应通过使用安全运营管理政策、目标、审核结果、监控事件分析、纠正和预防措施以及管理评审，持续改进SOMS的适宜性、充分性和有效性。

10.2.2 变更管理

组织应建立一个明确的、有文件记录的安全运营变更管理方案，以确保任何影响组织的内部或外部变更都与SOMS相关。组织应确定任何需要纳入SOMS变更管理方案的新关键活动。

10.2.3 改进机会

组织应监测、评价和利用SOMS绩效改进的机会，消除潜在问题的原因，包括：

a) 持续监测运营环境，以识别潜在问题和改进机会；

b) 确定并实施改善安保业务绩效所需的行动；

c) 审查为提高业绩而采取的行动的有效性。

所采取的措施应与潜在问题的影响以及组织的义务和资源现实相适应。

最高管理者应确保及时采取行动，利用改进机会。如果修订现有安排并引入可能影响运营和活动质量管理的新安排，组织应在实施前考虑相关风险。

审查结果和采取的措施应有明确的记录，应保存记录。后续活动应包括对所采取措施的验证以及验证结果的报告。

附件A

（信息性）关于使用本国际标准的指南

A.1 将军

本附录提供的附加文本旨在帮助理解本国际标准的要求。虽然本指南针对并符合这些要求，但在实施这些要求时，组织还需根据其风险评估和人权风险分析，考虑并实施适用于其范围、法律和合同义务以及运营环境的相关条款。本指南中与组织SOMS无关的部分需要在适用性声明中予以说明。

私营安保业务在保护公共、私营和非营利部门客户方面发挥着重要作用，这些客户在治理可能薄弱或因人为或自然事件而破坏法治的情况下开展业务。来自公共、私营和非政府组织（NGO）领域的客户，从执行或承包安全业务的组织那里获得广泛的服务，这些服务支持商业、人道主义、外交、发展和军事努力，并保护其他活动，包括基础设施重建。执行或承包安全业务的组织活动的范围和规模包括保护人员和物品，如车队、设施、指定地点、财产或其他场所（无论是否武装），以及其他需要组织人员在履行职责时携带或操作武器的活动。本国际标准为组织及其客户提供可审计的标准，以证明遵守人权和基本自由，并防止不当、非法和过度行为。

组织或承包安全运营的主要职责是确保客户能够在安全和有保障的环境中运作，同时完全遵守和支持人们在治理薄弱条件下保护自身和财产的基本且普遍的人权。在世界许多地方，这一基本权利正受到攻击。在很多情况下，这些攻击针对的是那些致力于减轻受影响人群苦难、恢复对个人和社会福祉至关重要的基础设施，或从事其他有助于人口长期稳定和发展活动的人们。这些攻击可能是为了即时的经济利益、政治动机，或是出于仇恨、偏见和/或报复。这些攻击不仅侵犯了暴力目标个体的基本权利，还影响了更广泛的人群，导致他们被剥夺食物、水、医疗、电力、就业和和平。通常，犯罪者会在平民中寻找掩护，利用无辜者来保护自己，常常使用恐吓和恐惧。当社区或有效当局缺乏广泛保护公民生命、权利和财产的能力——或者无法提供最低限度的安全保障，也无法将此类暴力行为的实施者绳之以法时，个人和组织可能会寻求商业安全服务提供商的帮助，以获得自卫的能力，防止发生严重威胁生命或造成严重身体伤害的犯罪行为。

本国际标准承认，开展或承包安保业务的组织在本质上不稳定和危险的环境中开展业务。本国际标准提供了管理与在治理薄弱或法治被人为或自然事件破坏的情况下开展业务相关的风险的原则和要求。本国际标准的目的是在确保尊重人权、法律和基本自由的框架内，提高和展示组织的专业水平，同时维护其运营和客户的安全。

组织在开展或委托安全运营时面临的挑战不仅限于事件响应和报告。组织应当参与一个全面且系统的过程，以预防性地管理与其运营相关的风险。这需要建立一个持续、动态且互动的管理流程，旨在促进尊重人权、法律和基本自由的文化，同时为客户提供支持其使命的服务水平。

尊重生命和人的尊严是本国际标准的核心原则。开展或委托安全运营的组织及其客户，有义务尊重内部和外部利益相关者（包括广大社区）的生命和尊严。通过使用本国际标准，组织可以更好地了解所面临的风险，并预先制定策略，以：

a) 管理对那些他们有合同义务保护的生命和财产构成的风险；

b) *支持2008年9月17日《关于武装冲突期间私营军事和安保公司运作的国际相关法律义务和良好做法的蒙特勒文件》、2010年11月9日《私营保安服务提供者国际行为准则》（ICoC）以及《工商企业与人权指导原则》的目标；执行联合国“保护、尊重和补救”框架2011；*

c) 表明对尊重人权、法律和基本自由的承诺、遵守和问责；

d) 降低风险，支持业务和运营任务；

e) 通过制定战略和行动计划，成功管理不良或破坏性事件，以保护其利益及其客户和其他利益相关者的利益。

对潜在的不良和破坏性事件进行适应性和预防性规划和准备，有助于降低事件的可能性和后果。整体管理过程可以帮助避免或最大限度地减少关键任务服务和运营的中断或暂停。

本国际标准为提供或承包安全操作的任何组织提供了指导或建议，以确定和制定最佳做法，协助和促进以下行动：

a) 降低其运营和供应链（包括分包商）中的风险；

b) 为保护有形和无形资产的战略提供由最高管理层推动的愿景和领导，同时尊重人权、法律和基本自由；

c) 识别和评估对其短期和长期成功至关重要的风险；

d) 最大限度地减少各种危险和威胁的可能性和后果；

e) 了解、提供和实施有关尊重人权的培训；

f) 了解保护资产和推进任务所需的角色和责任；

g) 管理事件响应措施和资源；

h) 制定、测试和维护事故预防和响应计划以及相关操作程序；

i) 制定和开展培训和演习，以支持和评估预防、保护、准备、减缓、应对、恢复和业务程序；

j) 制定和实施培训方案，以支持需要使用武力的行动；

k) 制定内部和外部沟通程序，包括对媒体或公众的信息请求作出回应；

l) 建立衡量和证明成功的指标；

m) 记录支持关键业务职能所需的关键资源、基础设施、任务和职责；

n) 建立流程，确保信息保持安全、及时和与不断变化的风险和运营环境相关。

管理体系的成功取决于组织内所有层级和职能的承诺，特别是最高管理层。决策者应准备好预算并确保获得必要的资源以实现这一目标。有必要建立适当的行政结构，以便有效处理预防、缓解和管理。这将确保所有相关方了解谁做出决策、决策如何实施以及所有代表组织工作的人员的角色和职责。本国际标准推动了组织内部的安全运营文化，其中所有安全活动都与尊重人权、法律和基本自由密不可分。

组织进行或委托安全运营的客户有固有的利益，确保这些组织遵守本国际标准的原则。因为一个组织的行为直接影响到其客户，特别是当客户是政府机构时。组织在进行或委托安全运营时，不当、非法和过度行为的后果可能包括令客户难堪、声誉风险和法律责任、扰乱关键的外交、援助和重建工作，以及增加威胁。因此，在委托这些组织的服务时，客户也有兴趣确保合同反映透明实施SOMS的情况。

A.2 人权和国际法

A.2.1概述

本条款中对人权和国际法的讨论是一个概括性的总结；在任何特定环境中开展安保行动之前，应寻求法律咨询意见。

有关适用的国际文书的引文，见参考书目。

A.2.2人权

A.2.2.1概述

在2008年9月17日《关于武装冲突期间私营军事和安保公司运作的国家相关国际法律义务和良好做法的蒙特勒文件》的基础上；《私营保安服务提供者国际行为准则》（ICoC）
9 2010年11月，以及《商业与人权指导原则》：实施联合国2011年3月21日的“保护、尊重和补救”框架，“人权”一词在此国际标准中出现时，指的是国际人权法中规定的所有人无歧视地享有的权利和自由。人权是普遍的，相互关联、相互依存、不可剥夺且不可分割。它们在国家法律和国际法律中都有明确规定。

为本国际标准的目的，开展或承包安保业务的组织应尊重所有人权，包括但不限于不可减损的人权，例如：

-生命权；

-免遭种族灭绝和危害人类罪；

-免受酷刑、残忍、不人道或有辱人格的待遇或处罚；

-从奴役、奴隶贸易和劳役中解放出来；

-正当程序、法律面前平等和公平审判的权利；

-免受刑法追溯适用的权利；

思想、良心和宗教自由的权利；

-免受歧视。

A.2.2.2自卫和保护他人

组织开展或承包安全行动的目的在于，在本质上不稳定和危险的情况下保障生命权，同时不侵犯其他人权。本国际标准认识到自卫对于保护生命权的根本重要性。自卫允许个人使用合理的武力来保护自己或他人。致命武力仅应在自卫或保护他人时使用，且必须是合理且必要的，以防止死亡或严重身体伤害。

A.2.3国际人道主义法

国际人道主义法（IHL）或武装冲突法（LOAC）是指管理战争或武装冲突的国际条约和习惯规则（战争法律和习俗）。为了本指南的目的，IHL和LOAC可以视为具有相同的意义。IHL定义了武装冲突中个人和国家的行为与责任。IHL的目标是通过保护未参与或不再参与敌对行动的人们，并限制战争的方法和手段，来减少战争造成的苦难。IHL的基本规则包括以下义务：

a) 采用有限的作战方法和手段；

b) 区分直接参与敌对行动者和平民（非战斗人员）；

c) 限制攻击仅限于军事目标；

d) 避免对平民和财产造成不必要的伤害；

e) 不伤害或杀害投降或不再参与战斗的对手；

f) 对不参与敌对行动的所有人（包括投降、受伤或生病的敌人）实行人道待遇；

g) 不得实施肉体或精神上的酷刑或残忍的惩罚。

《蒙特勒文件》第1部分第22至27段规定了特别适用于钙钛矿太阳能电池的国际法律义务。

在武装冲突期间，安全行动人员通常被视为国际人道法下的平民。作为平民，除非直接参与敌对行动，否则不得成为直接攻击的对象。根据本国际标准的规定，执行或承包安全行动的组织及其人员不得从事可能直接损害冲突各方军事行动或能力的行为，也不得参与战斗。这一限制通常意味着，安全行动人员不能攻击敌方武装力量或在敌方武装力量攻击下保卫军事目标而不失去其平民身份的保护。国际人道法并不禁止安全行动人员直接参与敌对行动。如果被俘，获准随军的安全行动人员不会因直接参与敌对行动而失去现有的战俘资格。但是，作为没有战斗特权的平民，安保行动人员可能要根据刑事和侵权法对他人造成的严重伤害或死亡或他们所犯的破坏财产的行为负责。

被俘的安全行动人员享有适当和人道的拘留条件。

自卫和保护他人免受非法攻击是固有的权利，不直接参与敌对行动。即使攻击者（们）是某国武装部队成员，只要这种攻击违反国际人道法，自卫权仍然适用。安全行动人员使用武力抵抗非法攻击并不会丧失其作为平民的保护地位。然而，针对合法攻击（例如，武装冲突一方对敌方军事目标的攻击）的防御性火力或以其他方式抵抗，可能被视为直接参与敌对行动，这会导致在该行动期间失去保护地位。

安全行动人员可因严重违反国际法，例如战争罪和危害人类罪而被起诉和定罪，这些罪行具有域外管辖权，适用程度不一，一些国家和国际组织提倡对这些罪行实行普遍管辖权。根据这一概念，被指控犯有此类罪行的人可以在任何国家、由任何法官审理。安保人员的主管、经理和监督者也可能因下属在其有效管辖下的犯罪行为而承担责任，无论是由于他们下达的命令或指示，还是安保监督者未能对其人员行使适当控制。公司也可能根据不断发展的刑法或侵权法被追究责任。

根据风险评估，建议组织咨询适当的法律顾问，以获得解释和不断发展的法律。在武装冲突条件下运作的组织应为代表其工作的人员提供更全面的培训，包括但不限于：

a) 自卫/保护他人与直接参与敌对行动之间的区别；

b) 具体的个人罪行，如酷刑和其他不人道待遇，可作为战争罪或危害人类罪指控他们；

c) 在国际和非国际武装冲突中使用武力的具体考虑，包括国际武装冲突与非国际性武装冲突之间的区别以及各种交战方和非国家武装团体的地位；

d) 武力使用程序与武装部队特有的交战规则之间的区别；

e) 组织及其代表人员可能被视为交战方或被编入武装部队的情况。

A.2.4习惯国际法

习惯国际法是指各国基于法律要求而采取行动的一致行为所衍生的法律规则。习惯国际法的要素包括：各国长期重复类似的国际行为（国家实践）、这些行为出于义务感发生，以及被大量国家接受。

习惯国际法对所有国家都具有约束力，无论它们是否是某一条约或公约的缔约方。上述多项人权如今被视为习惯国际法。关于国际人道法，涵盖国际武装冲突的法律中许多重要部分仍属于习惯法而非条约法。国际人道法在非国际武装冲突中的大部分适用问题属于习惯国际法。与武装冲突中的平民身份及直接参与敌对行动相关的问题仍在不断涌现，成为习惯法的一部分，并直接影响组织的活动。

A.2.5国际人权法

国际人权法是指旨在促进和保护人权的国际法体系，由各国之间的条约和协议组成。国际人权法对国家及其代理人具有约束力。国际人权标准具有强制执行力。

通过国家法律和各种国际和地区法院及法庭，以及联合国宪章和条约机制。《国际人权法公约》中所述的原则旨在指导本组织制定和执行符合国际人权法目标的政策和程序。

A.3 管理体系方法

管理系统是一个动态且多方面的过程，每个元素作为功能单元的结构集合相互作用。它提供了一个框架，基于这样的前提：系统的组成部分只有在相互关系及其与其他系统的关系中才能得到最好的理解，而不能孤立地看待。要全面理解和实施管理系统的各个要素，就必须将部分与整体联系起来理解。这导致了一个迭代过程，在这个过程中，建立背景和政策、风险评估、实施、运行、评价和审查并不是一系列连续的步骤，而是一个相互作用的功能网络。

管理系统方法的特点是：

a) 了解系统运行的上下文和环境；

b) 确定系统的核心元素以及系统边界；

c) 了解系统中每个元素的作用或功能；

d) 理解系统元素之间的动态交互。

系统方法确保了整体策略和政策的制定。它为在组织运营的复杂多变环境中实施的战略和政策提供了坚实的分析基础。建立一个评估策略和政策风险及有效性的框架，在实施前和实施过程中提供反馈循环，贯穿整个决策过程。

A.4 组织背景

A.4.1理解组织及其背景

A.4.1.1概述

为了管理风险和促进尊重人权的文化，本组织要求了解和理解可能影响其安保行动并影响利益攸关方的内部和外部因素。

组织通过识别和理解其内部和外部影响及环境来建立其SOMS的背景。通过建立这一背景，组织可以界定其SOMS的范围，并设计一个适合其安全运营管理的框架。这有助于确保组织满足内部和外部利益相关者的目标、需求和关切。背景将决定管理组织、客户及受影响社区风险的标准，从而为设定风险评估和处理过程的风险标准和参数提供基础。

在建立内部和外部环境的过程中，组织应确定组织的重要有形资产和无形资产。这包括确定各种类型资产对组织的生存能力和成功的重要性。

A.4.1.2内部环境

在确定组织内部环境时，必须考虑：

a) 影响组织安全运营和运营环境的内部因素；

b) 内部利益相关者，他们是风险制造者和风险承担者；

c) 受风险影响的内部利益相关者；

d) 影响风险接受的因素。

A.4.1.3外部环境

在确定组织的外部环境时，必须考虑：

a) 与行业部门和运营环境相关的风险因素；

b) 影响组织安全运营和运营环境的外部因素；

c) 外部利益相关者，他们是风险制造者和风险承担者；

d) 受到与安全操作相关的风险影响的外部利益相关者；

e) 影响外部利益相关者接受风险的因素。

A.4.1.4供应链和分包商映射和分析

管理供应链中的风险，包括分包商和合同下的当地部队，需要了解这些实体的文化和环境以及其供应链的端到端背景。组织供应链的每个节点都涉及一组需要管理的风险和管理流程。

供应链和分包商的使用是安全操作的组成部分。虽然供应链内部存在显著的相互依赖性，但供应链中的每个单独节点在某些方面都是独特的；这种独特性可能需要对所涉及的风险采取定制的方法进行管理。因此，为了管理供应链内的风险，组织需要确定：

a) 组织和个人在其上游和下游供应链或网络的每一层或级别上的作用；

b) 了解对任务成功至关重要的相互依赖性和支持性基础设施；

c) 每个节点如何直接或间接地为链中其他成员的性能增加价值；

d) 确定每个节点都有潜力对组织的风险状况产生正面和负面的影响；

e) 评估每个节点在实施管理体系过程中对风险最小化成功的影响。

在进行节点分析时，组织应认识到单个节点所作的决策可能对整个供应链产生影响。因此，需要了解并控制整个供应链中的风险因素，以成功实施SOMS。

A.4.1.5定义风险标准

组织应了解并定义其评估风险重要性的标准。风险标准应反映组织的价值观、目标和资源，以及安全操作的背景。风险标准将确定衡量风险因素和处理风险需求的基准。

A.4.2理解利益相关方的需求和期望

组织应确定并维护与组织的运营和本国际标准要求相关的利益相关方的登记册，并记录

与利益相关者的互动。组织应考虑相关利益相关者的要求、看法、价值观、需求、利益和风险承受能力。

相关利益方包括但不限于：

a) 客户和顾客；

b) 最终用户

c) 供应链和外包合作伙伴；

d) 负责国内安全和私人保安业务许可或授权及监管的主管法律当局；

e) 本国际标准适用范围内的当地社区（例如，正在执行安全操作的社区）；

f) 本组织雇用的或本组织采购物资和其他资产的外籍人员的状态；

g) 在经营环境中非政府组织和国际组织；

h) 组织人员；

i) 大众传播媒介

A.4.3确定安保业务管理系统的范围

组织定义实施其SOMS的边界。它可以选择在整个组织、特定运营单位、离散地理位置或明确界定的供应链流中实施SOMS。这些范围界定反映了SOMS的最高管理层目标以及组织及其活动的规模、性质和复杂性。一旦最高管理层确定了SOMS的范围，该范围内的所有资产、活动、产品和服务都将成为SOMS关注的要素。

组织应使用风险评估来证明任何排除在SOMS范围之外的理由。排除可能包括组织无法控制某些服务或运营；然而，排除并不免除组织尊重人权、法律和基本自由的责任。范围应确保组织及其客户的运营完整性。SOMS的可信度取决于范围中定义的组织边界的选择。

组织在各种环境进行安全操作，风险因素各不相同。根据安全操作和风险评估的背景，适用性声明应记录本附录中适用于在定义范围内建立和实施SOMS的相关条款。

外包和分包活动仍由组织负责，并应在SOMS范围内。如果外包或分包的产品、服务、活动或组织供应链的一部分仍受组织的风险责任和管理控制，那么最高管理层应将其纳入SOMS的范围。组织应与分包商和外包合作伙伴达成适当协议并采取适当措施，以确保有效的安全管理协议到位。

SOMS的详细程度和复杂性、所需文档的程度以及投入的资源应指导SOMS范围声明。当组织为特定运营单位实施此国际标准时，该组织可以使用其他部门制定的相关政策、计划和程序来满足此国际标准的要求。

A.4.4安保业务管理系统

本国际标准规定的SOMS的实施预期产生以下结果：

a) 改善安保行动和服务提供；

b) 内部和外部利益相关者的安全和保障；

c) 尊重人权、法律和基本自由的文化；

d) 示范如何落实《国际行为准则》的原则和承诺。

本国际标准基于组织将监控、审查和评估其SOMS的前提，以识别持续改进的机会以及实施纠正和预防措施。该持续改进过程的频率、范围和时间尺度由组织根据不断变化的风险环境、经济及其他情况确定。本国际标准要求组织：

a) 制定适当的安全操作管理政策；

b) 评估和管理与组织安全操作相关的风险；

c) 确定组织遵守的适用法律要求和其他要求；

d) 确定优先事项并设定适当的安全运营管理和目标；

e) 建立结构和方案，以执行政策、实现目标和达到指标；

f) 促进计划、控制、监控、预防和纠正措施以及审计和审查活动，以确保遵守政策并使SOMS保持适当；

g) 能够适应不断变化的环境。

A.5 领导

A.5.1领导和承诺

A.5.1.1概述

组织的最高管理层（如总经理或首席执行官）应表现出实施SOMS的决心和承诺。没有最高管理层的承诺，任何管理体系都无法成功。最高管理层应向其内部和外部利益相关者展示，在提供安全运营时，对人权、法律和基本自由的尊重。为了启动并持续SOMS工作，最高管理层应向所有代表组织工作的人员传达以下重要性：

a) 在组织所做的一切工作中培养组织和个人执行安全行动的能力；

b) 尊重人权、法律和基本自由是所有安全行动的组成部分；

c) 在整个组织中集成安全管理；

d) 把问题看作是改进的机会。

最高管理层应通过以下方式提供其致力于SOMS的制定和实施并持续改进其有效性的证据：

a) 在整个组织内传达满足本国际标准要求的重要性；

b) 制定和传达政策和风险标准；

c) 确保在所有级别和职能中确立安全业务目标；

d) 确保相关管理体系角色的职责和权限在组织内部分配和传达；

e) 为管理体系分配适当的资源；

f) 确保代表本组织工作的人员的胜任能力和培训；

g) 表明对管理体系和风险最小化的承诺；

h) 在整个组织内提高对风险和SOMS要求的认识；

i) 以身作则；

j) 参与评审并推动持续改进过程。

组织的最高管理层必须赞助、提供必要的资源并负责创建、维护、测试和实施全面的SOMS。这将确保组织内各级管理层和员工明白，SOMS是关键的高层管理优先事项。同样重要的是，高层管理应采取“自上而下”的方法来处理SOMS：使组织各层级的管理层都认识到系统维护的责任是整体治理重点的一部分。

A.5.1.2符合性声明

符合性声明确立并传达了最高管理层的承诺，即通过实施本国际标准的要求和以下内容，开展与组织尊重人权的责任相一致的安全运营：

a) *《私营保安服务提供者行为守则国际准则》；*

b) *蒙特勒关于武装冲突期间私营军事和安保公司运作相关的国际法律义务和良好做法的文件；*

c) *《工商业与人权指导原则》；《联合国“保护、尊重和补救”框架2011年执行情况》；*

d) 任何其他适用的国际公认的人权标准。

A.5.2政策

安全运营策略是实施和改进组织的SOMS的驱动因素。因此，该策略应反映高层管理对以下方面的承诺：

a) 将尊重人的生命和尊严作为首要任务；

b) 避免、预防和减少破坏性事件和不良事件的可能性和后果；

c) 遵守适用的法律要求和其他要求；

d) 尊重人权；

e) 持续改进

安全运营政策是组织设定目标和指标的基础框架。该政策应足够清晰，以便内部和外部利益相关者能够理解，并应定期审查和修订，以反映变化的情况和信息。其适用范围（即范围）应明确可辨，并应反映其活动、功能、产品和服务所面临风险的独特性质、规模和影响。

安全运营政策应传达给所有为组织工作或代表组织工作的人员，包括客户、供应链合作伙伴、分包商和当地社区的相关成员。向分包商和其他外部方传达可以采用不同于政策声明的形式，如规则、指令和程序。组织的安全运营政策应由其最高管理层在所属更广泛的企业机构的安全运营政策框架内定义并记录，并获得该机构的认可。

A.5.3.组织机构、职责和权限

风险管理不仅是高层管理的责任。为了使SOMS有效运作，需要每一位代表组织工作的人员共同参与。这是一种自上而下、自下而上的方法。保护人权和管理风险必须成为组织文化的一部分。因此，所有制造风险和承担风险的人都应该是风险管理者的角色。因此，代表组织工作的人员在SOMS范围内所承担的角色、职责和权限应明确界定并传达。

管理体系由组织内部人员实施。应任命并授权一名或多名合格人员来执行、测试或维护SOMS。最高管理层应定期审查和审计整体SOMS。可任命一个安全运营管理和规划团队，包括来自所有主要职能和支持部门的高级领导，以确保SOMS得到广泛接受。

A.6 规划

A.6.1应对风险和机遇的行动

A.6.1.1概述

组织在开展或承包安全业务时，本质上是在不确定性和风险的环境中运作。他们需要管理对客户的风险，同时也要管理对组织及其受影响的利益相关者和社区的风险。组织需要在其保护客户、代表客户工作的人员以及当地社区的生命和财产安全的背景下，实现其战术、运营和业务目标，同时尊重人权。尊重权利为企业创造价值，因此本质上是一个需要进行人权尽职调查以完成运营使命的业务目标，同时尊重人权并遵守当地、国家和国际法律。挑战在于评估、评价和处理风险，以便以成本效益的方式管理风险和不确定性，同时满足组织和客户的战略和运营目标。风险评估提供了对风险环境的清晰理解，使组织能够识别风险并做出明智的决策，优先处理其风险。

风险评估过程旨在让组织了解内部和外部利益相关者可能影响其运营和业务目标实现的风险。它旨在创建一个系统化的过程，帮助组织识别、分析和评估风险，确定哪些风险对组织及其利益相关者具有重要意义。风险评估为评估现有控制措施的充分性和有效性提供了基础，并为决定最合适的管理与处理风险的方法提供依据。它还确定了组织SOMS应优先解决的风险。风险评估为设定管理体系内的目标、指标和计划奠定了基础，同时也用于衡量SOMS的有效性。

A.6.1.2法律和其他要求

A.6.1.2.1概述

组织应识别并理解影响其目标实现的法律、法规和合同要求。这些要求可能包括地方、国家和国际层面的，以及法律和监管要求。识别并理解这些要求有助于确保合法合规，防止诉讼，减少责任，提升组织形象，并增强组织向客户提供负责任保护服务的能力。

组织应建立、实施并纳入其流程的措施，以识别、遵守和评估适用的法律和自愿要求，包括（但不限于）：

a) 适用于其活动和运营以及本国际标准适用范围内的任何分包商或合资企业活动和运营的相关当地、国家和国际法律、法规和其他要求；

b) 相关的国际人道主义法和人权法，包括但不限于禁止酷刑或其他残忍、不人道或有辱人格的待遇；提高认识并禁止性剥削和性虐待或基于性别的暴力，承认并防止人口贩运和奴役；

c) 适用的国际和国家就业和环境法律和法规；

d) 打击贿赂、腐败和类似犯罪的国际和国家措施；

e) 遵守当地、国家和国际法律的程序，涉及采购、发放和转运枪支（以及用于安全行动的其他管制物品，如防弹衣和炸药）；

f) *组织所加入的任何自愿性准则或公约，包括联合国《工商企业与人权指导原则》（UNGPs）、《私营保安服务提供者国际行为准则》（ICOC）和《安全与人权自愿原则》（VPs）。*

组织可遵守的其他要求示例包括：

a) 商业和其他合同义务；

b) 与公共当局、社区团体或非政府组织达成的协议；

c) 与客户的协议；

d) 非监管性指南；

e) 自愿原则或行为守则；

f) 产品或服务管理承诺（例如：保修）；

g) 行业协会的要求；

h) 组织或其母组织的公开承诺；

i) 非约束性协议；

j) 医疗保健要求；

k) 财务义务；

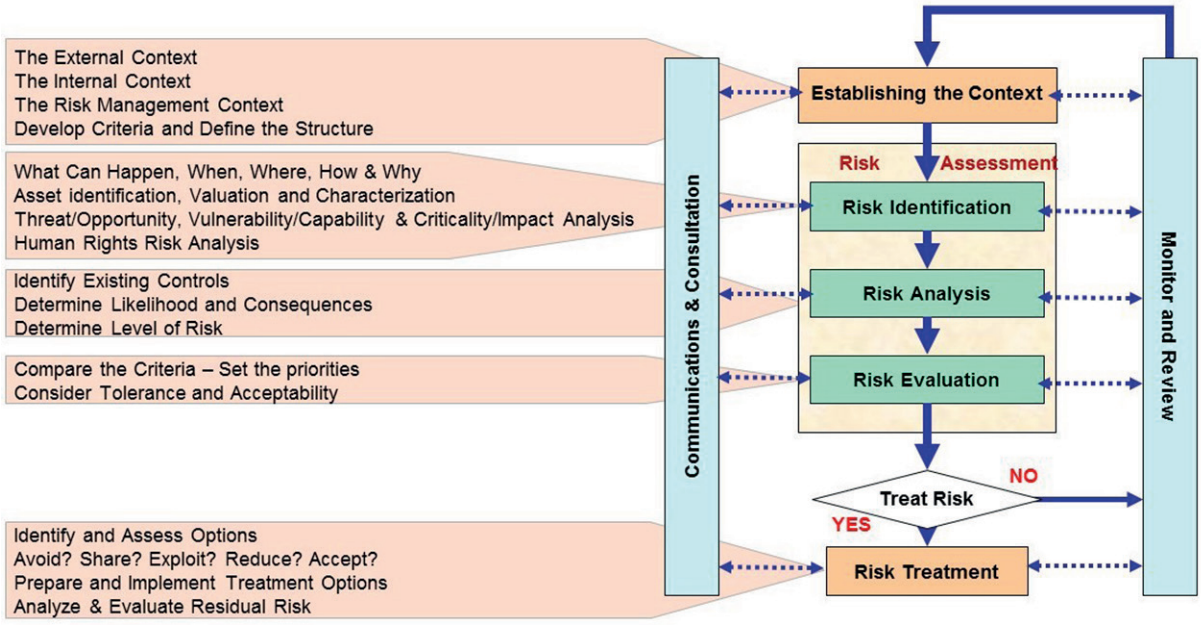
l) 社会责任和环境承诺；

m) 身份信息、保密和隐私要求。

《蒙特勒文件》第一部分E段总结了适用于组织及其人员开展或承包安保业务的相关国际法律义务。具体的法律义务因管辖区域、地理位置、业务类型和性质以及组织客户的位置、类型和性质而异。因此，组织必须了解其在运营环境中的义务。组织应定义并记录具体的运营控制措施及个人责任，以满足这些要求。

A.6.1.2.2 ISO 31000所述的风险评估过程

组织应采用ISO 31000中实施原则和指南，如图A.1所示。



注：来源：ASIS国际。

图A.1-管理风险的流程，包括对人权产生不利影响的风险

风险评估过程在组织的内部和外部环境中进行。

风险评估是风险识别、风险分析和风险评价的总体过程，如下所述。

a) 风险识别：通过威胁分析、重要性分析、脆弱性分析和人权风险分析，识别、分级和记录风险的过程。该过程考虑了风险的原因和来源，以及可能影响组织及其利益相关者的事件、情况和环境。

   识别应包括所有可能阻碍组织实现其业务、战术和运营目标的风险来源，包括客户、代表组织工作的人员以及其他内部和外部利益相关者的权利、安全和保障。

b) 风险分析：了解风险和风险程度的过程。它为确定哪些风险应该处理以及处理这些风险的最适当方法提供了基础。

它考虑了风险的原因和来源、后果（包括严重程度）以及事件及其相关后果发生的可能性。组织应确定如果威胁变为现实，事件对利益相关者的影响。风险水平是可能性、严重程度和后果的函数，为优先处理需要解决的风险提供了依据；

c) 风险评估：将估计的风险水平与在确定上下文时定义的风险标准进行比较的过程。它决定了风险水平和类型的重要性。风险评估利用在风险分析中获得的风险理解，来决定所需的风险优先级、控制和处理策略。

A.6.1.2.3人权风险分析

人权风险分析是识别、评估和记录与人权相关的风险及其影响的过程，旨在管理风险并减轻或防止不利的人权影响和法律违规行为。有时也称为“人权风险评估”或“人权影响评估”。人权风险分析应评估风险的正面和负面结果。负面后果根据其严重程度进行分级和优先排序。评估风险的正面结果可能为改善利益相关者的风险环境提供机会。人权风险分析是整体风险评估过程的重要组成部分。

进行彻底的人权风险分析，为查明、评估、管理和记录风险提供了基础，以防止、减轻和说明侵犯人权和违反法律行为，并构成必要的尽职调查的一部分，以避免本组织卷入侵犯人权和违反法律行为。各组织应查明与其活动有关或直接与它们的业务关系及其潜在来源有关的潜在和实际人权风险，并应分析其可能性、严重性和后果，以便确定风险的优先次序，并采取适当措施预防、减轻和处理这些风险。

人权风险分析过程：

a) 评估与组织安全运营活动直接相关并与其客户、分包商、外包合作伙伴、供应链和其他业务关系相关的风险；

b) 包括与受风险和相关活动影响的内部和外部利益相关者进行沟通和有意义的协商；

c) 确定并获得进行人权风险分析和证明评估人权风险过程的彻底性所需的人权专门知识和能力；

d) 记录风险评估过程，以便进行审查、整合和根据调查结果采取行动、跟踪应对措施的有效性、外部沟通以及报告如何处理影响以及诉讼保护。

A.6.1.2.4风险评估过程注意事项

风险评估提供了对风险、其原因、可能性、严重性和后果的理解。因此，组织应在SOMS范围内进行全面的风险评估，考虑与以下方面相关的输入和输出（预期和非预期）：

a) 其活动、产品和服务；

b) 与环境和社区的互动；

c) 与内部和外部利益相关者的联系；

d) 基础设施和相互依赖。

风险评估应包括对成功实现组织使命和尊重所有利益相关者权利的不确定性进行详细分析和评估，例如（但不限于）以下方面：

a) 与特派团和行动有关的战术风险；

b) 与组织和客户声誉相关的风险；

c) 本组织活动的政治、经济和社会影响；

d) 对代表本组织工作的人员的威胁和后果；

e) 对当地社区和其他利益攸关方的威胁和后果，以及业务活动对其人权的潜在影响；

f) 与业务关系相关的风险，例如使用分包商、外包合作伙伴以及与其他从事安全运营的组织的互动；

g) 战术和作战风险之间的相互关系以及尊重人类生命和权利的必要性。

风险评估存在多种方法。组织应建立、实施和保持正式的方法，该方法应有文件记录并可重复。假设、范围、评价标准和结果应由最高管理层明确界定和审查。

由于一个组织可能面临多种风险，因此应建立并记录标准和方法，以确定其认为重要的风险。确定重大风险没有单一的方法。然而，所使用的方法应提供一致的结果，并包括评估标准的建立和应用，例如与保护生命和人权、不利人权影响的严重性、防止或减轻不利影响的能力、活动和功能的关键性、法律问题以及内部和外部利益相关者的关切相关的标准。组织应分析破坏性和不利事件对其运营和利益相关者的影响的可能性、严重性和后果，并确定关键操作，这些操作被赋予高优先级，用于制定响应和恢复时间及目标。

在评估后果时，组织应考虑以下方面。

a) 人的代价：对客户、代表客户工作的人员、供应商、当地社区和其他利益相关者的身体和心理伤害。

b) 财务成本：设备和财产更换、停机时间、加班费、库存贬值、销售/业务损失、诉讼、监管罚款/处罚等。

c) 形象成本：声誉、在社区的地位、负面报道、失去客户等。

d) 人权影响：在具体业务范围内对特定个人和群体，特别是脆弱或边缘化群体的实际和潜在不利人权影响。

e) 间接影响：对区域经济的影响，对区域净经济的影响等。

f) 环境影响：对环境质量或濒危物种的退化。

风险评估是一个包容性进程，利用必要的内部和外部人权专门知识，并与包括可能受到不利影响的利益攸关方在内的内部和外部利益攸关方进行有意义的协商。风险和影响的识别、分析和评价过程是在组织的经营环境中进行的，因此，应考虑内部和外部背景以及法律和其他要求。

为了准确反映组织的风险状况，风险评估所需的数据应由一支训练有素的团队收集，包括适当资格认证的人权专家。选择用于收集行政、财务、技术、社会和物理数据的抽样方法时，应确保样本具有代表性。风险评估并非一门精确的科学，因此，假设和信息的可靠性应予以记录。在数据收集过程中，应直接咨询组织内所有受SOMS管辖的操作单位。风险评估的结果应由高层管理报告并审查，以确立安全运营管理的目标、指标和策略。组织应根据以下因素定义风险评估的范围：

a) SOMS范围（产品、服务和活动）；

b) 客户期望和义务；

c) 法律、法规和合同要求；

d) 尊重人权的责任；

e) 受影响社区和利益相关者的期望；

f) 风险偏好

g) 业务关系、相互依赖性和基础设施要求；

h) 数据/信息要求。

风险评估过程应考虑正常和异常操作条件，以及合理可预见的破坏性情况，以更好地控制破坏性和不良事件。然而，不可能预见所有破坏性和不良情况，因此组织还应考虑事件对关键资产、活动和功能的影响，以及受影响社区和利益相关者的后果，无论事件性质如何，以便预先管理其风险。

风险评估应：

a) 使用记录在案的定量和/或定性方法来估计已识别潜在风险的可能性或概率，以及如果事件发生其后果的重要性；

b) 应基于合理且明确的标准；

c) 对其业务中认识到的所有潜在风险给予适当考虑；

d) 考虑其对其他方的依赖以及其它方对组织的依赖，包括客户、社区、业务关系和供应链依赖及义务；

e) 评估管理组织活动的法律义务和其他义务以及自愿承诺的后果；

f) 考虑与利益相关者、承包商、外包合作伙伴、供应商和其他受影响方相关的风险；

g) 分析风险信息，选择可能造成重大后果的风险和/或后果难以确定其重要性的风险；

h) 分析和评估管理风险所需的成本、效益和资源；

i) 评估其可以通过杠杆控制和影响的风险和影响。

注：组织确定控制程度及其风险接受、规避、管理、最小化、容忍转移和/或处理策略。

在某些地方，关键基础设施、社区资产和文化遗产可能是组织运作环境中的重要因素，因此在了解其风险和对环境的影响时应考虑到这些因素。

在开发与其重大风险有关的信息时，组织应考虑保留信息以供历史用途的必要性，并设计和实施其SOMS。

风险识别和评估过程应考虑活动的地点、分析的成本和时间以及可靠数据的可用性。此过程中可使用为业务规划、监管或其他目的而开发的信息。

组织应定期重新评估活动的整个生命周期，以应对组织运营、运营环境的变化以及事件。可能需要重新评估的变化包括：

a) 合同和行业趋势；

b) 业务关系；

c) 新的活动和业务上的重大变化；

b) 监管要求；

c) 政治环境

d) 事件导致的情况；

e) 基于性能的测试/演习结果。

识别和评估风险的过程并不打算改变或增加组织的法律义务。

A.6.1.3内部和外部风险沟通与协商

组织应与相关利益相关方建立正式的沟通和协商程序，以便收集风险评估输入信息和受控传播结果。在风险沟通和协商过程中应考虑信息的敏感性和完整性。

A.6.2安保业务目标和实现这些目标的规划

A.6.2.1概述

目标和指标的设定旨在实现组织安全运营政策的目标和承诺。通过设定安全运营的目标和指标，组织可以将政策转化为其在安全运营策略中描述的行动计划。这些目标和指标应当具体且可衡量，以便跟踪进展并评估SOMS在提高整体组织准备情况方面的表现。

SOMS“目标”是最重要的考虑因素，例如减少事故。安全运营“目标”是基于关键绩效指标来衡量性能的具体度量。目标和目标应根据风险评估适合组织。
目标和指标应反映组织的业务、绩效以及期望实现的目标。适当的管理层应确定目标和指标。目标和指标应定期审查和修订。

当设定目标和指标时，组织应考虑建立可衡量的安全运营关键绩效指标。这些指标可作为安全运营绩效评估系统的基础，并可提供有关SOMS和特定预防、缓解、响应和恢复策略的信息。

在确定其目标和指标时，组织应考虑：

a) 政策承诺；

b) 与战略目标保持一致；

c) 风险评估结果；

d) 风险偏好和容忍度；

e) 法律和其他要求；

f) 内部和外部环境；

g) 性能标准

h) 基础设施要求和相互依赖性；

i) 利益相关者的利益；

j) 技术选择；

k) 财务、运营和其他组织考虑因素；

l) 实现目标所需采取的行动、资源和时间表。

在考虑技术选择时，组织应考虑在经济上可行、成本效益高且被认为适当的条件下使用最佳可用技术。

提及本组织的经费需要，并不意味着本组织必须采用特定的成本会计方法，但本组织可选择考虑直接、间接和隐性费用。

A.6.2.2实现安全运营和风险处理目标

安全运营策略和行动计划是实现组织目标和指标的记录方法。战略应与其他组织计划、战略和预算协调或整合，行动计划可细分为组织运营的具体要素。

要成功管理安全操作，策略和行动计划应定义：

a) 实现目标的责任（谁来做？在哪里做？）；

b) 实现目标的手段和资源（如何做到？）；

c) 实现这些目标的时间框架（何时完成？）。

这些战略可以细分为针对组织运营的具体要素。只要每个文件化计划中都充分定义了关键职责、战术步骤、资源需求和时间表，组织就可以使用多个行动计划。

在适当和可行的情况下，战略应包括考虑组织与规划、设计、施工、调试、运营、改造、生产、营销、外包和退役有关的所有活动阶段。战略制定可针对当前活动和新活动、产品和/或服务进行。

本组织的规划应考虑到活动的优先次序、合同义务、雇员和邻近社区的需要以及业务连续性。

战略应具有动态性，并在以下情况下进行监测和修改：

a) 风险评估变更的结果；

b) 修改或增加目标和指标；

c) 引入或变更相关法律要求；

d) 在实现目标和指标方面取得了实质性进展（或没有取得）；

e) 活动、产品、服务、流程或设施发生变化或其他问题出现。

确定安全运营策略使组织能够评估一系列选项。组织可以选择适合每项活动的适当方法，以便能够以可接受的水平运行。最合适的策略或策略组合应取决于一系列因素，例如：

a) 组织风险评估的结果；

b) 实施一项或多项战略的成本；

c) 不作为的后果。

最高管理层应批准文件化战略，以确认已适当确定安全运营战略，这些战略已解决不良或破坏性事件的可能原因和影响，并且所选战略适合于在组织的风险承受范围内实现组织目标。

策略还应考虑组织与外部利益相关者的关系、相互依赖性和义务。这些利益相关者包括客户、供应商和外包合作伙伴——以及公共机构和其他社区成员。组织应制定并维护首先保护利益相关者生命安全的战略，同时尊重人权并保持产品和服务交付的完整性。此外，与公共机构和其他社区成员的互动和协调应在战略制定中确定并纳入。这些与外部利益相关者的战略安排应支持实现安全运营目标，并且要明确界定和记录。

A.7 支助

A.7.1资源

A.7.1.1概述

应查明SOMS所需资源，包括人力资源和专门技能、设备、内部基础设施、技术、信息、情报和财政资源。最高管理者应确保提供必要的资源，以建立、实施、控制、测试和维护SOMS。

A.7.1.2结构要求

A.7.1.2.1概述

合同是客户与承包商之间关系的主要法律依据，订立合同的组织应为法人实体，且该组织的签字人应明确授权代表该组织订立合同。

A.7.1.2.2组织结构

本组织应建立一个管理结构，明确界定履行合同义务所必需的职责、责任和问责制。

A.7.1.2.3保险

组织应寻求足够的保险覆盖，以满足因个人伤害、死亡或财产损失而产生的任何责任，这需与其风险评估相符。此类保险的限额至少应达到客户规定的最低水平或行业公认的最高标准。保险应包括雇主责任险和公众责任险。外籍和本地员工应根据其工资结构和服务风险水平，依法提供相应的健康和人寿保险政策。

在寻求保险覆盖范围时，组织应考虑：

a) 组织应持有的政策和限制应在合同中明确规定；

b) 保单的管辖权以及在发生争议时；

c) 领土限制；

d) 赔偿的限制；

e) 涵盖所有活动，包括武器的使用；

f) 为代表本组织工作的人员和受影响社区提供医疗保险和治疗；

g) 分包商的活动；

h) 保护客户。

需要考虑的保险范围包括（但不限于）：

a) 责任

b) 劳工灾害补偿

c) 事故

d) 物产遭受的损害

e) 绑架、勒索和/或囚禁；

f) 关键人物

A.7.1.2.4外包和分包

合同应提供承包商和分包商之间关系的法律依据。组织负责外包给其他实体的所有活动。合同应规定分包商履行职责、条款和条件。

A.7.1.2.5财务和行政程序及控制

一个组织为支持提供有效的安全和风险管理而制定的财务和行政程序及控制措施也应处理突出的财务风险。

A.7.2能力

组织应确定任何具有代表其执行任务的责任和权力的人员所需的认识、知识、理解和技能，包括：

a) 为可能受到不良或破坏性事件影响的内部和外部利益相关者制定培训和意识提升计划：

b) 要求代表其工作的分包商能够证明其员工具备必要的能力和/或适当的培训：

c) 确定为确保对执行专门SOMS管理活动负有书面责任的人员的能力而必需的经验、能力和培训水平；

d) 应持续不断地监测和重新评估培训水平，以确定改进机会。

组织有责任确保所有代表组织工作的人员，在部署前和持续过程中，都接受充分培训，以履行其职责并遵守相关的当地、国家以及人道主义和人权法律。培训目标应基于风险评估，并促进培训要求的统一性和标准化。培训应特别包括关于关键主题的人权培训，例如：

a) 禁止酷刑和其他残忍、不人道或有辱人格的待遇；

b) 禁止和提高认识性剥削和性虐待或基于性别的暴力；

c) 承认和防止人口贩运和奴役。

组织应识别和评估执行安全操作活动所需的能力与执行该活动所需的个人所拥有的能力之间的任何差异。这种差异可以通过额外的教育、培训或技能发展计划来纠正，该计划可能包括以下步骤：

a) 能力与培训需求的确定；

b) 设计和制定培训计划，以满足规定的胜任力和培训需求；

c) 选择合适的方法和材料；

d) 验证是否符合SOMS培训要求；

e) 目标群体的培训；

f) 记录和监测所接受的培训；

g) 根据规定的培训需求和要求，对所接受的培训进行评估；

h) 根据需要改进培训方案。

培训可能包括一般性主题和特定任务及背景主题，为人员在特定合同和特定情况下执行任务做好准备。一般主题包括但不限于：

a) 使用武力程序和火器；

b) 人道主义法和人权法；

c) 宗教、性别和文化问题，以及对当地人口的尊重；

d) 处理平民的投诉：特别是将这些投诉转交有关当局；

e) 打击贿赂、腐败和其他相关犯罪的措施。

任务和上下文特定主题的示例可能包括：

a) 战术驾驶

b) 面谈技巧

c) 地面导航

d) 电子通信

e) 医疗救助

f) 社区联络员；

g) 伤员后送按分级救治原则

h) 合同条款或组织提供的服务项下的其他明示和暗示的任务。

组织应采用实用的情境驱动培训，要求受训人员在模拟安全人员执行任务时可能遇到的情况中做出决策，并应对这些决策的后果。国际人道法培训应针对组织在武装冲突条件下所面临的特定条件进行设计。培训将重点放在组织的平民身份、可能导致该身份丧失的活动后果，以及违反国际人道法或国际人权法的个人责任。

培训和提高认识方案可包括：

a) 与全组织工作人员就安保业务管理方案的实施进行协商；

b) 在组织的通讯、简报、入职培训或期刊（包括新员工入职培训）中讨论安全运营管理；

c) 在相关网页或内部网上包含安全操作管理；

d) 在线培训模块，存储在组织的学习管理系统中；

e) 通过行动后报告从内部和外部事件中学习；

f) 将安全运营管理工作作为管理团队会议的一项内容；

g) 会议和课堂培训；

h) 急救和其他实践培训。

所有人员都应接受培训，以履行其个人与SOMS相关的职责。他们应接受关于SOMS关键组成部分的简报和培训，以及直接影响其活动的人权、人道法和相关刑法。此类培训可能包括预防和缓解措施、应对、记录和问责要求，以及处理当地社区、客户和媒体询问的程序。

应按照书面标准进行武器训练，包括非致命性武器的训练，这些标准应适合武器和预期使用条件。培训应包括指导、基于情景的培训和机械培训，包括武器故障和实弹射击资格。初始培训应定期重复进行，每年至少一次，或根据合同或法规要求更频繁地进行。

事件响应团队应接受关于其职责和义务的教育和培训，包括与第一响应者及其他内部和外部利益相关者的互动。团队成员应定期（至少每年）接受培训。新成员加入组织时也应接受培训。这些团队还应接受预防不良事件的培训。组织应在能力、意识和培训计划中纳入相关的外部利益相关者和资源。

A.7.3意识

组织应建立、推广和嵌入组织内部的安全运营管理文化，该文化应：

a) 确保安全运营管理和尊重人权成为组织核心价值观和治理的一部分；

b) 使利益相关者了解安全运营管理和其在任何计划中的作用；

c) 福利提高了个人绩效。

A.7.4通信

A.7.4.1概述

应安排内部和外部的沟通与协商，无论是在正常还是异常情况下。有效的沟通是预防、管理和报告不良或破坏性事件最重要的因素之一。应与内部和外部利益相关者进行主动的沟通和协商规划，以传达日常、警戒、破坏性事件以及组织和社区的应对信息。为了向不同群体提供最佳的沟通和合适的讯息，可能需要对受众进行细分。通过这种方式，可以定制消息，然后将其发布给特定的群体，如员工、客户、当地社区或媒体。

沟通和协商程序和过程应考虑：

a) 组织内部各级和各项活动之间以及与分包商、客户和合作伙伴实体之间的内部沟通；

b) 利益相关者的需求；

c) 接收、记录和回复来自外部利益相关者（包括当地社区）的相关信息；

d) 主动规划与外部利益相关者（包括媒体）的沟通；

e) 向相关利益相关者预先传达应对和报告计划，促进沟通并确保利益相关者已制定适当计划；

f) 促进与应急响应人员的结构化沟通；

g) 在破坏性情况下通信信道的可用性；

h) 信息的敏感性和详细程度；

i) 作战环境。

本组织应执行一项程序，以接收、记录和回复来自内部和外部利益攸关方的相关信息。此程序可包括与利益相关者的对话，并考虑他们相关的关切。在某些情况下，对利益相关者关切的回应可能包括有关组织活动和运营相关的风险、影响及控制程序的相关信息。这些程序还应涉及与公共当局就应急计划及其他相关问题进行必要沟通。

A.7.4.2业务通信

为对正在进行的安全行动进行充分的控制、协调和监督，必须制定行动通信计划。此类计划应包括安全行动人员、军事部队和法律部门之间如何共享相关威胁信息的说明。

执法机构，以及如何向参与敌对情况的安全行动人员提供适当的援助。信息应在各个绩效层级上以易于理解的方式进行交流，包括与客户或其他受组织保护的人，以及与组织安全团队遇到的军事或其他公共安全部队。

A.7.4.3风险沟通

组织还应识别并与社区、公共部门机构、负责情报、预警、预防、响应和恢复的组织及官员建立关系，这些关系涉及潜在的不希望发生和破坏性的事件。组织应正式规划其预防、缓解和响应沟通策略，考虑针对相关目标群体的具体决策、适当的信息和主题以及选择的手段。

组织应建立程序，与内部和外部利益相关者沟通和协商其风险、影响和控制程序。这些程序应考虑特定的利益相关者群体、要传达的信息类型、破坏性事件的类型及其后果、通信方法的可用性以及组织的个别情况。外部通信方法可包括：

a) 新闻或新闻稿；

b) 媒体

c) 财务报告

d) 时事通讯(的复数

e) 网站；

f) 社交媒体

g) 电话、电子邮件和短信（手动发送和/或通过自动紧急通知系统）；

h) 语音邮件；

i) 社区会议。

组织应预先规划应对突发事件的沟通。可以提前起草消息模板、脚本和声明，针对风险评估中识别出的威胁进行准备，以便分发给风险评估中确定的一个或多个利益相关者群体。还应建立程序，确保在短时间内能够分发沟通内容。

本组织应指定并公布主要发言人（并确定后备人员）的姓名，该发言人负责向媒体和其他人管理/传播危机信息。这些人员应接受媒体关系培训，以应对危机，并持续进行。所有信息都应通过一个团队传达，以确保信息的一致性。高层管理应强调，所有组织人员都应迅速被告知如何处理媒体电话，只有授权的公司发言人可以接受媒体采访。在某些情况下，还需要一名经过适当培训的现场发言人。

A.7.4.4申诉和投诉程序

组织应建立并向相关利益相关者传达内部和外部投诉和申诉程序。这些程序应确保隐私和保密性，并根据目标受众的文化、语言、教育和技术要求量身定制。应建立创建匿名和非匿名投诉和申诉报告机制的程序。

A.7.4.5通报举报人政策

举报行为发生在某人代表组织提出关于危险、不道德行为或非法行为的担忧时，这些行为可能影响内部或外部的其他人。代表组织工作的人员可能会担心，提出警告会导致同事或雇主的报复。然而，组织应当鼓励代表其工作的人员就任何内部或外部利益相关者的不当行为和不正当行为发声。举报政策将帮助组织以适当的方式处理问题。举报政策还可以作为威慑，防止那些考虑从事非法、不当或不道德行为的人。良好的举报政策将有助于减少问题，改善工作条件和运营效率。

有效的举报人政策为个人提供了一条除直接上级管理之外的其他渠道，以提出他们的关切。因此，组织应建立并传达一项举报政策，该政策提供一个明确的内部机制，用于匿名报告不符合规定的情况以及对危险、不道德行为或非法行为的担忧，这些行为可能影响内部或外部的其他人。政策还应规定哪些情况下外部披露是可以接受和受到保护的，以及哪些事项需要提交给适当的主管机构。只要举报人出于善意并有合理的理由提出关切，就应受到保护。

A.7.5记录的信息

A.7.5.1概述

文档的详细程度应足以描述SOMS及其各部分如何协同工作。文档还应提供获取特定SOMS部分操作更详细信息的途径。这些文档可以与其他组织实施的管理系统文档整合。不必以手册的形式呈现。

SOMS文档的范围可能因组织而异，原因如下：

a) 组织的规模和类型及其活动、产品或服务；

b) 过程及其相互作用的复杂性。

文件示例包括：

a) 政策、目标和指标；

b) 适用性声明、符合性声明和道德规范；

c) 重大风险和影响信息；

d) 程序

e) 过程信息；

f) 组织结构图；

g) 内部和外部标准；

h) 事故响应、缓解、应急和危机计划；

i) 记录

任何关于记录程序的决定应基于：

a) 不这样做的后果，包括对有形资产和无形资产的后果；

b) 证明组织遵守法律和其他要求的需要；

c) 确保活动持续进行的必要性；

d) 本国际标准的要求。

有效文件编制的优势包括：

a) 通过沟通和培训，使实施更加容易；

b) 更易于维护和修订；

c) 减少模棱两可和偏差的风险；

d) 可演示性和可视性。

最初为SOMS以外的目的创建的文件可以作为该管理系统的一部分使用（如果使用），并且应在系统中引用。

A.7.5.2创建和更新

A.7.5.2.1概述

程序应包括对文件化信息的识别、可访问性、完整性和安全性的控制。

A.7.5.2.2记录

除了本国际标准要求的记录外，记录还应包括（除其他外）：

a) 合规记录；

b) 持有武器的授权；

c) 对序列化和敏感设备的责任；

d) 燃料、弹药和训练材料的报告；

e) 追踪武器、爆炸物、车辆和危险材料；

f) 使用武力报告（致命和非致命）；

g) 合同合规审计报告；

h) 导入/导出合规性报告；

i) 审计跟踪文件；

j) 批准

k) 运动和测试结果；

l) 访问控制记录；

m) 分包商文件。

A.7.5.3文档信息控制

组织应以足以实施SOMS的方式创建和维护文档。但是，组织的主要重点应是有效实施SOMS和安全运营管理和绩效，而不是复杂的文档控制系统。

应适当考虑机密信息。应建立、传达和维护处理分类信息的程序。应明确分级和标记这些信息，以保护：

a) 信息的敏感性；

b) 个人的隐私、生命和安全；

c) 客户的形象和声誉。

组织应与组织内的相关法律机构进行协商，以确定文件应保留的适当时间，并建立、实施和维护有效执行该等程序。记录应至少保留七年或根据法律要求或限制而定。

A.8 操作

A.8.1运营规划和控制

A.8.1.1概述

一个组织应评估其与已确定的重大风险相关的业务活动，并确保以一种能够控制或减少与这些风险相关的可能性和不利后果的方式开展业务活动，以满足其安保业务管理政策的要求并实现其目标和指标。这应包括其运营的所有部分，包括分包商、供应链和维护活动。

由于本SOMS部分提供了如何将系统需求纳入日常运营的方向，因此需要使用记录程序来控制在没有记录程序的情况下可能导致偏离安全运营管理政策、目标和指标的情况。

为了尽量减少不良或破坏性事件的可能性，这些程序应包括行政、操作和技术控制。如果对现有安排进行修订或引入可能影响运营和活动的新安排，组织应在实施前考虑相关威胁和风险的最小化。

A.8.1.2安全相关功能的性能

A.8.1.2.1概述

程序应支持提供与安全有关的职能，以符合法律要求、合同义务和尊重人权的方式保护人员和有形及无形资产。

A.8.1.2.2急救和伤员护理

所有人员都应接受初次和反复的急救和伤员护理培训，特别强调在袭击或事故后立即应对创伤性伤害。培训应达到公认的标准。至少，培训应包括维持或建立适当的治疗区域的安全保障、伤员稳定、准备和请求撤离。这包括确保接受治疗的个人不会继续对周围的人构成故意或无意的威胁。培训还应包括根据伤势严重程度优先处理伤员，而不考虑友军/敌军身份、种族、民族背景或其他歧视因素。组织应确保个人和安保团队配备必要的材料，以提供即时治疗和稳定可救治的创伤性伤害，同时等待伤员撤离。

A.8.1.3尊重人权

组织有义务遵守国际人道法和适用国家法律所规定的权利，以及国际人权标准。它们应建立、实施并记录保护人类尊严和善待所有人的程序。这些程序应向相关方传达，以便报告和纠正任何不合规行为。

A.8.1.4不良或破坏性事件的预防和管理

程序应强调对可能导致不良和破坏性事件的风险进行预防性和主动性的管理，并且在事件发生时应对响应、恢复和补救措施进行说明。

组织应在不良或破坏性事件发生之前、期间和之后建立适当的行政和财务结构，以有效支持SOMS。应制定并记录程序，确保授权的透明度，符合公认会计程序和行业良好实践。因此，应明确界定管理结构、决策的权限和责任分配（包括支出限制、实施的权限和责任）。

A.8.2制定行为规范和道德操守准则

组织应为其员工、分包商和外包合作伙伴制定、实施并维护一份《道德规范》。《道德规范》应明确传达对人权和人类尊严的尊重，以及禁止贿赂、利益冲突、腐败和其他犯罪行为（例如使用影响表现的合法或非法物质）。《道德规范》应确保所有代表组织工作的人员了解其遵守人权、地方法律、国家法律和国际法的责任，并防止和报告任何侵犯人权的行为，包括但不限于：

a) 酷刑或其他残忍、不人道或有辱人格的待遇或处罚；

b) 性剥削和性虐待或基于性别的暴力；

c) 贩卖人口

d) 奴役和强迫劳动；

e) 最恶劣形式的童工劳动；

f) 非法歧视。

组织应向代表组织工作的所有人员清楚地传达并提供有关《道德规范》的培训。组织应记录和保存沟通和培训的记录。

A.8.3使用武力

A.8.3.1概述

私人安保行动带来的最大风险与组织人员不当使用武力和枪支有关。这包括组织人员在特定情况下使用超出必要或合理限度的武力。不当使用武力可能导致无辜者死亡或严重受伤，从而损害组织声誉，使公司及其保护对象面临法律责任。还可能引发进一步的安全问题和不稳定，影响组织、被保护对象以及该地区其他行动者。不当使用武力还包括未能使用必要的武力来防止组织人员、受保护的人和资源以及其他附近人员的生命损失。

组织使用武力程序是管理不当使用武力风险的关键工具，因此需要：

a) 所有有权携带武器和监督武器的人都能清楚地理解；

b) 适用于复杂情况和模糊情况；

c) 即使在使用武力的法律执行力度较弱的情况下，该组织也会严格执行。

明确的程序、有效的培训和明确的执行将有助于本组织及其支持的任何当事方的使命，并将促进遵守法治和本组织运作地区的长期稳定。

A.8.3.2使用武力政策

组织可制定一项武力使用政策，作为关于在组织业务环境中允许使用的武力的总体声明。该政策应描述一般适用原则，包括：

a) 仅在自卫、保护他人或限制进入或防止特定财产被毁时使用武力；

b) 将使用武力限制在消除威胁所必需和合理的范围内；

c) 仅在自卫或为他人防卫迫在眉睫的死亡或严重身体伤害威胁时使用致命武力，且没有其他合理的替代办法；

d) 限制从事独特的军事职能，如作战行动、类似作战的行动、警戒和搜索行动，或单独或与一国武装部队联合进行进攻行动。

制定时，组织的使用武力政策是根据业务范围和该地点的条件或工作情况制定使用武力程序的基础。

A.8.3.3使用武力程序

使用武力程序：

- 记录在何种情况下可以使用枪支和其他武力进行自卫，保护特定人员（包括其他安保人员）或财产免受他人非法攻击或其他伤害；
- 指导人员使用武力，确保任何符合该政策的武力使用也符合当地法律或其他控制法规以及组织遵守的任何行为准则。

在可能的情况下，这些程序应与组织保护的当事方协商制定。这可确保提供保护的一方与被保护的一方之间有共同的理解，并促进支持被保护方的使命和意图的程序。

A.8.3.4使用武力、火器或其他武器的一般考虑

在使用武力方面，具体限制因地点和具体行动环境而异，但是，本组织在制定使用武力程序时应考虑一些广泛适用的原则，包括以下原则。

a) 致命武力仅在极端必要的情况下使用，并且作为最后手段，在所有较轻的手段都已失败、可能失败或无法合理使用时才可采用。致命武力仅应在自卫或保护他人免受迫在眉睫的致命威胁时使用，或者在合理且必要的情况下，防止涉及严重生命威胁或严重身体伤害的严重犯罪行为。

b) 较小的武力可以用于应对不构成即时死亡或严重身体伤害威胁的情况。这些措施包括物理存在、使用警棍和神经冲击装置（如泰瑟枪）等，以及介于两者之间的手段。这些措施通常被称为“非致命”武力，以提醒无论意图如何，任何武力的使用都可能导致意外的重伤或死亡。随着设备的复杂性和有效性增加，意外致死的风险也随之增加；而随着使用者及其指挥者的训练水平和熟练度提高，这种风险则会降低。

c) 在不同地区，甚至同一国家政府下的不同区域当局之间，使用武力保护财产的授权也会发生变化。通常，不得使用致命武力来保护财产或阻止未经授权进入财产。常见的例外情况包括：

   1) 在个人为阻止进入或防止盗窃或破坏财产而进行的行动中，如果他（或她）感到自己面临死亡或严重伤害的迫在眉睫的威胁，则属于上述情况：在这种情况下，使用武力即为自卫；

   2) 为了防止对本质上危险的财产进行实际盗窃或破坏，这些财产的损失或毁坏会立即威胁到生命或严重身体伤害（例如枪支和其他弹药、放射性材料以及高毒性化学物质或生物制剂）：合理且必要的使用武力来保护这类财产通常被视为对他人进行防卫。

d) 主管法律机构也可以授权使用致命武力，如果合理且必要以防止破坏或摧毁对公共健康或安全至关重要的关键基础设施（如基本公共服务设施），这些设施的损坏会构成迫在眉睫的死亡或严重身体伤害威胁。在这种情况下，当局通常会发布具体规则，规定使用武力以保护此类基础设施。

e) 使用武力连续体。组织的武力使用程序应描述沿操作连续体应用武力的过程。安保人员应在最低级别的武力下尝试解决问题，或在情况和条件允许的情况下逐步减少武力。然而，延迟使用武力或沿连续体逐步增加武力并不是解决情况或威胁的必要手段。在某些情况下，逐步增加或升级武力可能会增加所有相关方的风险。使用武力连续体的目标是在使用武力实现合法目的时，使用合理的武力。

组织使用武力程序并非法律文件。它无法为组织或其人员因使用武力导致严重伤害或死亡而受到的起诉提供任何保护。使用武力程序可以作为辩护，以应对谋杀、过失杀人或其他杀人、袭击或殴打的指控，证明该组织在使用武力时有明确规定的程序，并且这些程序与当时适用的法律一致。组织的人员也可以使用这些程序来证明，在个人当时所面临的环境下，使用武力的程度和持续时间是合理的，并且这不是一个考虑不周的反应，而是经过纪律约束和控制的，同时考虑到他人的安全。

该组织使用武力的程序可能比适用法律允许的更为严格。例如，警告射击可能在相关法律或规定中被允许，但并非强制要求。该组织可能会认为使用警告射击会因致命武器的非瞄准发射而对旁观者造成不必要的伤害风险。同样，某些法律制度授权广泛使用武力来保护附近的人，即使这些人与持枪者及其职责无关。然而，该组织的使用武力程序可能会限制在这些情况下为他人辩护时使用武力。在考虑这种限制时，该组织应考虑到一些法律制度要求在为他人辩护时使用合理、必要且可用的武力。然而，在任何情况下，本组织使用武力的程序都不应限制个人固有的自卫权利。

A.8.3.5使用武力规则（RUF）

在某些情况下，组织可能由主管法律当局授予RUF。主管法律当局包括对组织所在地区行使控制的政府、与组织签订安全合同的政府或行使相当于军事占领某地区的权力的军事指挥官。

RUF代表组织在其业务运营中使用枪支和其他武力的官方授权和限制。通常，此类RUF包括关于武器授权程序的指示，包括武器类型、武力升级的要求，以及自卫时使用武力的警告、澄清和限制，还有与使用武力相关的沟通和报告要求。

组织应全面审查RUF、本国际标准以及组织所承诺的其他内容。组织的使用武力程序应涵盖这些来源中RUF未包含的任何要素。组织还应审查RUF，以确保其不超过本国际标准允许的武力使用范围，或限制正当防卫中合理且必要的武力使用。如果已发布的RUF超出本国际标准或其他适用法律允许的武力使用范围，或不合理地限制正当防卫中的武力使用，组织应寻求修改RUF。

在可能的情况下，本组织应寻求主管法律当局批准其使用武力程序，以发布为RUF。

A.8.3.6武器授权

组织应制定程序，确定需要武装以执行组织安全行动的具体人员及其携带武器的情况。武装授权应仅限于合格人员，依据合同条款或有合理预期若不携带武器将危及生命或资产时。组织应记录其尽职调查程序，这些程序适用于执行安全操作的地区，并根据适用的相关国家法律评估个人是否被禁止持有或携带武器。组织不应在完成背景调查之前向人员发放武器。武装授权程序应限制人员在安全操作中携带武器，直到个人接受培训并获得使用特定武器的认证。组织的程序应规定暂停或撤销武器授权的条件以及此类行动的权限。

本组织还应考虑在下列情况下限制武器的获取：

a) 不执行安全操作时；

b) 在饮酒后8小时或更长时间内；

c) 在服用可能影响反应或判断力的处方药时；

d) 不良事件报告后立即；

e) 在收到关于不遵守既定RUF或使用武力程序的指控后。对于所有被授权代表本组织携带武器的人员，应有下列记录：

a) 携带武器的授权证明；

b) 针对授权型号和型号的武器训练、资格和能力的最新记录；

c) 颁发和归还执行公务时使用的特定武器；

d) 武器维护；

e) 武器使用（训练之外的武器发射）

该组织应制定程序，为每个人保存和查阅这些记录，只要个人被授权使用或携带武器，或者根据法律要求更长时间。

A.8.3.7使用武力训练

RUF和使用武力的政策及程序应以适合目标受众的详细程度传达给代表组织工作的人员。培训应包括组织使用武力程序的所有主要要素以及与受训人员的级别和预期任务相适应的授权RUF。特别需要注意以下领域：

a) 将自卫的适用法律适用于特定的安全行动；

b) 组织人员何时何地可以携带武器；

c) 非执勤时的武器储存；

d) 自卫和保护他人的概念；

e) 什么是合理和必要的；

f) 违反使用武力程序或授权RUF的后果；

g) 个人或组织因使用武力而可能面临的潜在刑事和民事责任（这包括对行动或不作为的监督责任以及个人责任，无论是否收到监督命令或指示）；

h) 武装部队适用的交战规则（ROE）与适用于平民自卫的使用武力程序或RUF之间的差异。（在许多情况下，私人安保人员来自军事背景，在那里他们学习了符合ROE的使用武力方法。此外，私人安保行动可能在与军事力量一起或协同作战的环境中进行，这些军事力量也在ROE下运作。）明确理解这些差异对于私人安保和军事行动都至关重要。

培训应包括关于作为一系列反应的一部分的武力应用的指导，并评估个人在这一连续体中的理解。目标是让个人能够理解和仅使用合理必要的力量来阻止威胁，同时这种力量又足以有效保护人们和财产免受攻击或其他暴力行为。至少，逐步使用武力的连续体应包括以下技术的培训及其使用和成功或失败的适当指标。

a) 人员存在：以威慑为目的的存在。

b) 口头化：强制不是物理的；大声喊叫口头警告以停止活动。

c) 徒手控制：使用身体力量控制局面，对对手进行身体约束、阻拦或拘留。

d) 非致命方法：使用非致命技术来控制局势。

e) 致命武力威胁：展示武器并表明使用它的意图。

f) 致命武力：使用致命武器来控制局势。只有在必要时才开枪消除威胁。只发射瞄准射击，并且要考虑到旁观者的安全。

使用武力训练应解决：

a) 武力使用连续体；

b) 监管机构在控制该部队方面的作用（包括指挥和升级或降级部队的权力和权限）；

c) 组织监督人员、受保护方和警察或军事人员等法律当局在指挥或限制使用武力方面的角色和权力。

培训计划应包括学术（课堂）、机械、实弹和情景模拟训练。个人应面对与执行安全操作时可能遇到的情况相似的情境。这些情境应适合个人任务，并要求个人在复杂性和模糊性逐渐增加的情况下，运用判断力并采取适当的应对措施。实弹训练还应与特定的安全操作需求相关。例如但不限于近距离快速射击、针对移动车辆的致盲射击、使用路障和障碍物，或从移动车辆中射击。组织应使用现实、可测量和客观的标准来证明熟练度。武器鉴定标准应与公布的军事或行业标准一致，这些标准应适合于对个人所期望的安全任务，并且在可能的情况下应得到受保护实体的同意。

A.8.4逮捕和搜查

A.8.4.1逮捕人员

组织应为其人员提供抓捕行动的培训。这通常仅限于在组织保护下的人员、客户或财产遭受攻击后被捕的人。还应包括当个人试图未经许可离开访问控制点时采取的措施。培训应包括理论和实践内容，强调保护人员和财产免受进一步攻击，同时以人道方式对待被捕人员。培训还应包括保护被捕人员免受攻击或暴力的措施、向客户和相关部门报告逮捕情况，以及尽早将被捕人员移交给适当的当局。该组织应记录移交情况，包括被拘留者的身份、所指控的罪行以及移交给谁。

A.8.4.2搜索

组织应建立搜查人员的程序，确保搜查过程中尊重被搜查者的尊严和人道待遇，同时保障客户、受保护财产以及组织人员和旁观者的安全。组织应记录并妥善保管搜查后保留的个人物品。培训将区分静态岗哨处的最小侵入式搜查与逮捕后所需的全面搜查。

对被逮捕人员的搜查程序应包括：

a) 因受到攻击或迫在眉睫的威胁而被拘留的人与在出入检查点自愿搜查人员之间的区别；

b) 在提供任何必要的急救以挽救生命和确保被搜查者不会对附近的人构成死亡或严重身体伤害的紧迫威胁之间取得平衡；

c) 针对拒绝接受搜查或在得知将被搜查后试图离开该地区的人员采取的行动。

A.8.5支持执法的行动

本组织在开展执法或相关活动之前，应与合格的法律顾问进行协商。

A.8.6资源、作用、责任和权限

A.8.6.1概述

SOMS的成功实施需要组织内所有人员或代表组织的人员的承诺。应明确界定个人的角色、职责和权限，以确保SOMS的实施，防止误解（特别是在不希望发生或造成破坏性事件期间）并避免遗漏任务。

角色、职责和权限也应明确、记录并传达给外部利益相关者。这包括与分包商、合作伙伴、供应商、公共机构和当地社区的互动。组织应定义并传达所有参与安全管理运营人员的职责和权限，无论他们在组织中的其他角色如何。高层管理提供的资源应能够履行分配的角色和职责。当组织的操作环境发生变化时，应对角色、职责和权限进行审查。

有必要建立适当的行政结构，以有效应对不希望发生或具有破坏性的事件中的事故管理。应有明确的定义来界定管理结构、决策权和执行责任。组织应设立一个“事故管理团队”，在最高管理层或其代表的明确指导下领导事件响应。该团队应包括以下职能：

a) 计划

b) 事故响应和管理；

c) 人力资源管理

d) 健康、安全和医疗响应；

e) 信息管理

f) 保护措施

g) 合法的

h) 传播/媒体关系；

i) 其他关键支持功能。

事件管理团队可根据组织规模、类型、员工数量、位置等因素，适当支持多个团队。各团队应制定应对计划，涵盖潜在危机的各个方面，如损害评估与控制、沟通、人力资源、信息技术和行政支持。事件响应和管理计划应与整体SOMS保持一致，并纳入其中。应根据个人的技能、承诺程度和利益相关性招募其成为事件管理团队成员。

A.8.6.2人员

A.8.6.2.1概述

人员、能力和培训需求是组织环境及其合同要求的输出，也是风险评估和目标定义的输出。

各组织应制定与其代表工作有关的人员福利程序，与适用的劳工法和其他法律提供的保护一致，包括：

a) 向人员提供其参与的任何合同的副本，以他们理解的语言；

b) 为工作人员提供与其职责和工作条件相称的适当薪酬和报酬安排；

c) 通过作业安全和健康政策；

d) 确保人员不受限制地使用自己的旅行证件；

e) 防止就业中的非法歧视。

个人信息的隐私和保密性应当受到保护。关于个人的背景和操作信息可能非常敏感。组织必须建立并维持适当的程序，以确保信息在内部和外部都得到适当且严格的安全保护。组织应以安全的方式保存相关文件，保存时间应符合适用的法律法规、合同要求以及组织的记录政策。

至少应记录所有人员的以下信息：

a) 姓名、地址和联系信息；

b) 直系亲属和在发生伤害或死亡时通知的人员的联系信息；

c) 个人身份信息；

d) 法律和其他要求所需的信息。

A.8.6.2.2人员甄选、背景审查和审查

组织应建立书面程序，用于对代表组织工作的个人进行入职前背景调查和审查。组织应制定、记录、实施并维护筛选出不符合岗位最低资格要求的人员的程序，并根据其知识、技能、能力和其它属性选择适当合格的人员。筛选和选择程序应符合法律、合同要求以及《蒙特勒文件》和《国际职业行为准则》的原则。筛选和审查过程应基于候选人所考虑职位的性质、个人的权力级别和专业领域。在向候选人提供职位并开始工作之前，应进行筛选和审查。候选人应在进行背景调查前签署适当的授权书和同意书。保留某个人的服务的决定应基于候选人的全部资格和背景审查和审查的结果。

在可能的情况下，筛选和审查过程应包括：

a) 身份验证

b) 个人历史核查；

c) 经验、资格；

d) 其他证书验证。

当信息不可用、不可靠或不适当时，应记录排除情况。

身份验证应包括对潜在雇员的个人历史的有效性和最低年龄的验证。个人历史，可通过可用的个人历史搜索进行验证，应考虑（但不限于）：

a) 家庭住址；

b) 就业记录；

c) 电子宣传工具

d) 刑事和民事记录历史；

e) 侵犯人权的记录；

f) 军事或执法服务记录；

g) 机动车记录；

h) 信用报告；

i) 性犯罪者指数；

j) 政府和行业制裁名单；

k) 行业特定许可记录。

在核实候选人提供的经验和资格时，组织应查找无法解释的差距。这应该提供以下信息，但不仅限于：

a) 教育验证；

b) 就业核查；

c) 许可/认证/注册验证；

d) 人称代词

e) 主管和同事面试；

f) 军事和执法历史核查。

本组织还应根据以下方面，为个人的甄选和审查制定明确界定的标准：

a) 药物滥用

b) 身体和精神上的健康，以便进行活动；

c) 不适合携带武器；

d) 在压力和不利条件下操作的能力。

应保护个人资料的隐私和机密性，如护照、执照及出生证明等个人证件应在合理的时间内归还给员工。

A.8.6.2.3选择、背景审查和审查分包商

组织应仅临时或持续地保留能够按照本国际标准及《蒙特勒文件》和《国际合同条款》原则运作的合格分包商的服务。组织应对分包商的工作负责并承担相应责任。组织应制定、维护并记录明确界定的筛选和审查分包商的标准，以供合同使用。与分包商签订的合同协议应根据适用法律和与客户的合同义务进行记录和保存。

分包标准应包括分包商的以下能力：

a) 满足本国际标准的要求；

b) 按照相关法律（地方、国家、人道主义和人权）开展活动；

c) 维护客户的形象和声誉；

d) 提供足够的资源和专门知识，包括合格人员，以实现业务目标；

e) 确保在履行分配职责的过程中具有透明度、问责制和适当的监督；

f) 考虑到财务和经济义务（包括适当的个人薪酬和保险范围）；

g) 获得必要的注册、许可证或许可；

h) 保持准确和最新的人员和财产记录；

i) 按照适用法律和合同义务获取、使用、返还和处置武器弹药。

本组织应：

a) 确保与分包商或外包合作伙伴签订适当的书面协议；

b) 以书面形式向客户说明安排，并在适当情况下获得客户的批准；

c) 负责监督分包商提供的用于合同的人员的培训，包括尊重人权和避免不利影响；

d) 确保为分包商的活动提供全面保险覆盖；

e) 保持分包或外包工作的符合本国际标准的记录。

A.8.6.3.武器、危险材料和弹药的采购和管理

该组织应建立并记录其遵守国家和国际法律和条例的程序，涉及采购、发放和转运用于行动的火器（以及其它管制物品，如防弹衣和炸药）。因此，该组织应建立、维护和记录确保以下事项的程序：

a) 合法获得其弹药和装备，特别是武器（包括“最终用户承诺”）；

b) 根据适用的国际和国内法律的要求，获得并保持拥有、运输、出口和转运枪支弹药和其他管制物品的合法授权；

c) 能够识别和记录所有弹药和设备，特别是武器和危险材料（例如：序列号登记册、材料安全数据表（MSDS）、安全数据表（SDS）、产品安全数据表（PSDS）或批号）；

d) 使用弹药和装备，特别是国际法未禁止的武器；

e) 在自卫或保护他人的情况下使用装备、材料和武器的标准，这些装备、材料和武器适合任务和行动；

f) 建立设备、材料和武器的可追溯性系统；

g) 为设备、材料和武器的安全和有保障的储存、发放、维护、运输和使用提供适当的保障；

h) 对枪支和安全设备进行定期维护，确保其适合并安全地用于目的；

i) 遵守了有关武器和弹药的返还和/或处置的合同规定。

根据合同规定，组织及其分包商应授权拥有和使用武器。对于代表组织工作的人员，应有以下记录：

a) 携带武器的授权证明；

b) 武器训练、资格和能力的最新记录；

c) 武器维护；

d) 武器使用。

A.8.6.4制服和标志

组织应采用并使用能够表明安保团队成员身份及其所属公司的制服和装备标识，这些标识的图案、颜色或标记不应与军队和警察等公共安全部队的标识混淆。组织选择或客户指定的制服和标识还需获得该组织运营所在国家相关部门的批准。

标准化制服和标有标记的车辆向公众、警察、军队和其他当局表明安保行动小组成员有权携带和使用武器。制服应包括徽章编号、姓名或其他方式来区分组织人员。车辆标识应包括公司标志和唯一编号。制服和其他标识有助于在发生扰乱或不希望的事件时，公众能够正确识别。这种识别使得报告更加公开透明，并减少了同一地区内一个组织可能因另一个组织的不当行为而受到指责的可能性。

制服能够展现组织的正面形象，并鼓励公司人员表现出专业和负责任的行为。在武装冲突的情况下，可辨识的制服和标识可以减少安全行动人员被误认为战斗人员并遭到敌对武装力量攻击的可能性——前提是这些武装力量遵守国际人道法。为了有效，应向当地当局、公众以及适用时向敌对武装力量提供有关制服、公司标志、徽章和车辆独特标识的信息。

在某些特定情况下，客户可能不希望安全操作人员被轻易识别。在其他情况下，风险评估可能表明，武装安保人员的明显身份标识会增加对客户、公众和安全人员的暴力和危险威胁。在这种情况下，当更隐蔽的方法符合当地法律时，安保人员可能会被指示穿着不易与平民服装区分的功能性服装，不公开携带武器，车辆也不会从其他民用交通中脱颖而出。即使在隐蔽或低调的情况下，安保人员仍应随身携带不可转让的个人身份识别手段。

A.8.7职业健康和安全

组织应提供安全、健康的作业环境，同时认识到当地环境可能带来的固有危险和局限性。在高风险或危及生命的情况下，应采取合理的预防措施保护代表组织工作的所有人员或受其照管的人员。

A.8.8事件管理

A.8.8.1概述

组织应制定针对不良和破坏性事件的预防、准备、缓解、响应、恢复和补救程序。组织应建立详细说明组织将如何管理破坏性事件以及如何处理的书面程序。

根据管理层批准的恢复目标，将活动恢复或维持到预定水平。程序应：

a) 应基于风险评估中确定和优先考虑的风险；

b) 利用风险评估来识别潜在不良和破坏性事件的具体情况，包括任何前兆和警告信号；

c) 根据风险评估的输出，以系统和整体的方式管理风险；

d) 综合考虑避免、消除、减少、扩散、转移和接受等风险处理策略，提供最佳解决方案；

e) 包括通知有关当局和利益相关方的条款。

组织应制定程序，以识别何时出现明显的特定危险，从而需要采取一定程度的反应来避免、预防、减轻或应对不良事件的可能性。一个强有力的检测和避免政策及程序计划应支持这一过程。

一旦发现潜在的破坏性事件，应立即向指定的主管机构、管理层成员或负责危机通知和管理的其他人员报告。应制定具体的通报标准，并予以记录和遵守。

问题评估（决策过程中的评价环节，旨在确定待解决的问题性质）和严重性评估（确定中断及其相关后果严重性的过程）应在不希望发生的事件之初进行。需要考虑的因素包括问题的规模、潜在升级的可能性以及情况对组织及其利益相关者（如当地社区和客户）可能产生的影响。

预防措施可包括与内部和外部利益相关者协调的主动步骤。组织文化、运营计划和管理目标应激励个人对预防、避免、威慑和检测负起个人责任。应采用成本效益高的缓解策略，以防止或减轻潜在事件的后果。应确定有助于缓解过程的各种资源。

应围绕现实的“最坏情况”制定准备和响应计划，同时理解响应可以适当扩大以匹配实际危机。考虑因素包括：

a) 人员是任何准备和响应计划中最重要的方面；

b) 组织如何管理人力资源将影响事件管理的成功或失败；

c) 事先做出的后勤决策将影响到良好准备和应对计划的成功或失败；

d) 应检查现有资金和保险政策。

A.8.8.2事件监测、报告和调查

组织应建立事件报告程序，记录任何涉及代表其工作的人员使用武器的情况（除授权训练外）、任何武力升级、设备损坏、人员受伤、财产破坏、袭击、犯罪行为、交通事故、涉及其他安全部队的事件以及客户要求的任何其他此类报告。组织还应建立内部调查程序，以确定以下事项：

a) 事件发生的时间和地点；

b) 所涉人员的身份，包括其地址和其他联系信息；

c) 受伤/损坏；

d) 导致事件发生的环境；

e) 组织针对该事件采取的任何措施；

f) 造成内部和外部伤亡的原因；

g) 通知有关当局；

h) 识别根本原因；

i) 采取的纠正和预防措施。

在完成调查后，组织应以书面形式编制事件报告，包括上述信息，并向相关利益相关者（例如客户和管辖当局）提供事件报告副本。事件报告应提供足够的信息，以评估响应的充分性。

代表本组织工作的人员应了解事件报告的责任和机制，包括收集和保存证据。事件报告方案应纳入本组织的培训方案。

A.8.8.3内部和外部投诉和申诉程序

组织应建立投诉和申诉程序，任何内部或外部利益相关者若认为存在潜在或实际不符合本国际标准的情况，或违反国际、国家和地方法律，或人权问题，均可提出申诉。该程序应规定，组织或其代表人员不得对提出申诉或协助调查申诉的人进行报复。

投诉和申诉程序不仅仅是为了记录申诉，它们应该被设计成通过确定根本原因、提高问责制、评估有效性标准和推动持续改进文化来解决纠纷。一旦投诉或申诉得到证实，应以加快的方式实施纠正和预防措施。

在制定投诉和申诉程序时，应指定一名或多名人员负责协调调查和解决组织收到的任何投诉，这些投诉涉及威胁人类生命、权利或安全的行为，或不符合本国际标准的要求，或客户要求。组织应采用并公布其申诉程序，确保投诉得到及时和公正的处理。

程序应包括但不限于：

a) 提交申诉或投诉的机制；

b) 提交人的信息要求，包括提交佐证信息；

c) 提交、调查和结果的时间表；

d) 保密和隐私条款；

e) 解决过程的分层步骤；

f) 内部和外部调查程序；

g) 与申诉和调查有关的文件和记录的维护要求；

h) 纪律处分；

i） 解决投诉或申诉的步骤，包括防止再次发生的措施；

j） 结果的文件记录和沟通；

k) 通知有关当局；

l） 评价投诉和申诉程序的有效性。

A.8.8.4举报人政策

举报人是指代表组织揭露不符合本国际标准或与组织的法律义务和自愿承诺不符的行为和行动的人。举报人可以在内部或外部（例如向监管机构、执法部门或关注该问题的团体）提出指控。组织应建立并传达其举报政策给相关利益相关者。

A.9 业绩评价

A.9.1监测、测量、分析和评价

A.9.1.1概述

绩效评估涉及对组织的安全操作、法律遵从性和人权表现的衡量、监控和评估。组织应采用系统的方法定期衡量和监控其安全操作的关键绩效指标。指标确保组织的政策、目标和指标得以实现，并阐明改进领域。

为了衡量和监控组织的安全运营绩效，应制定一套绩效指标来评估管理系统及其成果（包括其安全运营的影响）。这些指标可以是定量的或定性的，直接关联于风险评估和安全运营的目标与指标。绩效指标可以是管理、运营或经济指标。这些指标应提供有用的信息，以识别成功之处以及需要纠正或改进的领域。

SOMS应提供定义指标、收集数据和分析所收集数据的程序。应建立指标以监控和衡量SOMS的有效性，并识别改进领域，以提升性能，预防潜在的不良和破坏性事件。从这些信息中获得的知识可用于实施纠正和预防措施。关键特征是组织需要考虑的特征，以确定如何管理重大风险、实现目标和指标以及提高安全运营绩效。

为确保结果的有效性，必要时，应按照规定的时间间隔或在使用前，根据可追溯至国际或国家测量标准的测量标准校准或验证测量设备。如果没有这样的标准，则应记录用于校准的依据。

A.9.1.2合规性评价

该组织应能够证明其已评估了对所确定的法律和人权要求的遵守情况，包括适用的许可证或许可。

组织应能够证明其已评估了对所承诺的其他已确定要求的遵守情况。

A.9.1.3练习和测试

应使用风险评估中确定的事件来设计演习和测试场景。演习和测试可以作为有效的培训工具，并可用于验证风险评估的假设和结论。

演练确保技术资源按计划运行，并确保代表组织工作的人员接受充分的使用和操作培训。演练可以保持代表组织工作的人员在其职责中高效，明确他们的角色，并识别SOMS、其计划及其程序中的改进领域。演练可以揭示SOMS中的弱点，这些弱点需要纠正。对演练的承诺赋予SOMS可信度和权威性。

在进行演习和测试时，第一步应该是设定目标和期望。一个关键的目标是确定某些预防和应对过程是否有效，以及如何改进。组织应使用演习和记录的演习结果来确保SOMS的有效性和准备状态，特别是其安全操作计划、团队准备和设施，以执行和验证其安全操作功能。

锻炼和测试的好处包括：

a) 规划范围、假设和战略的确认；

b) 审查和提高代表本组织工作的人员的能力；

c) 容量测试（例如，呼叫入站或呼叫出站电话系统的容量）；

d) 提高效率并减少完成一个过程所需的时间（例如，使用重复的练习来缩短响应时间）；

e) 让内部和外部利益相关者了解SOMS及其作用。

组织应设计演练场景，以评估安全运营计划。应制定定期演练SOMS及其组件的时间表和时间线。演练和测试应具有现实性，评估安全管理的能力和容量，并确保涉及人员和资产的安全。演习的范围和细节应根据组织的经验、资源和能力成熟。早期测试可能包括清单、简单演习和SOMS的小部分。演习成熟度增加的例子包括：

a) 方向：介绍、概述或教育会议；

b) 桌面：以叙述形式呈现的实际或模拟练习；

c) 功能：在受控环境中尽可能真实地模拟场景的步行或专门锻炼；

d) 全尺寸：模拟实时、真实生活场景的实时或真实生活练习。

有几个角色可以由参与者承担。所有参与者都应了解他们在演练中的角色。演练应涵盖由演练范围定义的所有组织参与者；在适当的情况下，可以包括外部利益相关者。作为演练的一部分，应安排与所有参与者进行审查，讨论问题和经验教训。这些信息应记录在正式的演练报告中，并由高层管理审查。对计划和程序进行更新，并迅速实施纠正和预防措施。

测试和演习的设计应根据需要进行评估和修改。这些设计应当具有动态性，考虑到SOMS的变化、人员流动、实际事件以及以往演习的结果。从演习和测试中汲取的经验教训，以及实际经历的事件，都应纳入未来SOMS的演习和测试计划中。

应记录并保存运动和测试结果作为记录。

A.9.2内部审计

进行SOMS内部审计至关重要，以确保SOMS实现其目标，符合计划安排，得到妥善实施和维护，并识别改进机会。SOMS内部审计应在预定的时间间隔内进行，以确定并向高层管理提供有关SOMS适当性和有效性的信息，同时为设定持续改进SOMS绩效的目标提供依据。

组织应建立审计计划（见ISO 19011指南），以指导计划和开展审计，并确定为满足计划目标所需的审计。该计划应基于组织活动的性质、风险评估、以往审计的结果和其他相关因素。

内部审计计划应基于SOMS的全部范围；但是，每次审计不必涵盖整个系统。只要审计计划确保在组织指定的审计期内，所有组织单位、活动和系统要素以及SOMS的全部范围都在审计计划中接受审计，那么审计可以分为较小的部分。

内部SOMS审核的结果可以以报告的形式提供，并用于纠正或防止特定的不符合项，以及为管理评审的实施提供输入。

SOMS的内部审计可以由组织内部人员或由组织选定的外部人员代表组织进行。无论哪种情况，执行审计的人员都应具备相应的能力，并能够公正、客观地开展工作。在较小的组织中，审计独立性可以通过审计员不受被审计活动责任的影响来体现。

注：如果组织希望将其SOMS审计与安全、弹性、安全或环境审计相结合，则需要明确界定每项审计的目的和范围。由独立于组织的机构进行的第三方符合性评估，可向内部和外部利益相关者提供信心，证明符合本国际标准的要求。认证的价值在于公正、合格的外部评估所建立的公众信任和信心的程度。

A.9.3管理评审

管理评审为最高管理层提供了评估SOMS持续适宜性、充分性和有效性的机会。管理评审应涵盖SOMS的范围，尽管并非所有SOMS要素都需要一次性审查，且评审过程可能需要一段时间。管理评审将使最高管理层能够应对关键SOMS要素变更的需求，包括：

a) 政策

b) 资源分配；

c) 风险偏好和风险承受能力；

d) 目标和指标；

e) 安全操作策略。

最高管理层应定期安排并评价SOMS的实施和结果。虽然建议进行持续的系统审查，但正式审查应有结构、适当记录和在合适的条件下安排。参与实施SOMS并分配其资源的人员应参与管理审查。

除定期管理系统审查外，以下因素可触发审查，否则应在安排审查时予以检查。

a) 风险评估：每次组织完成风险评估时，都应审查SOMS。风险评估的结果可用于确定SOMS是否继续充分应对组织面临的风险。

b) 行业/部门、合同和政治趋势：行业/部门、合同和政治趋势的重大变化应启动SOMS审查。可以使用行业/部门和安全操作规划技术的一般趋势和最佳实践进行基准测试。

c) 监管要求：新的监管要求可能需要对SOMS进行审查。

d) 事件经历：无论预防、缓解或响应计划是否启动，都应在不良或破坏性事件发生后进行审查。如果启动了计划，则审查应考虑计划本身的历史、如何运行、为何启动等。如果计划未被激活，审查应检查原因以及该决定是否恰当。

e) 测试和试验结果：根据测试和试验结果，应根据需要修改SOMS。

持续改进和SOMS维护应反映组织风险、活动和操作的变化，这些变化将影响SOMS。以下是一些可能影响SOMS的程序、系统或过程示例：

a) 政策变化；

b) 危险和威胁变化；

c) 组织及其业务流程的变更；

d) 风险评估假设的变化；

e) 人员变动（员工和承包商）及其联系方式；

f) 分包商和供应链变化；

g) 工艺和技术变更；

h) 系统和应用软件变更；

i) 从锻炼和测试中吸取的经验教训；

j) 从外部组织的不良和破坏性事件中吸取的经验教训；

k) 在实际调用计划过程中发现的问题；

l) 外部环境的变化（新客户需求、政治变化、与当地社区的关系等）；

m) 在计划审查期间注意到的其他项目以及在风险评估期间确定的其他项目。

A.10 改进

A.10.1 不符合项和纠正措施

组织应建立有效的程序，以确保及时识别和传达与SOMS（其计划和程序）相关的未满足要求、规划方法的不足、事件、接近失误和弱点，以防止进一步发生。

识别情况的发生，以及确定和解决根本原因。程序应能够持续检测、分析和消除实际和潜在的不合格原因。

应调查任何已识别的不合格的根本原因（或根本原因），以便制定纠正行动计划，立即解决问题以减轻后果，做出必要的改变以纠正情况并恢复正常运营，并采取措施防止问题再次发生，消除根本原因。行动的性质和时机应与不合格的规模和性质及其潜在后果相适应。

有时，可能会发现潜在问题，但实际并不存在不符合项。在这种情况下，应采取预防措施，采用类似的方法。潜在问题可以从内部SOMS审核过程中识别的实际不符合项的纠正措施、行业趋势和事件分析或在演习和测试中发现的问题推断出来。识别潜在的不合格情况也可以成为意识到注意和传达潜在或实际问题重要性的人的日常职责的一部分。

建立处理实际和潜在不合格项以及持续采取纠正和预防措施的程序，有助于确保SOMS的可靠性和有效性。这些程序应明确责任、权限及规划和实施纠正与预防措施的具体步骤。最高管理层应确保纠正和预防措施已得到执行，并有系统地跟进以评估其有效性。

导致SOMS变更的纠正和预防措施应反映在文件中，并触发对与系统变更相关的风险评估的重新审查，以评估对计划、程序和培训需求的影响。变更应传达给受影响的利益相关者。

组织应采取措施消除与SOMS的实施和运行相关的不合格的原因，以防止其再次发生。纠正措施的文件化程序应规定以下要求：

a) 识别任何不符合项；

b) 确定不合格的原因；

c) 评估是否需要采取行动，以确保不重复出现不符合项；

d) 确定并实施所需的纠正措施；

e) 记录采取行动的结果；

f) 审查所采取的纠正措施和该措施的结果。

A.10.2预防措施

组织应采取措施防止潜在的不符合项的发生。所采取的预防措施应与不符合项的潜在影响相适应。

预防措施的书面程序应规定以下要求：

a) 识别潜在的不合格及其原因；

b) 确定并实施所需的预防措施；

c) 记录采取的行动的结果；

d) 审查所采取的预防措施；

e) 识别变更风险并确保关注重点放在重大变更风险上；

f) 确保所有需要了解的人员都了解不合格情况和已采取的预防措施；

g) 基于风险评估结果的预防措施的优先级。

A.11 分阶段实施的成熟度模型

实施管理体系标准可能是一项艰巨的任务，特别是对于中小企业而言。所有组织都面临着在组织目标和可用资源范围内管理风险的挑战。只有通过全面实施并符合本国际标准的所有要求，持续维护和不断改进SOMS，组织才能实现其最终目标，即确保安全运营的专业性与尊重人权相一致。分阶段构建SOMS并达到成熟度基准，为组织提供了目标与资源之间的桥梁。

通过使用成熟度模型来分阶段实施SOMS，组织定义了一系列步骤，旨在帮助其评估当前在安全运营和人权尊重方面的状况，设定未来的发展目标，衡量当前相对于这些目标的位置，并规划一条符合商业逻辑的道路，以实现SOMS的全面实施。(ANSI/ASIS PSC.3-2013提供了更多关于使用成熟度模型的信息。)

附件B

（说明性）一般原则

B.1 将军

SOMS的目标是以一种增强人类安全和安保的方式管理组织的安全运营，同时保护资产（包括有形和无形资产），并遵守国际、国家和地方法律及人权。这在治理可能薄弱或因人为或自然灾害导致法治受到破坏的情况下尤为重要。组织需要通过管理所有利益相关者面临的风险来开展业务并实现客户的目标，这些利益相关者包括为其工作的人员、受影响社区及其客户。这是通过将法律、社会、文化环境问题融入业务运营和与利益相关者的互动中，制定适当的预防措施来实现的，以保护托付给他们的人员和物理资产。其目的是通过以下方式最小化破坏性或不良事件的可能性及其后果：

-在可能的情况下，预防；

-减轻事件的影响；

-在事件发生时有效地、高效地做出响应，保持约定的性能水平；

-确保事后问责；

-采取措施防止复发。

SOMS将促进组织内部的文化，确保安全操作与尊重国际、国家和当地法律及人权相一致。

通过开发、设计、记录、部署和评估符合需求的SOMS，可以实现一致且公认的表现水平。本国际标准第4至10条及附件详细规定了执行安全操作时尊重人权的管理体系要素。在开发、实施和改进SOMS过程中，最高管理层/决策者应遵循以下一般原则。

组织应在设计和实施SOMS时将以下所有原则整合在一起，目的是实现组织和客户的目标，保护资产（有形和无形），同时确保人身安全和安保并尊重人权。安全运营管理将取决于这些原则融入组织管理框架的有效性，这推动了与尊重人权相一致的安全运营文化，在组织的所有层级中得以体现。运用这些原则应建立一个环境，确保信息得到充分报告，并作为决策和问责的基础，在所有相关组织层级中发挥作用。

B.2 以结果为导向

管理系统不仅仅是一套管理流程；它是实现预期结果的工具。SOMS用于实现与尊重人权、合同和法律义务相一致的安全运营成果。定义关键绩效指标（KPI）以支持目标的实现。KPI推动了通过测量进行持续管理的文化。

监控和性能改进。任何SOMS的结果都是有效管理与以下方面相关的风险：

—安全操作和管理；

-保护客户、资产和被保护人员；

-人权；

-受影响的社区；

-安全服务提供商的安全性；

—声誉和信息

B.3 领导力和远见

最高管理层（指负责决策并有权实施这些决策的个人或团队）确立愿景，设定目标，并为组织提供方向。他们促进一种归属感文化，在这种文化中，每个人都将尊重人权和管理不希望发生的破坏性事件视为实现组织目标和宗旨的一部分。最高管理层致力于推动安全运营文化的建设，同时尊重国际、国家和地方法律及人权，并在实施和维护这一国际标准方面发挥有效领导作用。

B.4 治理

确保专业安全运营被视为整体良好治理策略的一部分，是全企业范围的责任。按照国际、国家和地方法律及人权开展安全运营，体现了组织的宗旨和价值观。在实现使命目标的过程中保护人类生命和安全，是管理不希望发生和破坏性事件风险的主要关切。

B.5 面向需求

评估和理解组织的资产、需求和期望对于私人安保运营管理的成功至关重要。安全管理需要响应客户的需求和期望，同时也要考虑其他利益相关者的需求和期望——例如受影响社区，他们的积极或消极支持对于组织及其客户的成功是必要的。组织的目标与内部和外部利益相关者的需要和期望相联系。利益相关者关系采用平衡方法系统地进行管理，平衡方法兼顾组织、客户和其他利益相关者（如受影响社区）的需求。

B.6 整体组织风险管理策略

管理安全运营时尊重人权是组织整体风险管理策略的一部分。除非有效管理风险，否则组织无法最大化机会并最小化风险。风险是不确定性对实现目标的影响，强调人员安全和安保以及资产（有形和无形）的保护，同时遵守国际、国家和地方法律及人权。风险管理过程需要清楚了解组织的内外环境，以主动识别机会并最小化风险。评估和了解组织可接受的风险水平对于组织制定先发制人且有效的风险管理策略至关重要，该策略应符合其内部和外部利益相关者在运营环境风险水平背景下的需求和期望。

B.7 系统方法

SOMS需要多维度、迭代的方法。识别、理解和管理相互关联的过程和要素有助于组织有效且高效地控制其风险。系统方法考察构成整个系统的各个要素之间的联系和互动。系统各部分最好在其相互关系的背景下理解，而不是孤立地看待，并需作为一个整体来处理。

B.8 适应性和灵活性

大多数组织，特别是那些进行或承包安全运营的组织，在内部和外部环境不断变化的情况下运作。组织需要持续进行运营监控，以识别变化并实施有效的变更控制策略。组织必须具备适应能力：能够并且愿意进化——不断调整以反映不断变化的运营环境。SOMS应被视为一种管理框架，而不仅仅是一系列活动。随着任务、预算、优先事项和工作人员的不断变化，当具体用途发生变化时，框架结构将保持可预测性。

B.9 管理不确定性

安全管理并不总是基于可预测的威胁和可量化的风险。进行或委托安全运营的组织通常在治理薄弱或法治因人为或自然事件而受到破坏的情况下工作。分析已知和未知威胁的可能性及其后果，以及组织和利益相关者在不断变化环境中的脆弱性时，需要做出估计和假设。风险管理明确考虑了不希望发生的破坏性事件的不确定性、这种不确定性的性质以及如何应对这些不确定性。

B.10 文化变革与交流

最高管理层必须制定明确的战略、沟通、培训和意识方案，以确保各级管理人员和员工了解管理体系的目标。SOMS支持组织内部的文化和认知变革，从而保护组织及其客户的形象和声誉。SOMS需要在企业高层得到充分理解和支持，并传达给所有代表组织工作的人员，作为组织核心文化的一部分。

B.11 决策的依据

评估安全管理业务和风险相关问题，推动决策制定，并根据事实分析——结合经验和行业公认的最佳实践——指导采取行动。SOMS提升了审查、质疑和改变意见及决策的能力，增强了解决问题的能力，通过引用事实记录来证明过去决策的有效性，并确保数据和信息准确、可靠且及时——符合公司政策。

B.12 持续改进

管理人员通过持续改进周期对SOMS过程、程序、能力和信息进行监控、测量、评审和后续修改，从而提高其SOMS。定期进行正式的书面审查，审查结果应由最高管理层考虑并酌情采取行动。

附件C

（信息性）开始-差距分析

组织应通过差距分析来确定其当前在管理潜在风险情景方面的地位。差距分析将使组织能够将其实际表现与实现目标所需的表现进行比较。分析应考虑组织的风险（包括潜在影响），作为建立SOMS的基础。

差距分析应涵盖五个关键领域：

a) 风险识别，包括与运行条件、紧急情况、事故和潜在不良和破坏性事件相关的风险；

b) 人权风险分析，以确定组织安全行动的影响的严重性，并确定改进机会；

c) 识别适用的法律要求和组织遵守的其他要求；

d) 对现有的风险管理实践和程序进行评估，包括与分包活动相关的实践和程序；

e) 对以往紧急情况和事故的评价，以及为预防和应对不良和破坏性事件而采取的措施。

在所有情况下，都应考虑组织内的运作和职能、与相关利益相关者的联系，以及可能引发混乱和紧急情况。进行差距分析的工具和方法可能包括检查表、访谈、直接检查和测量，或以往审计或其他审查的结果，具体取决于活动的性质。

附件D

（信息性）管理系统方法

管理系统方法鼓励组织分析自身及利益相关者的需求，并定义有助于成功的流程。它为制定政策和目标、建立实现预期结果的程序以及衡量和监控目标及结果的达成提供了基础。管理系统为持续改进提供了框架，以提高提升安全运营专业性的可能性，同时确保人权和基本自由得到保护。它让组织及其客户都相信，该组织能够管理其合同、安全和法律义务，并尊重人权。

管理系统方法考虑了当地政策、文化、行动或变化如何影响整个组织及其环境。系统各组成部分在相互关系的背景下理解最为恰当，而不是孤立地理解。因此，管理系统考察构成整个系统各要素之间的联系和互动。管理系统方法系统地定义了实现预期结果所需的活动，并明确了管理关键活动的责任和问责制。该管理系统标准提供了建立、实施、运行、监控、审查、维护和改进组织安全运营管理体系的要求，确保其符合人权尊重原则。为了有效运作，组织需要识别并管理许多活动。任何能够将输入转化为输出、使用资源且正式管理的活动都可以被视为过程。通常，一个过程的输出直接成为下一个过程的输入。

本国际标准中提出的安全管理操作管理的管理系统方法鼓励其用户强调以下方面的重要性：

a) 了解组织的风险、安全和人权保护要求；

b) 确定安全行动的结果，符合尊重人权、合同和法律义务；

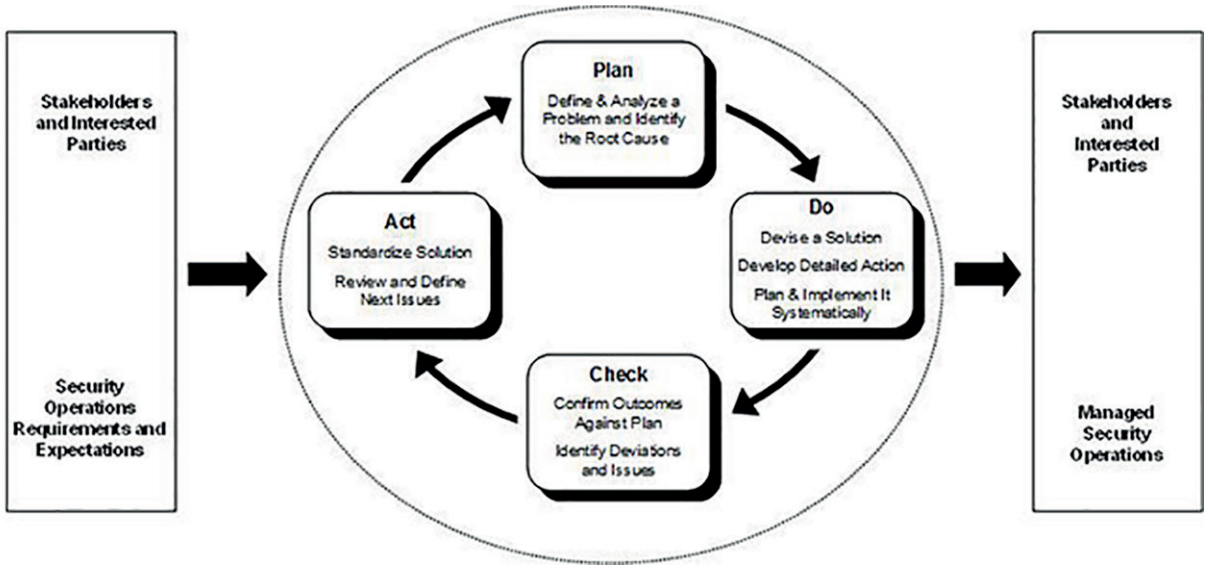
c) 制定风险管理政策和目标、流程、系统和文化；

d) 实施和操作控制，以管理组织的风险和安全要求，并尊重人权；

e) 从行政和业务角度监测和审查SOMS的绩效和有效性；

f) 基于客观测量的持续改进。

本国际标准采用了“计划-执行-检查-行动”（PDCA）模型，用于构建安全运营流程。图D.1展示了SOMS如何以安全运营管理需求和利益相关者的期望为输入，通过必要的行动和过程，产生满足这些需求和期望的安全运营和风险管理结果。图D.1还展示了本国际标准中所呈现的流程中的联系。



图D.1-计划-执行-检查-行动模型

PDCA循环可简要描述如下：

-计划（建立管理体系）：建立与管理运营和改进风险管理相关的管理体系政策、目标、过程和程序，以按照组织的总体政策和目标交付成果。

—执行（实施和运行管理体系）：执行并运行管理体系方针、控制、过程和程序。

-核查（监控和评审管理体系）：根据管理体系方针、目标和实际经验评估和衡量过程绩效，并将结果报告管理层进行评审。

-行动（保持和改进管理体系）：根据内部管理体系审核和管理评审的结果，采取纠正和预防措施，实现管理体系的持续改进。

PDCA模型是一种清晰、系统且有文档记录的方法，用于：

a) 设定可衡量的目标和指标；

b) 监控、衡量和评估进展；

c) 发现问题时，及时识别、预防或纠正；

d) 评估能力要求并培训代表组织工作的人员；

e) 为最高管理层提供反馈循环，以评估进展并作出适当的管理体系变更。

此外，它有助于组织内部的信息管理，从而提高业务效率。

本国际标准旨在与组织内的质量、安全、环境、信息安全、韧性、风险、安保等管理体系相集成。因此，一个设计得当的管理体系可以满足所有这些标准的要求。采用管理体系方法的组织（例如根据ISO 9001、ISO 14001、ISO/IEC 27001、ISO 28000、OHSAS 18001、ANSI/ASIS PSC.1-2012、ANSI/ASIS SPC.1-2009)可以利用其现有的管理体系作为基础，按照本标准的规定实施SOMS。

国际标准。符合本国际标准可通过与ISO/IEC 17021-1方法一致的审核过程进行验证。

附件E

（说明性）申请的限定条件

采用并系统地实施一系列安全运营管理技术，可以为所有利益相关者和受影响方带来最佳结果。然而，仅采纳这一国际标准并不能保证安全运营的最佳效果。为了实现其目标，SOMS应在适当且经济可行的情况下，纳入最佳可用实践、技术和方法。这些实践、技术和方法的成本效益应得到充分考虑。

本国际标准没有为安全操作性能制定超出组织政策承诺的绝对要求：

a) 遵守适用的法律要求和组织遵守的其他要求；

b) 支持预防不良和破坏性事件以及风险最小化；

c) 促进持续改进。

本国际标准的主体部分包含可客观审计的通用标准。关于支持安保业务管理技术的指南载于其他附件。

对于有此需要的组织，外部或内部审核过程可验证其SOMS是否符合本国际标准。验证可由可接受的第一、第二或第三方机制进行。验证不需要第三方认证。

本国际标准不包括其他管理体系的具体要求，例如质量、职业健康与安全或韧性管理的要求——尽管其要素可以与其他管理体系的要素对齐或整合。组织可以根据需要调整现有的管理体系（或多个体系），以建立符合本国际标准标准的SOMS。然而，根据预期目的和涉及的利益相关者不同，管理体系的各个要素的应用可能会有所不同。

SOMS的详细程度和复杂性、文档编制的程度以及投入的资源将取决于多个因素，如系统的范围、组织的规模及其活动、产品、服务和供应链的性质。特别是对于中小企业而言，情况可能尤为如此。

本国际标准为安全运营管理和计划提供了一套通用标准。本国际标准使用的术语强调概念的共性，同时承认在各个学科中术语使用的细微差别。为了与ISO 31000保持一致，风险评估是风险识别、分析和评价的过程。

参考书目

[1] ISO 9000：2015，质量管理体系—基础和词汇

[2] ISO 9001，质量管理体系要求

[3] ISO 14001，环境管理体系-要求和使用指南

[4] ISO/IEC 17021-1，符合性评估—管理体系审核和认证机构的要求—第1部分：要求

[5] ISO 19011：2011，管理体系审核指南

[6] ISO/IEC 27000：2014，信息技术-安全技术-信息安全管理体系-概述和词汇

[7] ISO/IEC 27001，信息技术-安全技术-信息安全管理体系-要求

[8] ISO/IEC 27035，信息技术-安全技术-信息安全事件管理

[9] ISO 28000，供应链安全管理系统规范

[10] ISO 31000，风险管理-原则和指南

[11] OHSAS 18001，职业健康与安全管理

[12] ASIS International（2008），ASIS国际安全术语词典。[在线]。可从以下网址获取：< https://www.asisonline。org/Membership/Library/Security-Glossary/Pages/Security- Glossary-A.aspx >

[13] ASIS International4)（2012），ANSI/ASIS PSC.1-2012，私营保安公司运营质量管理体系——要求与指南标准

[14] ASIS International（2012），ANSI/ASIS PSC.2-2012，私营保安公司运营质量的符合性评估和审核管理体系标准

[15] ASIS International（2013），ANSI/ASIS PSC.3-2013，私营保安服务提供商质量保证管理体系分阶段实施成熟度模型

[16] ASIS International（2013），ANSI/ASIS PSC.4-2013，私营保安公司海上作业的质量保证和安全管理指南

[17] ASIS International（2009），ANSI/ASIS SPC.1-2009，组织弹性：安全准备和连续性管理系统——要求及使用指南

[18] ASIS International（2012），ANSI/ASIS SPC.4-2012，组织弹性管理系统分阶段实施成熟度模型

[19]《关于战时保护平民的公约》（日内瓦第四公约），1949年8月12日；< http://www.icrc.org/ihl.nsf/INTRO/380 >

[20]《关于陆地战争法规和惯例的公约》（海牙第四公约）；1907年10月18日；<http://avalon.law.yale.edu/20th_century/hague04.asp>

[21]红十字国际委员会，关于国际人道主义法中直接参加敌对行动概念的解释性指南，日内瓦，红十字委员会，2009年5月

4) ASIS文档可在< http://www.asisonline.org >中找到。

[22] Parks W.H.关于随军平民和民用承包商角色的政策和法律演变，华盛顿特区，(c)。Hays Parks，W.，2005

[23]1949年8月12日日内瓦四公约关于保护非国际性武装冲突受难者的附加议定书（第二议定书），1977年6月8日，< http://www.icrc.org/ihl. nsf/INTRO/475？OpenDocument >

[24]联合国，1990年《执法人员使用武力和火器的基本原则》，http://www.ohchr.org/EN/ProfessionalInterest/Pages/UseOfForceAndFirearms.aspx

[25]联合国，《禁止酷刑和其他残忍、不人道或有辱人格的待遇或处罚公约》（CAT）1984年。< http://www2.ohchr.org >

[26]联合国。《消除对妇女一切形式歧视公约》（CEDAW）1979年，< http://www.un.org >

[27]联合国。《防止及惩治灭绝种族罪公约》，1948年，<http://www.un.org>

[28]联合国，《儿童权利公约》（CRC）1989年，< http://www2.ohchr.org >

[29]联合国，《全球契约原则》，http://www.unglobalcompact。org/AboutTheGC/ TheTenPrinciples/index.html >

[30]联合国。劳工组织《关于工作基本原则和权利宣言》。国际劳工大会，第八十六届会议，日内瓦，1998年6月18日（附件于2010年6月15日修订），<http://www.ilo.org/declaration/thedeclaration/textdeclaration/lang--en/index.htm>

[31]联合国。《公民权利和政治权利国际公约》（ICCPR）1966年，< http:// www2.ohchr.org >

[32]联合国。《经济、社会、文化权利国际公约》（ICESCR）1966年，< http://www2.ohchr.org >

[33]联合国。《消除一切形式种族歧视国际公约》（ICERD）1966年，< http://www2.ohchr.org >

[34]联合国。《世界人权宣言》，1948年，< http://www.un.org >

[35]联合国。保护、尊重和补救：工商企业与人权框架A/HRC/8/5 2008年4月7日，< http://www.reports-and-materials.org/Ruggie-report-7- Apr-2008.pdf >

[36]美国国防部，国防部指令5210。56、从事安全、法律和秩序或反情报活动的国防部人员携带枪支和使用武力，华盛顿特区，USGPO，2011年4月1日

[37]《安全与人权自愿原则》，http://www.voluntaryprinciples.org/files/ voluntary_principles_english.pdf

ICS 03.080.20; 13.310
基于98页的价格