CTS

广东中嘉认证有限公司企业标准

保安服务管理
体系认证技术规范

2025-08-18发布　　2025-08-18实施

广东中嘉认证有限公司　　发布

目录

前言

本标准按照GB/T 42765-2023给出的规则起草。

本标准由广东中嘉认证有限公司起草。

本标准主要起草人：彭一康、邱可为、丁飞、吴峰、罗延君、麦永洪、陈燕

1、范围

本文件确立了建立、实施、保持和持续改进保安服务管理体系的原则、要求以及使用指南，为开展保安服务提供风险管理的框架。

本文件适用于有如下需求的从事保安业务的组织：

a)建立、实施、保持并持续改进保安服务管理体系；

b)评估保安服务与其管理方针的一致性；

c)证实稳定满足客户需求的能力。

2、术语和定义

下列术语和定文适用于本文件。

2.1资产

组织中具有有形或无形价值的任何事物。

注1:有形资产包括人(在本文件中予以重点阐述)、实物和环境资产。

注2:无形资产包括信息 、品牌和信誉。

2.2审核

为获得客观证据并对其进行客观的评价，以确定满足审核准则的程度所进行的系统的、独立的并形成文件的过程。

注1:审核可以是内部审核(第一方)或外部审核(第二方或第三方)，也可以是多体系审核(包括两个或两个以上专业)。

注2:组织自身可进行内部审核 ，或由一个外部实体代表其进行内部审核。

注3:“证据”与“准则”的定义见 GB/T 19000—2016。

2.3审核员

实施审核的人员。

2.4客户

雇用、曾经雇用或计划雇用一个组织来代表其进行保安服务的实体或个人，根据具体情况 ，可包括该组织与另一公司或其他单位分包的情况。

示例：用户、承包商、最终用户、零售商、受益人、买方。

注：客户可以是组织的内部(如 ，其他部门)或外部客户。

2.5能力

应用知识和技能实现预期结果的本领。

2.6沟通和咨询

组织管理风险时， 提供信息、共享信息、获取信息以及与利益相关方及其他各方，展开对话的持续、往复的过程。

注1: 信息可能涉及风险和保安服务管理的存在、性质、形式、可能性、严重性、评价、可接受性和应对或其他等方面。

注2: 咨询是组织与其利益相关者及其他方在针对某一问题做出决策或确定方向前，针对该问题进行的双向沟通过程。咨询是:

——通过影响力而不是通过权力来影响决策的过程;

——对决策的输入，而非参与决策。

2.7社会群体

拥有共同利益的相关组织、个人和群体。

2.8合格

满足要求。

3.9持续改进

提高绩效的循环活动。

2.10后果

某事件对目标影响的结果。

注1:一个事件可导致一系列后果

注2:后果可以是确定的 ，也可以是不确定的 ，对目标的影响可以是正面的 ，也可以是负面的。

注3:后果可以定性或定量表述。

注4:一个事件引发一连串事件时 ，最初的后果可能通过累积效应升级。

注5:后果按影响的等级或严重程度进行分级。

2.11纠正

为消除已发现的不合格所采取的措施。

2.12纠正措施

为消除不合格的原因并防止再发生所采取的措施。

2.13危害性分析

基于组织的任务或职责的重要性，及风险人群、非预期事件或干扰性事件对组织实现预期的影响性，系统识别和评估组织资产的过程。

2.14关键控制点

能够施加控制，且使威胁或危险得到预防、消除或降至可接受水平的点、步骤或过程。

2.15干扰性事件

使所规划的活动、业务或功能中断的事件或变化 ，无论是可预见的或不可预见的。

2.16成文信息

组织需要控制和保持的信息及其载体。

注1:成文信息可以任何格式和载体存在 ，并可来自任何来源。

注2:成文信息可涉及：

——管理体系 ，包括相关过程；

——为组织运行产生的信息(一组文件)；

——结果实现的证据。

2.17有效性

完成策划的活动并得到策划结果的程度。

2.18演练

用以评估保安服务管理方案，排练团队成员和人员角色，测试组织系统(如技术、报告 规程、管理等)以证明保安业务管理能力的活动。

注:演练包括培训和调节组织工作人员的活动，以响应组织实现最高绩效的目标。

2.19事件

某一类情形的发生或变化。

注1:事件的性质 、可能性(3. 26)和后果(3. 10)不可能完全可知。

注2:事件可以是一个或多个情形 ，并且可以由多个原因导致。

注3:可以确定与事件相关的可能性。

注4:事件可由一个或多个没有发生的情形组成。

注5:造成某一结果的事件有时被称为“事故”。

2.20事故

造成伤亡、资产损害、对内外部利益相关方的合法权益和基本自由产生不利影响等后果

的事件。

2.21固有危险物

如果掌握在未经授权的组织或个体手中，将会造成死亡威胁或严重人身伤害的物品。

示例：枪支、弹药、炸药、化学制剂、生物制剂和毒素、核能或放射性物质等。

2.22完整性

保障资产准确性和完整性的特性。

2.23利益相关方

可影响决策或活动、受决策或活动影响、自认为受决策或活动影响的个人或组织。

注1:决策者可以是利益相关方。

注2:受影响的社会群体和当地居民被视为外部利益相关方。

注3:本文件中对条文“利益相关方 ”的使用应与保安服务保持一致。

2.24关键绩效指标

组织为完成其战略和服务目标用来测量或比较绩效的可量化措施。

2.25防卫装备

依法提供保安服务时，为完成岗位任务和保障自身安全所需要的非杀伤性的自卫装备。

2.26可能性某件事发生的机会。

注1:无论是以客观的或主观的、定性或定量的方式来定义、度量或确定，还是用一般词汇或数学术语来描述(如概率，或一定时间内的频率)，在风险管理术语中，“可能性”一词都用来表示某事发生的机会。

2.27管理计划

具有明确规定和记录的行动计划，通常包含执行事件管理过程所需的关键人员、资源、服务和行动。

2.28管理体系

组织建立方针、目标和实现目标所需过程的相互关联或相互作用的一组因素。

注1:一个管理体系可以针对单一的领域或多个领域。

注2:体系因素包括组织的结构、岗位和职责、策划及运行。

注3:管理体系的范围可以包括整个组织、组织中可被明确识别的职能或可被明确识别的部门，以及跨部门的单一职能或多个职能。

注4:组织通过管理体系实施其方针并根据目标和指标采用以下方式实施：

——规定人员岗位、职责、权力等的组织结构；

——实现该目标和指标的系统过程和相关资源；

——针对该目标和指标用于对绩效进行评定的测量和评估方法学，结果的反馈用于改进体系计划；

——确保问题得到纠正、改进有机会得到确认和实施的评审过程。

2.29测量

确定数值的过程。

2.30监视

确定体系、过程或活动的状态。

注:确定状态可能需要检查 、监督或密切观察。

2.31不合格

未满足要求。

2.32目标

要实现的结果。

注1:目标可以是战略的、战术的或操作层面的。

注2:目标可以涉及不同的领域(如财务、职业健康与安全的和环境)，也可应用于不同层次[如战略、组织整体、项目、产品和过程]。

注3:目标可以用其他方式表述，如采用预期的结果、活动的目的或运行准则作为保安服务目标，或使用其他 有类似含义的词[如宗旨、指标]。

注4:在保安服务管理环境中，组织制定的保安服务目标与保安服务方针保持一致，以实现特定的结果。

2.33组织organization

为实现目标,由职责、权限和相互关系构成自身功能的一个人或一组人。

注：组织的概念包括但不限于代理商、公司、集团、商行、企事业单位、行政机构、合营公司、慈善机构或科研机构，政府或公共机构，或上述组织的部分或组合，无论是否为法人组织，公有的或私有的。

2.34外包outsource

安排外部组织承担组织的部分职能或过程。

注：虽然组织的管理体系包括外包功能或过程,但不包括外部组织。

2.35绩效performance

可测量的结果。

注1:绩效可能涉及定量的或定性的结果。

注2:绩效可能涉及活动、过程、产品(包括服务)、系统或组织的管理。

2.36策划planning

管理的一部分，致力于制定保安服务目标并规定必要的运行过程和相关资源以实现保安服务目标。

2.37方针policy

由最高管理者正式发布的组织的宗旨和方向。

2.38预防prevention

能够使组织避免、杜绝或限制非预期事件或潜在干扰性事件的措施。

2.39预防措施preventive action

为消除潜在不合格或其他潜在不期望情况的原因所采取的措施。

注1:一个潜在不合格可以有若干个原因。

注2:采取预防措施是为了防止发生，而采取纠正措施是为了防止再发生。

2.40保安从业单位security service provider; security company

依法设立的保安服务公司和自行招用保安服务人员单位的统称。

2.41程序procedure

为进行某项活动或过程所规定的途径。

注：程序可以形成文件，也可以不形成文件。

2.42过程process

输入转化为输出的相互关联或相互作用的一组活动。

2.43记录record

阐明所取得的结果或提供所完成活动的证据的文件。

注1:记录可用于正式的可追溯性活动，并为验证、预防措施和纠正措施提供证据。

注2:通常，记录不需要控制版本。

2.44要求requirement

明示的、通常隐含的或必须履行的需求或期望。

注1:“通常隐含”是指组织或利益相关方的管理或一般做法，所考虑的需求或期望是不

言而喻的。

注2:规定要求是经明示的需求，如：在成文信息中阐明。

2.45剩余风险residual risk

风险应对之后仍然存在的风险。

注1:剩余风险可包括未识别的风险。

注2:剩余风险还被称为“留存的风险”。

2.46恢复力resilience

组织对复杂变化环境的适应能力。

2.47资源resources

有潜在价值并可以被利用的资产、设施、设备、材料、产品或废弃物。

2.48评审review

确定管理体系及其组成要素实现规定目标的适宜性、充分性或有效性的活动。

2.49风险risk

不确定性对目标的影响。

注1:影响是指偏离预期，可以是正面的和/或负面的。

注2:不确定性是对事件、及其后果、或可能性、等信息缺乏理解或了解的状态。

注3:通常以潜在“事件”和“后果”或两者的组合来描述风险。

注4:通常用事件(包括情形的变化)的后果和事件发生的相关“可能性”的组合表示风险。

注5:目标可以有不同方面(如合法权益保护、安全管理、遵守法律、财务、健康和安全、环境等),也可以体现在不同层面[例如战略、组织范围、项目、产品和过程]。

注6:风险可分为故意、无意和自然性的来源。

2.50风险接受risk acceptance

接受某一特定风险的决定。

注1:风险接受可以不经风险应对,还可以在风险应对过程中发生。

注2:接受的风险要受到监视和评审。

2.51风险分析risk analysis

理解风险性质、确定风险等级的过程。

注1:风险分析是风险评价和风险应对决策的基础。

注2:风险分析包括风险估计。

2.52风险偏好risk appetite

组织寻求、保留或接受风险的准备。

2.53风险评估risk assessment

包括风险识别、风险分析和风险评价的全过程。

2.54风险准则risk criteria

评价风险重要性的依据。

注1:风险准则的确定需要基于组织的目标、外部环境和内部环境。

注2:风险准则可以源自标准、法律、政策和其他要求。

2.55风险评价risk evaluation

对比风险分析结果和风险准则,以确定风险和/或其大小是否可以接受或容忍的过程。

注：风险评价有助于风险应对的决策。

2.56风险识别risk identification

发现、确认和描述风险的过程。

注1:风险识别包括对风险源、事件及其原因和潜在后果的识别。

注2:风险识别可能涉及历史数据、理论分析、专家意见以及利益相关方的需求。

2.57风险管理risk management

在风险方面，指导和控制组织的协调活动。

2.58风险登记risk register

已识别风险的信息记录。注：风险评估过程中对已识别、分析和评价过的所有风险的汇编，包含可能性、后果、应对和风险所有者等信息。

2.59风险容忍risk tolerance

组织或利益相关方为实现目标在风险应对之后承担风险意愿。

注：风险容忍会受到客户、利益相关方、法律法规要求的影响。

2.60风险应对risk treatment

处理风险的过程。

注1:风险应对可以包括：

——不开始或不再继续导致风险的行动，以规避风险；

——为寻求机会而承担或增加风险；

——消除风险源；

——改变可能性；

——改变后果；

——与其他各方分担风险(包括合同和风险融资)；

——慎重考虑后决定保留风险。

注2:针对负面后果的风险应对有时指“风险消除”“风险预防”“风险降低”等。

注3:风险应对可能产生新的风险或改变现有风险。

2.61保安服务security operations；security services

由保安服务公司根据保安服务合同，派出保安员为客户单位提供的门卫、巡逻、守护、押运、随身护卫、安全检查以及安全技术防范、安全风险评估等服务；机关、团体、企业、事业单位招用人员从事的本单位门卫、巡逻、守护等安全防范工作；以及物业服务企业招用人员在物业管理区域内开展的门卫、巡逻、秩序维护等服务。

2.62保安服务管理security operation management

指导和管理组织关于保安服务的协调活动。

注:关于保安服务管理的指导和管理一般包括建立方针、策划和目标,指导运行过程(3.42)和持续改进。

2.63保安服务目标security operation objective

保安服务管理的目的。

注1:保安服务目标通常根据组织的保安服务方针制定。

注2:保安服务目标通常依组织中相关职能和级别作出规定。

2.64保安服务方针security operation policy

组织关于保安服务的总体意图和方向，由最高管理者正式发布。

注：一般保安业务方针与组织的总体方针一致，并为保安服务目标的制定提供框架。

2.65保安服务方案security operation programme

最高管理者支持的持续进行的管理和治理过程,确保采取必要的步骤来协调各项工作,实现保安服务管理体系的目标。

2.66保安服务人员security operation personnel

为组织直接或间接从事保安服务的人员。

注：根据GA/T 1279-2015的定义，保安员特指依法取得保安员证，为公民、法人和其他组织提供保安服务人员。

2.67自卫self-defence

保护自身或财产免受他人侵害。

2.68分包subcontracting

与外部组织签订合同以履行现有合同规定义务。

注1:当一方签订合同履行一系列服务时,它可以将其中一个或多个服务分包给“分包方”。

注2:母公司的子公司可被视为分包组织。

2.69供应链supply chain

组织、人员、过程、物流、信息、技术和资源之间的双向关系，从事活动并通过提供产品或服务创造价值。

注：供应链可以包括供应商、分包方、生产设施、物流供应商、内部配给中心、分销商、批发商及其他供应给终端用户的实体。

2.70指标target

为实现目标而制定的适用于组织的详细(或部分)绩效要求。

2.71威胁分析threat analysis

对可能会损害人身、资产、体系或组织、环境或社会群体的非预期事件的潜在原因进行识别、限制和量化的过程。

2.72最高管理者top management

指导和控制组织的最高级人员或群体。

注1:最高管理者在组织内有授权或提供资源的权力。

注2:如果管理体系的范围仅覆盖组织的一部分，在这种情况下，最高管理者是指管理和控制组织的这部分的一个人或一组人。

注3:最高管理者可被称为组织的领导者。

2.73非预期事件undesirable event

可能造成人身伤亡、资产损失或对内外部利益相关方的合法权益造成负面影响的事件。

2.74脆弱性分析vulnerability analysis

对可能造成后果的风险来源产生敏感性的识别和量化的过程。

3、认证模式

初次认证+监督审核+再认证+非例行监督（必要时）

4、组织环境

4.1理解组织及其环境

4.1.1总则

组织应确定与其宗旨相关并影响其实现保安服务管理体系预期结果的各种外部和内部因素。

管理体系框架的设计与实施应建立在对组织及其内外部运行环境理解基础之上。因此，组织应确定并记录其内部和外部环境，包括其供应链和分包方。组织在建立、实施和保持保安服务管理体系时，应考虑这些因素并确定优先顺序。

组织应评价可影响管理风险方式的内部和外部因素。

4.1.2内部环境

组织应识别、评价和记录以下内部环境，包括：

a)组织的目标、战略及经营使命；

b)实现目标的方针、计划及指南；

c)组织机构、岗位、职责和权限；

d)全面风险管理策略；

e)内部利益相关方；

f)价值观、道德和文化；

g)信息传递和决策过程；

h)能力、资源和资产；

i)程序、过程和实践；

j)活动、职能、服务及产品；

k)品牌及声誉。

4.1.3外部环境

组织应确定并记录其外部环境，包括：

a)文化与政策环境；

b)法律、法规、技术、经济、自然与竞争环境；

c)合同协定，包括合同范围内的其他组织；

d)公共基础设施与业务相关性；

e)供应链和承包商关系及承诺；

f)可能影响组织过程和/或目标的关键问题和趋势；

g)外部利益相关方的观点、价值观、需求及利益(包括服务区域内的社会群体)；

h)业务能力及权限界线。

4.1.4供应链和分包方信息收集与分析

组织应识别并记录其上下游供应链，尤其是使用可能对风险有影响，并有可能引发非预期或干扰性事件的分包方。组织的整体保安服务管理方案中应包括识别可能引起非预期事件或干扰性事件的重大风险的供应链风险管理。组织应确定并记录供应链和分包方在保安服务管理方案中的级别。

4.1.5确定风险准则

组织应确定并形成评价风险的准则。风险准则应体现组织的价值、目标及资源。确定风险准则时，组织应考虑：

a)主要活动、功能、服务、产品及利益相关方关系；

b)管理制度或法规不健全环境下业务运行中的业务环境及内在的不确定性；

c)与非预期事件、干扰性事件相关的潜在影响；

d)法律法规要求及组织承诺的其他要求(如合同义务、合法权益)；

e)组织的整体风险管理方针；

f)对其资产、业务造成威胁和后果的性质与类型；

g)风险可能性、后果及其等级确定方式；

h)利益相关方的需求和所受影响——尤其是人身、安全和合法权益(见C.6.1.2.3)；

i)信誉风险和感知风险；

j)组织及其客户风险容忍或风险规避的程度；

k)对多重风险的组合和排序。

虽然风险准则是在风险评估过程开始时建立的，但它们是动态的，应持续监视和评审其适宜性。

4.2理解利益相关方的需求与期望

组织应确定：

——与保安服务管理体系有关的利益相关方；

——这些利益相关方的要求。

为了履行合同并将风险降到最低，最高管理者应识别、评价并记录内外部利益相关方的利益。组织明确内外部利益相关方的需求和要求时，应考虑：

a)利益相关方的风险偏好；

b)客户规定的合同义务；

c)法律法规要求及自愿承诺；

d)提供保安服务对相关方合法权益的影响；

e)对外部利益相关方(如地方社会群体、客户及其他保安从业单位)的相互影响；

f)服务交付和不合格项的文件化记录要求。

4.3确定保安服务管理体系的范围

组织应明确保安服务管理体系的边界和适用性，以确定其范围(即整个组织，或其一个或多个组成部分或职能部门)。组织应考虑规模、性质、复杂性并从持续改进的角度确定保安服务管理体系范围。

在确定其范围时，组织应考虑：

——组织的目标，4.1.2和4.1.3所提及的内部和外部因素；

——4.2中所提及的要求；

——在组织环境中，对组织运营和活动产生不利影响的潜在可能性和后果的风险因素。

范围应形成文件并可获取。组织应确定适用保安服务管理体系的所有运营要素，以及适用的例外情况。

组织确定范围时，应保护组织的完整性，包括与利益相关方的关系。

适用性说明应根据风险评估和合法权益影响分析,定义适用于组织的范围、法律法规和合同义务以及运行环境的相关条款。这些条款一经确定，组织应予以处理和执行。具体的免责条款和其说明应被记录。

4.4保安服务管理体系

组织应按照本文件要求，建立、实施、保持并持续改进保安服务管理体系，包括所需过程及其相互作用。组织应按照本文件要求形成实现预期结果的文件，并持续改进其有效性。

当组织对体系适用范围内的某些过程和活动进行分包或外包时，应确保在其保安服务管理体系中对这些分包或外包过程和活动的控制予以识别和管理。

5、领导作用

5.1领导作用与承诺

5.1.1总则

最高管理者应通过以下方面，证实其在建立和实施保安服务管理体系并持续改进其有效

性方面的领导作用及承诺：

——确保制定保安服务的方针和目标，并与组织的战略方向相一致；

——确保将保安服务管理体系要求融入组织的业务运行过程；

——确保保安服务管理体系可获得所需的资源，用于建立、实施、运行、监视、评审、保持和改进保安服务管理体系；

——就有效开展保安服务管理并符合保安服务管理体系及法律法规要求的重要性进行沟通；

——确保保安服务管理体系实现预期结果；

——指导和支持员工对保安服务管理体系的有效性做出贡献；

——推动持续改进；

——支持其他相关管理者在其职责范围内发挥领导作用；

——按计划的时间间隔对保安服务管理体系进行管理评审。

最高管理者应通过监督其保安服务管理体系的建立和执行，以及鼓励个人将保安服务与尊重合法权益相结合作为组织使命和其文化的组成部分，从而为在保安服务管理体系所起的积极领导作用提供证实。

5.1.2符合性声明

最高管理者应制定符合性公开声明并公开发布，表明组织承诺并遵守保安服务管理体系和相关法律法规规定的责任，满足利益相关方对合法权益的期望。该符合性声明应满足以下要求：

a)形成文件、保持并实施；

b)传达到组织内外部利益相关方，并可被公众所获取；

c)获得最高管理者的批准。

5.2方针

最高管理者应制定保安服务方针：

——适合组织的宗旨；

——为建立保安服务目标提供框架；

——包括满足适用的法律及其他要求的承诺，包括组织签署的自愿承诺；

——包括持续改进保安服务管理体系的承诺；

——提供尊重合法权益的承诺；

——包括避免、预防和降低干扰性事件或非预期事件产生的可能性及其造成的后果的承诺。保安服务方针应：

——可获取并保持成文信息；

——在组织内得到沟通；

——传达到所有为组织工作或代表组织工作的人员；

——适宜时，可为有关相关方所获取；

——获得最高管理者的批准；

——在计划时间间隔内或出现重大变化时得到评审。

5.3组织岗位、职责和权限

最高管理者应确保组织相关岗位的职责、权限得到分配、沟通。

最高管理者应在组织内指定一人或多人，不管其是否有其他职责，应使其具有以下方面的能力、岗位、职责和权限：

a)确保保安服务管理体系符合本文件的要求；

b)向最高管理者报告保安服务管理体系的绩效；

c)确保保安服务管理体系按照本文件要求建立、沟通、实施和保持；

d)识别、监视并管理4.2中利益相关方的需求与期望；

e)确保可获得足够的资源；

f)推动整个组织对保安服务管理体系要求的认识；

g)向最高管理者报告保安服务管理体系的绩效以供评审并将其作为持续改进的依据。

最高管理者应确保那些负责实施和维护保安服务管理体系的人有必要的权限和能力，并对组织业务负责。

6、策划

6.1应对风险和机遇的措施

6.1.1总则

在策划保安服务管理体系时，组织应考虑4.1.2和4.1.3所提及的因素和要求，并确定需要应对的风险和机遇，以：

——确保保安服务管理体系能够实现其预期结果；

——预防或减少非预期影响；

——实现持续改进。

6.1.2法律法规和其他要求

组织应确保在建立、实施和保持保安服务管理体系时考虑适用的法律法规和其他要求：

a)识别与保安服务相关的法律法规、合同、执照及其他要求和承诺；

b)识别法律法规规定以外的与其业务和保安服务相关的合法权益责任；

c)确定如何将上述要求应用于组织的运营中，以及分包、外包的保安服务业务。

组织应记录上述信息并持续更新，应组织人员和相关方传达有关法律法规和其他要求。组织和其客户具有遵守上述法律法规和道德责任的义务。

6.1.3风险评估

组织应为保安服务管理体系(包括其相关的供应链合作方和分包方的活动)建立、实施和保持一个文件化的风险评估过程。该风险评估过程应包括：

a)风险识别——识别和评估威胁、弱点、后果和侵犯合法权益，用以识别由人为和自然事件可能引起的直接或间接影响组织的活动、资产、业务、职能和利益相关方战略、战术和运营等风险；

b)风险分析——系统地分析风险发生的可能性和后果，以确定对活动、职能、服务、产品、供应链、分包方、利益相关方关系、社会群体和环境的重要影响；

c)风险评价——系统地对风险控制和风险应对以及相关成本进行评价和优先级排序，以决定如何使之在风险准则可接受的水平内。

组织应：

a)记录、持续更新上述信息，并确保信息的安全；

b)定期评审保安服务管理的范围、方针、风险准则和风险评估是否适用于组织的内部和外部环境；

c)在组织内部环境或组织的经营环境、流程、职能、服务、合作关系和供应链变化时，重新进行风险评价；

d)评价风险管理和增强可靠性、恢复力的直接和间接的收益和成本；

e)事故后和演习后评价风险应对方案的实际有效性；

f)确保在建立、实施和运行保安服务管理体系时考虑到优先级高的风险和影响；

g)监视和评价风险管理和风险应对的有效性。

风险评估应识别需要进行管理的活动、业务和过程，输出应包括：

a)形成包含风险应对方法的风险优先排序记录；

b)风险接受的依据；

c)关键控制点(CCP)的识别；

d)外包和分包方控制要求。

组织应建立与保安服务一致的监视、评估、评价和应对风险环境变化的过程。组织应策划：

a)应对这些风险和机遇的措施；

b)如何在保安服务管理体系过程中整合并实施这些措施及如何评价这些措施的有效性。

6.1.4内部和外部风险沟通和咨询

在风险评估过程中，组织应与内外部利益相关方建立、实施和保持文件化的沟通和咨询过程，以确保：

a)明确服务目标和客户的利益(客户包括受保护的人员、组织、社会群体和/或活动等)；

b)风险被充分识别和沟通；

c)明确内外部利益相关方的利益；

d)风险和风险应对方法已与合适的利益相关方沟通；

e)明确与分包方和供应链内部的从属和联系；

f)保安服务风险评估过程与其他管理准则可对接；

g)风险评估是在与组织及其分包方和供应链相关且适当的内外部环境和参数内进行的。

6.2保安服务目标及实现策划

6.2.1总则

组织应针对相关职能和层次建立保安服务目标。保安服务目标应：

a)与方针保持一致；

b)可测量；

c)考虑适用的要求；

d)予以监视；

e)予以沟通；

f)适时更新。

组织应保持有关保安服务目标的成文信息。

策划如何实现保安服务目标时，组织应确定：

——要做什么；

——需要什么资源；

——由谁负责；

——何时完成；

——如何评价结果。

组织应建立、实施和保持文件化的目标和指标来进行风险管理，以预测、避免、预防、阻止、减少、响应干扰性事件或非预期事件的发生并从中恢复。文件化目标和指标应能为组织建立内部和外部预期，为组织的指标完成、产品和服务交付、职能运作起关键作用的分包方和供应链建立内部和外部预期。

目标应来源于保安服务方针和风险评估，且保持一致，包括承诺：

a)通过降低可能性和后果实现风险最小化；

b)遵守法律法规及保障合法权益；

c)财务、运营和商业要求(包括分包方和供应链承诺)；

d)持续改进。

组织在建立、评审目标和指标时，应考虑其财务、运营和商业要求，法律法规和其他要求，合法权益影响，重大风险、技术方案和利益相关方的意见等。

与关键绩效相关联的指标应能以定性和/或定量的方式进行计算。指标应来源于保安服务目标且保持一致，同时应：

a)达到一定的详细程度；

b)与风险评估相符；

c)具体、可测量、可实现、有相关性且具有时效性；

d)传达给所有相关员工和包括分包方和供应链合作伙伴第三方，使他们了解个人义务；

e)定期评审，确保与保安服务目标保持一致并进行相应的修改。

6.2.2实现保安服务运行和风险应对目标

组织应建立、实施和保持可实现保安服务和风险应对目标的方案。方案用于管理和应对与其运行、分包方和供应链相关的风险，应实现优化和优先排序。组织应建立、实施和保持文件化的风险应对过程，考虑以下因素：

a)尽可能消除风险来源；

b)消除和降低某个事件及其后果发生的可能性；

c)消除、降低或减缓危害性后果；

d)与其他各方分担风险，包括风险保险；

e)将风险分散至其他资产和职能；

f)通过知情决定接受风险或寻求机遇；

g)规避或暂停引起风险的活动。

最高管理者应：

a)评估用以消除、减少或保留风险的各方案的收益和成本；

b)评价其保安服务方案，以确定这些措施是否引发新的风险；

c)定期评审因风险应对带来的外部环境的变化，包括法律法规和其他要求，以及组织的方针、设施、信息管理体系、活动、职能、产品、服务和供应链的变化。

7、支持

7.1资源

7.1.1总则

组织应确定并提供所需的资源，以建立、实施、保持和持续改进保安服务管理体系，同时应考虑：

a)现有内部资源的能力和局限；

b)需要从外部获得的资源。

可利用资源包括内部及外包的相关的信息、管理工具、人力资源、技术和防护设备以及后勤支持等，其中人力资源又包括有相关经验和专业知识技能的人员。

7.1.2结构要求

7.1.2.1总则

组织应是法人实体或法人实体的确定部分。组织的各层级(包括在其范围内的子公司)，应有明确的管理结构显示管理和义务。

7.1.2.2组织架构

明确定义的管理结构应确定其运行和服务的岗位、责任和权限。组织应：

a)记录其组织架构，证实管理的义务、责任和权限；

b)明确并记录组织是否是法人实体的一部分以及与该法人实体其他部分的关系；

c)明确其保安服务管理体系范围内的任一合资企业或合伙人关系的安排。

7.1.2.3保险

组织应证明其有保险，能承担因业务和活动(与其风险评估一致)引起的风险和相关责任。

组织应确保保险适当地覆盖到了其外包或分包服务、运行或职能活动。

7.1.2.4外包和分包

组织对分包或外包活动、职能和业务应有清晰明确的流程。组织应建立、记录、沟通和监视行为准则和特定条款中就保安服务和尊重合法权益方面对分包方和外包伙伴规定的要求。

组织应对其分包或外包活动有一份文件化协议，包括：

a)分包方承诺遵循组织同样认可且在本文件中所述的法律法规、道德以及合法权益的承诺与义务；

b)风险报告过程，以及非预期事件和干扰性事件的发生和应对；

c)保密和利益冲突协议；

d)所提供服务的明确定义和文件记录；

e)命令、控制的范围及局限；

f)外包伙伴与分包方之间支持关系的界定；

g)与本文件适用条款的一致性。

7.1.2.5财务和管理程序

组织应制定财务和管理的控制程序，以支持在所有策划和运行、干扰性事件或非预期事件的预期和应对中提供有效的保安和风险管理。程序应：

a)确保可以加快财政决策的制定；

b)遵照既定的权限级别和会计原则；

c)在与客户协商、协调中得以确立。

7.2能力

7.2.1总则

组织应：

——确定可能会影响保安服务绩效的人员具备胜任的能力；

——基于适当的教育、培训或经验，确保这些人员是胜任的；

——适用时，采取措施以获得所需的能力，并评价措施的有效性；

——保留适当的成文信息，作为人员能力的证据。

注：适用措施可包括对在职人员进行培训、辅导或重新分配工作，或者聘用、外包胜任的人员。

7.2.2能力认定

组织应确定与其保安服务有关的能力、能力水平和培训需求，尤其是每个人的职能绩效应与法律法规和合同义务一致，并保障合法权益。

组织应建立、实施和保持程序，以确保提供服务的人员在下列各方面都能具备出适当的能力水平：

a)保安职能的履行；

b)风险评价；

c)管理风险评价中识别的风险和与其工作相关的潜在合法权益影响；

d)在其所处环境中的文化，如习俗和宗教等；

e)减少干扰性事件或非预期事件发生可能性和/或结果的程序，包括应对和报告事件的应对和缓解程序；

f)事故报告和文件化程序；

g)急救、健康和安全程序；

h)防卫装备使用，包括组织授权和规定的特定防卫装备的机械操作及实弹演练，以适用于特定的保安服务。

i)与保安业务相关的防卫装备的使用限制；

j)沟通协议、方法及程序；

k)内外利益相关方的申诉程序。

7.2.3培训和能力评定

组织应提供能力培训，并制定衡量检验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，以证明所需的能力和熟练程度。

组织应：

a)为培训方案建立胜任能力指标；

b)通过培训传授理念：尊重合法权益是组织核心价值观和管理的一部分；

c)对所有批准在履行其职责时配备防卫装备的人员提供岗前和定期在岗的理论、体能、机械知识、实弹演练的培训并评定；

d)按照法律法规或合同要求，为使用防卫装备提供反复培训和提高培训效果，以确保相关人员具备组织要求的能力等级；

e)确定需要定期进行培训的其他能力，以保持所需的绩效水平和适应新的要求；

f)对符合保安服务管理体系方针、程序、要求的重要性，以及违反保安服务管理体系和保安服务规定程序的潜在后果，通过培训予以说明。

7.2.4成文

组织应保留以下记录：

a)能力鉴定和检验指标；

b)培训方案；

c)为代表其工作的人员提供培训和评定的相关记录。

7.3意识

组织应确保在其控制下工作的人员知晓：

7.4沟通

7.4.1总则

——保安服务方针；

——相关的保安服务目标；

——他们对保安服务管理体系有效性的贡献，包括改进绩效的益处；

——不符合保安服务管理体系要求的后果。

组织应确定与保安服务管理体系相关的内外部沟通，包括：

——沟通什么；

——何时沟通；

——与谁沟通；

——如何沟通；

——谁来沟通。

组织应为下列事项建立、实施和保持程序：

a)与内外部利益相关方的沟通；

b)接收、记录和应对内外部利益相关方的沟通；

c)定义并确保在非典型情况和干扰期间的沟通方式的可用性；

d)正常和异常情况下的沟通体系的常规测试。

沟通程序应考虑业务信息的敏感性和对信息共享的法律约束。

7.4.2运行沟通

组织应制定沟通程序，以分享有关保安团队活动、位置、运行和后勤状态以及向公司管

理层、客户和其他保安团队的相关威胁信息和事故报告等。这应包括向政府、其他保安团队和紧急医疗支持请求立即提供援助的程序。

组织应确保所有层级的人员都能接受和理解口头或书面形式的沟通，并且所有级别可用特定的语言或方式予以回应，这种回应可被内外部利益相关方所恰当理解。

保安团队应能够以受保护一方理解的形式向其传达与安全有关的信息。

7.4.3风险沟通

根据以人为本的原则和利益相关方协商的结果，组织应决定是否就重大风险及其影响和处理，向利益相关方进行外部沟通，并记录其决定。若决定向外部沟通，应建立和实施一套或多套方案，用于外部沟通(包括警告、报警和通报媒体等)。

7.4.4投诉和申诉沟通程序

应将投诉和申诉程序传达给内外部利益相关方。程序应在网站上公开，并尽可能减少由语言、教育水平或对害怕报复及考虑保密性和隐私所引起的访问障碍。

7.4.5与举报人沟通

对于有理由相信已出现不符合本文件的组织工作人员，组织应与代表其工作的人员进行沟通，他们有权向内部和向外部有关当局匿名报告不符合规定的情况。

7.5成文信息

7.5.1总则

组织的保安服务管理体系应包括：

——本文件要求的成文信息，包括记录；

——保安服务方针、符合性说明、目标和指标；

——保安服务管理体系范围说明；

——适用性说明；

——保安服务管理体系的主要元素及其相互作用，以及相关文件的引用说明；

——保安服务管理体系有效实施和运营所需要的文件化信息；

——组织所确定的、为确保保安服务管理体系的有效性所需的成文信息。

注：对于不同组织，保安服务管理体系成文信息的多少与详略程度可以不同，取决于：

——组织的规模，以及活动、过程、产品和服务类型；

——过程及其相互作用的复杂程度；

——人员的能力。

7.5.2创建和更新

7.5.2.1总则

在创建和更新成文信息时，组织应确保适当的：

——标识和说明(如标题、日期、作者、索引编号)；

——形式(如语言、软体版本、图表)和载体(如纸质的、电子的)；

——评审和批准，以确保适宜性和充分性。

7.5.2.2记录

组织应建立并保持记录，以证明符合保安服务管理体系的要求。记录应包括下列内容：

a)本文件要求的记录；

b)执照和经营许可证；

c)人员筛选；

d)培训记录；

e)过程监视记录；

f)检查、维护和校准记录；

g)相关分包方和供应商记录；

h)事故报告；

i)事故调查和处理记录；

j)审计结果；

k)管理评审结果；

l)外部沟通决策；

m)适用法律法规要求的记录；

n)重大风险和影响记录；

o)防卫装备库存和防卫装备发放收据；

p)管理体系会议记录；

q)保安、保安服务和合法权益绩效信息；

r)与利益相关方的沟通。

7.5.3成文信息的控制

应控制保安服务管理体系和本文件所要求的成文信息，以确保：

a)在需要的场合和时机，均可获得并适用；

b)予以妥善保护(如防止泄密、不当使用或缺失)。

为控制成文信息，适用时，组织应进行下列活动：

——分发、访问、检索和使用；

——存储和防护，包括保持可读性；

——更改控制(如版本控制)；

——保留和处置。

组织应建立、实施、维护程序，以：

a)在发布之前对文件的充分性进行审批；

b)保护信息敏感性和保密性；

c)审核，必要时更新和重新批准文件；

d)记录对文件的修订；

e)随时更新和获批的文件；

f)确保文件保持清晰和易于识别；

g)确保文件的外部来源经过识别并且其分配受控；

h)防止对作废文件的无意使用；

i)确保对作废文件的合理、合法及透明的销毁。

对于组织确定的策划和运行保安服务管理体系所必需的来自外部的成文信息，组织应进行适当识别，并予以控制。

注：对成文信息的“访问”可能意味着允许查阅，或者意味着允许查阅并授权修改。

组织应建立、实施和维护程序，以保护记录的敏感性、机密性和完整性，包括访问、识别、存储、保护、检索、保留和销毁记录。应按合同和适用法律的要求保留记录。雇佣和服务记录应至少保留7年，或按适用法律要求进行保留。组织应对文件进行安全备份以确保其完整性，文件仅限授权人员使用，并防止未经授权的披露、修改、删除、损坏、变质或丢失。

8、运行

8.1运行的策划和控制

8.1.1总则

组织应按照体系的要求，策划、实施和控制所需的过程，并通过以下的方式实施6.1确定的措施：

——为过程建立准则；

——按照准则实施过程控制；

——在必要的范围和程度上保留成文信息，以确信过程已经按策划进行。

组织应识别与已确定的重大风险相关的活动，以及符合组织保安服务管理方针、风险评估、目标和指标的活动，以确保活动能在规定的情况下进行，使组织能够：

a)与法律法规和监管要求相一致，包括营业执照和保安服务许可证等；

b)在保护客户声誉的前提下完成指标；

c)遵守相关的法律法规以及本文件所述的其他义务；

d)保障代表组织工作的人员的安全、健康和权利；

e)尊重当地社会群体的权利；

f)实施风险管理控制，以尽量降低干扰性事件或非预期事件发生的可能性和后果；

g)实现其保安服务运行目标和指标。

组织应建立、实施和保持文件化程序，以控制因缺失相关程序而可能导致的偏离保安服务管理体系政策、目标和指标的情形。

组织应对计划内的变更进行控制，并对非预期变更的后果予以评审，必要时应采取措施降低任何不利影响。

组织应确保外包过程可控。

8.1.2保安服务的要求

8.1.2.1客户沟通

与客户沟通的内容应包括：

a)提供有关保安服务的信息；

b)处理问询、合同或协议，包括更改；

c)获取有关保安服务的客户反馈，包括客户投诉；

d)处置或控制客户财产；

e)关系重大时，制定应急措施的特定要求。

8.1.2.2保安服务要求的确定

在确定向客户提供保安服务的要求时，组织应规定：

a)适用的法律法规要求；

b)客户明示的要求；

c)组织认为的必要要求；

d)提供的保安服务能够满足所声明的要求。

8.1.2.3保安服务要求的评审

组织应确保有能力向客户提供满足要求的保安服务。在承诺向客户提供保安服务之前，组织应对如下各项要求进行评审：

a)客户规定的保安服务要求，包括增值服务的要求；

b)客户虽然没有明示，但规定的服务范围或已知的预期服务范围所必需的要求；

c)组织规定的要求；

d)适用于保安服务的法律法规要求；

e)与前述不一致的合同或协议要求；

f)组织应确保与前述不一致的合同或协议要求已得到解决；

g)若客户没有提供成文的要求，组织在接受客户要求前应对客户要求进行确认。

适用时，组织应保留与下列方面有关的成文信息：

a)评审结果；

b)保安服务的新要求。

8.1.2.4保安服务要求的更改

若保安服务要求发生更改，组织应确保相关的成文信息得到修改，并确保相关人员知道已更改的要求。

8.1.3保安服务的设计和开发

8.1.3.1总则

组织应确立、实施及记录和保存适当的设计和开发过程，以确保后续的保安服务提供。

8.1.3.2设计和开发策划

在确定设计和开发的各个阶段和控制时，组织应考虑：

a)适用的法律法规要求；

b)新型保安服务的性质、持续时间和复杂程度；

c)确认客户的需求和期望及后续保安服务提供的要求；

d)对新型保安服务实施安全风险评估，确定是否具备可操作性；

e)对设计和开发所需的过程阶段进行评审；

f)设计和开发验证及确认活动；

g)设计和开发过程涉及的职责和权限；

h)新型保安服务设计和开发所需的内部和外部资源；

i)设计和开发过程参与人员之间接口的控制需求；

j)证实已经满足设计和开发要求所需的成文信息。

8.1.3.3设计和开发输入

组织应针对所设计和开发的具体类型的保安服务，确定必需的要求。应考虑：

a)确认客户的需求和期望；

b)来源于以前类似设计和开发活动的信息；

c)法律法规要求；

d)组织承诺实施的标准或行业规范；

e)由服务性质所导致的潜在的失效后果。

针对设计和开发的目的，输入应是充分和适宜的，且应完整、清楚。

相互矛盾的设计和开发输入应得到解决。

组织应保留有关设计和开发输入的成文信息。

8.1.3.4设计和开发控制

组织应对设计和开发过程进行控制，以确保：

a)规定拟获得的结果；

b)实施评审活动，以评价设计和开发的结果满足要求的能力；

c)实施验证活动，以确保设计和开发输出满足输入的要求；

d)实施确认活动，以确保形成的保安服务能够满足规定的使用要求或预期服务范围；

e)针对评审、验证和确认过程中确定的问题采取必要措施；

f)保留这些活动的成文信息。

注：设计和开发的评审、验证和确认具有不同目的。根据组织的产品和服务的具体情况，可单独或以任意组合的方式进行。

8.1.3.5设计和开发输出

组织应确保设计和开发输出：

a)满足输入的要求；

b)满足后续保安服务提供过程的需要；

c)制定实施方案并进行评价；

d)确定实施方案的可操作性；

e)包括或引用监视和测量的要求，适当时，包括接收准则；

f)规定服务特性，这些特性对于预期目的、安全和正常提供是必需的。

组织应保留有关设计和开发输出的成文信息。

8.1.3.6设计和开发更改

组织应对保安服务设计和开发期间以及后续所做的更改进行适当的识别、评审和控制，以确保这些更改对满足要求不会产生不利影响。组织应保留下列方面的成文信息：

a)设计和开发更改；

b)评审的结果；

c)更改的授权；

d)为防止不利影响而采取的措施。

8.1.4保安服务的提供

组织应建立、实施和保持过程，以支持对人员、有形和无形资产以及其他与安全相关的职能的保护，包括但不限于：

a)管理在风险评估中已识别出的风险；

b)客户或主管部门要求的特定职能；

c)其他任务和环境的特定职能。

组织所提供的保安服务内容包括但不限于门卫、巡逻、守护、押运、随身护卫、安全检查、安全技术防范、安全风险评估等，组织应确保在受控条件下进行保安服务的提供。

适用时，受控条件应包括以下内容。

a)可获得成文信息，以规定：

1)拟提供的服务或进行的活动的特性；

2)拟获得的结果。

b)可获得和使用适宜的监视和测量资源。

c)在适当阶段实施监视和测量活动，以验证是否符合过程或输出的控制准则以及产品和服务的接收准则。

d)为过程的运行使用适宜的基础设施，并保持适宜的环境。

e)配备胜任的人员，包括所要求的资格。

f)若输出的结果不能由后续的监视或测量加以验证，应对服务提供过程实现策划结果的能力进行确认，并定期再确认。

g)采取措施防止人为和自然事件不符合发生。

h)实施放行、交付和交付后的活动。

i)对保安服务的更改进行必要的评审和控制，以确保持续地符合要求。

8.1.5尊重合法权益

组织应建立、实施和保持程序，以尊重所有人员的尊严和合法权益，并报告任何不合格情况。组织应建立并向代表组织工作的人员传达符合尊重合法权益原则的程序，以及适用于该组织保安服务的法律法规、合同要求。

8.1.6非预期事件或干扰性事件的预防与管理

组织应建立、实施和保持程序，记录组织如何预防、减缓并应对非预期和干扰性事件的发生，应考虑以下几点：

a)保安职能的履行；

b)保护生命，加强员工和内外部利益相关方人员的安全；

c)尊重生命和人格尊严；

d)首要考虑对非预期事件的预测和预防；

e)应对和缓解干扰性事件，以防止其升级；

f)尽量减少对运行和服务的破坏；

g)尽量降低对当地社会群体造成不利影响的可能性；

h)通报有关部门；

i)总结经验教训，采取纠正及预防措施以避免复发。

8.2建立行为规范和道德准则

组织应建立、实施和保持道德准则，作为代表组织工作的所有人员(包括雇员、分包方和外包合作伙伴)的行为守则。该道德准则应形成书面文件，确立保安服务中职业行为的重要性并明确传达尊重合法权益。该道德准则应确保所有代表组织工作人员理解其防止和报告任何侵犯合法权益的责任。

组织应向所有代表其工作的人员和客户传达该道德准则，并成文相关信息。

8.3防卫装备使用

8.3.1总则

组织应建立并形成文件的程序，指导保安从业人员在服务过程中正确使用防卫装备。程序应具体说明组织业务范围和执行任务的条件，且获得客户的同意。

注：防卫装备是指保安从业人员依法提供保安服务时，为完成岗位任务和保障自身安全配备的保安棍、防暴叉等防卫装备及执行武装守护、押运任务配备的防暴枪支弹药。

防卫装备使用程序应包含：

a)保安从业人员配备和使用防卫装备的授权；

b)防暴叉使用；

c)保安棍使用；

d)防暴枪弹使用(仅适用于从事武装守护押运服务的组织)；

e)其他防卫装备使用；

f)培训。

8.3.2防卫装备使用原则

程序应明确防卫装备使用原则，应包括：

a)根据当时适用的情况，防卫装备使用强度、持续时间和幅度应合理；

b)如形势或环境允许，警告相应人员并提供撤回威胁的机会或停止威胁行动；

c)如形势和环境允许，降低防卫装备的使用强度；

d)对防卫装备使用强度的监督控制，以及监督控制授权的限制。

程序应明确，为防止人员被持续攻击或受到伤害，防止组织所保护的财产遭到损失，保安从业人员可使用防卫装备，使用防卫装备时应以有效制止为目的。

对有关行为人采取制服措施，以尽快消除安全威胁时，保安从业人员可使用防卫装备。包括下列情况：

a)法律法规赋予的正当防卫权利；

b)保卫他人；

c)保卫财产，此类财产包括关键基础设施和固有危险物(如果丢失或损坏，将立即威胁生命或造成严重人身伤害)；

d)其他紧急情况。

8.3.3防卫装备授权

从事专职守护、押运业务的组织应建立和成文其人员在执行保安服务时配备防卫装备的授权程序。授权应仅面向被组织确定适合执行任务，且经背景审查适合履行职责的员工。

防卫装备发放给个人之前，组织应以书面形式授权并保留记录。

8.3.4防卫装备使用培训

组织的防卫装备使用程序应说明初次培训和周期性培训的要求。从事武装守护押运服务的保安人员更应充分接受熟悉枪支(文化课)、实弹射击和防卫装备使用等培训；枪支使用培训应为由人民警察院校、人民警察培训机构等负责的专业培训。组织应保留劳动关系存续的所有人员的培训记录和能力证明。

组织的防卫装备使用培训应包括下列要素：

a)适用于特定保安服务中正当防卫的法律；

b)从事武装守护、押运组织对其枪支、弹药授权、储存和携带政策的评审；

c)对使用防卫装备导致人员死亡或严重伤害的法律责任的审核；

d)可合理确定使用防卫装备的指令明显违法时，以服从上级指令为理由的辩护应属无效；

e)防卫装备使用原则的应用。

组织应开发员工可随身携带的培训教具，以帮助其员工理解、记忆和应用特定或适用的防卫装备使用规则。

8.4关键资源

8.4.1总则

最高管理者应提供建立、实施、保持和改进保安服务管理体系必要的可用资源。应包含信息、管理工具和人力资源(包括具有专业技能和知识的人员)及财务支持。应确定、记录和传达岗位、职责和权限，以促进有效的保安服务管理，包括具有承接性的控制、协调及监督责任。

为有效地处理非预期事件或干扰性事件，组织应成立具有明确岗位、适当职权和充足资源(包括安全有效的设备和经演练的作业计划及程序)的规划、安全、事故管理、响应及/或恢复团队。

如果组织选择分包或外包的过程对本文件要求一致性有影响，组织应确保上述过程可控。

8.4.2人员

8.4.2.1总则

组织应有足够数量具有适当能力的人员(雇员、承包商或分包方)来履行合同义务。应向人员提供相应的薪酬和待遇等，包括保险。组织应根据具体情况保护上述信息的机密性，并以各方都能理解的语言提供相关文件。

组织应为所有人员保持成文信息：

a)按照法律法规和合同义务的要求；

b)与个人及其直系亲属保持联系；

c)便于在事故发生时协助人员恢复；

d)便于通知家属其伤亡信息。

8.4.2.2人员背景审查、选择

组织应建立、实施和保持相应程序并形成成文信息，以便对代表其工作的所有人员进行背景审查，确保他们是能够完成任务的适当人选(例如分包方、外包合作伙伴和子公司)。在依法保护信息安全的基础上，审查应包括：

a)与法律法规及合同要求的一致性；

b)身份、最低年龄和履历审核；

c)教育和从业经历评审；

d)兵役、从警经历和保安服务从业记录审查；

e)无犯罪记录的评审；

f)无吸毒和药物滥用评审；

g)对指定活动进行体能和心理健康的适合性评价；

h)是否适合配备防卫装备以履行职责的评价。

人员应提供证明其行为不违背组织的道德准则、符合性声明或本文件条款的个人承诺书，有关情况发生变化时及时报告组织。

组织应制定适当的程序，以确保背景审查所涉及高度敏感信息在内外部披露过程中予以保密，并按照法定时效保存记录。

应根据岗位所要求的能力(包括知识、技能、能力和品质)选择合格人员。

8.4.2.3分包方选择、背景调查

组织应建立明确的程序，进行分包方选择、背景调查。组织对分包方的工作承担责任，且在适当情况下及在法律法规规定的范围内对分包方的行为承担责任。组织应：

a)与分包方签订适当的书面合同；

b)将工作安排书面通知客户，并在适当的情况下获得客户的批准；

c)保留所有分包方的登记记录；

d)将本文件规定的责任传达给分包方；

e)保留分包工作是否符合本文件的证据记录。

8.4.3制服、标识和可追溯性

在满足客户、公民安全要求同时，履行合同时组织应依法采用能识别其人员和交通工具的制服和标识。该标识宜在一定距离内可见，并区别于军队和警察所用的标识。组织应建立关于制服和标识使用的成文程序。程序应规定记录该标识与本条款要求不一致的情况。

需要时，组织应采用适当的方法识别输出，以确保产品和服务合格。组织应在保安服务提供的整个过程中按照监视和测量要求识别输出状态。当有可追溯要求时，组织应控制输出的唯一性标识，并应保留所需的成文信息以实现可追溯。

8.5职业健康与安全

组织应建立、实施和保持程序，包括合理的预防措施，提供安全、健康的工作环境，以保护高风险或危及生命作业的人员，并履行合同义务要求。程序应包括：

a)评估组织工作人员的职业健康与安全风险，以及对外可能造成的风险；

b)恶劣环境训练；

c)提供个人防护及其他适当的保安装备；

d)医疗和心理健康意识培训、治疗和支持；

e)识别和处置工作场所暴力、酗酒、吸毒、性骚扰等不当行为的指导方针。

8.6事件管理

8.6.1总则

组织应建立、实施和保持形成文件的程序，以识别可能影响组织活动、服务、利益相关方、合法权益及环境的非预期事件和干扰性事件，明确如何积极预防、缓解和应对上述事件，考虑以下措施：

a)保护生命，确保内外部利益相关方的安全；

b)尊重合法权益和人格；

c)防止干扰性事件的进一步升级；

d)尽量减少对运行的干扰；

e)通报有关部门；

f)保护(组织和其客户的)形象和声誉；

g)纠正和预防措施。

8.6.2事件监视、报告和调查

组织应建立、实施并保持事件监视、报告、调查、专业安排和补救措施的程序。

事件涉及防卫装备使用、人员伤亡、人身伤害、虐待指控、敏感信息或装备的遗失、药

物滥用等不合规情形的，应按照以下步骤进行报告和调查：

a)记录事件；

b)通报有关部门；

c)实施调查；

d)识别根本原因；

e)采取的纠正和预防措施；

f)对受影响各方提供的补偿和赔偿。

组织应确保所有人员了解职责，了解监视和报告的机制。

应保留不合格项和事件的记录并依据法定时效保存。

8.6.3内外部投诉和申诉程序

组织应建立形成文件的程序，有效处置内外部利益相关方(包括客户和其他受影响方)的投诉和申诉。该程序应传达给内外部利益相关方，以便于个人报告潜在的和发生的不合格或不合规的情况。组织应遵循保密原则，依法及时对投诉和申诉进行公平调查。程序应包括下列内容。

a)接收和处理投诉和申诉。

b)建立解决过程的分级步骤。

c)对投诉和申诉进行调查，包括：

1)与正式的外部调查机制合作；

2)防止恐吓证人或妨碍收集证据；

3)保护投诉或申诉的个人不受报复。

d)识别根本原因。

e)采取纠正及预防措施，包括与任何违规行为相适应的处罚。

f)与有关部门沟通。

组织应及时处理涉嫌违法犯罪、侵害他人合法权益或对个人安全构成威胁的投诉和申诉。

8.6.4举报制度

组织应建立保护举报人的制度。尊重举报人向内部及外部有关部门匿名举报的权利。组织不应对善意举报的个人采取不利行为。组织应将被举报的违法行为或侵害他人合法权益的情况告知客户。

8.7保安服务质量检查

组织应在适当阶段实施策划的安排，以验证保安服务质量满足要求，并保留适当的成文信息。

9、绩效评价

9.1监视、测量、分析和评价

9.1.1总则

组织应通过定期评价、演练测试、事后报告、经验教训及绩效评价对保安服务管理的计划、程序及能力进行评价。上述因素的重大变化应在程序中即时反映。

组织应确定：

——需要监视和测量什么；

——需要用什么方法进行监视、测量、分析和评价，以确保结果有效；

——何时实施监视和测量；

——何时对监视和测量的结果进行分析和评价。

组织应保留定期评价的成文信息，以作为结果的证据。

组织应对其保安服务运行绩效和保安服务管理体系的有效性进行评价。

组织应建立、实施并保持绩效指标的监视测量程序，以定期对其运行有实质性影响的绩效特征(包括伙伴关系、分包合同和供应链关系)实施监视测量。该程序应包括对绩效、运行控制及其与组织保安服务管理目标指标符合性实施监视的成文信息。

组织应评价并记录资产(人和物)保护系统、沟通机制和信息系统的有效性。

9.1.2合规性评价

组织应建立、实施并保持相应的程序，以定期对适用法律法规和合法权益的合规性进行评价。组织应保留定期评价的成文信息。

9.1.3演练和测试

组织应通过演练和其他方式来测试其保安服务管理体系计划、过程和程序的适宜性和有效性，包括利益相关方关系和与分包方中间的相互依赖程度。运行和事故应急方案的演练应解决风险评估和风险管理程序响应能力测试中发现的问题，以识别潜在的问题或薄弱环节。演练的策划和执行方式不应影响运行，且应将人员、资产和信息暴露的风险降至最低。

演练应定期(至少每年一次)进行，在此基础上，或在组织的指标、结构、外部环境发生重大变化后进行。

每次演练后应形成正式报告，该报告应评估组织保安服务管理体系的计划、过程及程序

(包括不合格项)的适宜性及有效性，并提出纠正和预防措施。

演练报告应作为管理评审输入。

9.1.4顾客满意

组织应监视客户对其需求和期望已得到满足的程度的感受。应确定获取、监视和评审该信息的方法。

注：监视客户感受的例子可包括客户调查、客户对保安服务的反馈、客户座谈、市场占有率分析、客户赞扬、合作伙伴和分包方报告。

9.2内部审核

9.2.1组织应建立、实施并保持保安服务管理内部审核程序，按照策划的时间间隔进行内部审核，以提供保安服务管理体系有关的下列信息。

a)是否符合：

——组织自身的保安服务管理体系要求；

——适用法律法规、合法权益及合同义务；

——本文件的要求。

b)是否得到有效的实施和保持。

c)是否符合预期。

d)是否有效达成组织保安服务管理体系的方针、目标和指标。

9.2.2组织应：

a)依据有关过程的重要性、对组织产生影响的变化和以往的审核结果，策划、制定、实施并保持审核方案，审核方案包括频次、方法、职责、策划要求和报告。

b)规定每次审核的审核准则、范围和频次、方法、职责、策划要求和报告；

c)选择审核员并实施审核，确保审核过程客观公正(如：审核员不应审核自己负责的工作)；

d)确保将审核结果报告给受审核区域的相关管理者；

e)保留成文信息，作为实施审核方案及审核结果的证据。

负责受审核区域的管理者应确保及时采取适宜的纠正措施，以消除发现的不合格及其原因。后续活动应包括对所采取措施的验证和验证结果的报告。

9.3管理评审

9.3.1总则

最高管理者应按计划的时间间隔对组织的保安服务管理体系进行评审，以确保其持续的

适用性、充分性和有效性。评审内容包括对保安服务管理体系(包括方针及目标)的改进时机和变更需要进行评价。应保留评审结果的成文信息。

管理评审应考虑下列内容。

a)以往管理评审所采取措施的情况。

b)与保安服务管理体系相关的内外部因素的变化。

c)下列有关保安服务管理体系绩效和有效性的信息，包括其趋势：

——不合格及纠正措施；

——监视和测量结果；

——审核结果。

d)对保安服务的影响。

e)风险管理准则和控制。

f)持续改进的机会。

管理评审的输入应包括有关持续改进机会和任何保安服务管理体系变更需求的决定。组织应保留成文信息，作为管理评审结果的证据。

9.3.2评审输入

管理评审输入应包括：

a)保安服务管理体系审核和评审的结果；

b)利益相关方反馈，包括顾客满意；

c)组织内部可用来提高保安服务管理体系绩效和有效性的技术、产品或程序；

d)预防和纠正措施的状态；

e)演练和测试的结果；

f)以往风险评估中未充分解决的风险；

g)事件报告；

h)有效性测量结果；

i)以往管理评审的跟进措施；

j)任何可能影响保安服务管理体系的变化；

k)方针和目标的充分性；

l)改进建议。

9.3.3评审输出

管理评审输出应包括与保安服务管理体系的方针、目标、指标及其他要素的可能变更有关的决策和措施，以促进持续改进，包括：

a)提高保安服务管理体系的有效性；

b)风险评估和风险管理计划的更新；

c)必要时修改影响风险的程序和控制措施，以应对可能影响到保安服务管理体系的内外部事件；

d)资源需求；

e)改进控制的有效性。

10、改进

10.1不合格和纠正措施

组织应建立、实施及保持处理不合格、采取纠正及预防措施的程序。该程序应规定识别和纠正不合格，以及采取措施减轻其后果。当出现不合格时，组织应采取以下措施。

a)对不合格做出应对，并在适用时：

——采取措施控制和纠正不合格；

——处置后果。

b)通过下列活动，评价是否需要采取措施以预防不合格并消除产生不合格的原因，避免其再次发生或者在其他场合发生：

——评审和分析不合格；

——确定不合格的原因；

——确定是否存在或可能发生类似的不合格。

c)调查不合格，确定其原因并采取措施防止其再发生。

d)实施所需的适宜的措施，旨在避免不合格发生。

e)评审所采取的纠正和预防措施的有效性。

f)记录实施纠正和预防措施的结果。

g)必要时，对保安服务管理体系进行更改。

纠正措施应与不合格产生的影响相适应。组织应确保对保安服务管理体系文件按修订建议进行更改，并保留成文信息作为下列事项的证明：

——不合格的性质以及随后所采取的措施；

——纠正措施的结果。

10.2持续改进

10.2.1总则

组织应通过保安服务管理方针、目标、审核结果，对监视事件的分析、纠正和预防措施以及管理评审，以持续改进保安服务管理体系的适用性、充分性和有效性。

10.2.2变更管理

组织应建立一个明确的文件化的保安服务变更管理方案，以确保对影响组织的任何内外部的有关保安服务管理体系的变更都进行评审。保安服务变更管理方案应识别需要包含的任何新的关键活动。

10.2.3改进时机

组织应监视、评估和利用改进保安服务管理体系绩效的机会，消除潜在问题产生的原因，包括：

a)持续监视运行状况，以发现潜在问题和改进机会；

b)确定并实施改进保安服务绩效所需的措施；

c)评审改进绩效措施的有效性。

最高管理者应确保利用改进机会及时采取措施。措施应与潜在问题的影响、组织的义务和资源的现状相适应。

如需对现有安排进行修改或引入可能影响运行和活动的质量管理的新安排，则组织应在实施前考虑相关的风险。

应清晰记录评审结果和采取的措施，并保留成文信息。后续活动应包括对所采取措施的验证和验证结果的报告。