ICS 13.310
CCS A 90

中华人民共和国国家标准

GB/T 42765—2023

保安服务管理体系　要求及使用指南

Management system for security operation—Requirements with guidance for use

（ISO 18788:2015，Management system for private security operations—Requirements with guidance for use，MOD）

2023-11-27 发布　　2024-06-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　次

前　言

本文件按照 GB/T 1.1—2020《标准化工作导则　第 1 部分：标准化文件的结构和起草规则》的规定起草。

本文件修改采用 ISO 18788:2015《民营安保业务管理体系 要求及实施指南》。

本文件与 ISO 18788:2015 相比，在结构上有较多调整。两个文件之间的结构编号变化对照一览表见附录 A。

本文件与 ISO 18788:2015 相比，存在较多技术差异，在所涉及的条款的外侧页边空白位置用垂直单线(|)进行了标示。这些技术差异及其原因一览表见附录 B。

本文件做了下列编辑性改动：

——标准名称调整为《保安服务管理体系　要求及使用指南》；

——在提及国际、区域法律时，更改为法律法规。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国公共安全基础标准化技术委员会(SAC/TC 351)提出并归口。

本文件起草单位：公安部治安管理局、江苏省质量和标准化研究院、中国标准化研究院、中国保安协会、山东华威保安集团股份有限公司、华信中安(北京)保安服务有限公司、北京华远润泽国际认证有限公司、方圆标志认证集团江苏有限公司、苏州市东吴物业管理有限公司、江苏省保安协会、北京市科学技术研究院、同方威视技术股份有限公司、南京现代服务业联合会、中国物资储运协会、江苏华远企业管理咨询有限公司。

本文件主要起草人：顾岩、杨华书、吴笑颜、管旭琳、刘珏、秦挺鑫、王皖、杨中河、吴杰、柳庆、胡永明、曹惠华、刘立生、郭立志、许磊、王峰、朱伟、毛朔南、李军、姜茂伟、保蕊、朱敬云、杜舒雅、刘守道、张承祥、王建峰、张华、孔肖菡、刘谨谨、唐庆华、王亚飞、许歆宜。

保安服务管理体系　要求及使用指南

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　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 19000—2016　质量管理体系　基础和术语（ISO 9000:2015，IDT）

GB/T 23694—2013　风险管理　术语（ISO Guide 73:2009，IDT）

3　术语和定义

GB/T 23694—2013、GB/T 19000—2016 界定的以及下列术语和定义适用于本文件。

3.1

资产　asset

组织（3.33）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。

3.2

审核　audit

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（3.42）。

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（3.33）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。

[来源：GB/T 19000—2016，3.13.1]

3.3

审核员　auditor

实施审核（3.2）的人员。

[来源：GB/T 19011—2021，3.15]

3.4

客户　client

雇用、曾经雇用或计划雇用一个组织(3.33)来代表其进行保安服务(3.61)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。

3.5

能力　competence

应用知识和技能实现预期结果的本领。

3.6

沟通和咨询　communication and consultation

组织(3.33)管理风险(3.49)时，提供信息、共享信息、获取信息以及与利益相关方(3.23)及其他各方，展开对话的持续、往复的过程(3.42)。

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(3.26)、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。

[来源：GB/T 23694—2013，4.2.1，有修改]

3.7

社会群体　community

拥有共同利益的相关组织(3.33)、个人和群体。

3.8

合格　conformity

满足要求(3.44)。

3.9

持续改进　continual improvement

提高绩效(3.35)的循环活动。

3.10

后果　consequence

某事件(3.19)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。

[来源：GB/T 23694—2013，4.6.1.3，有修改]

3.11

纠正　correction

为消除已发现的不合格(3.31)所采取的措施。

3.12

纠正措施　corrective action

为消除不合格(3.31)的原因并防止再发生所采取的措施。

3.13

危害性分析　criticality analysis

基于组织的任务或职责的重要性，及风险(3.49)人群、非预期事件(3.73)或干扰性事件(3.15)对组织实现预期的影响性，系统识别和评估组织(3.33)资产(3.1)的过程。

3.14

关键控制点　critical control point；CCP

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(3.42)。

3.15

干扰性事件　disruptive event

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。

3.16

成文信息　documented information

组织(3.33)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(3.28)，包括相关过程(3.42)；

——为组织运行产生的信息(一组文件)；

——结果实现的证据[记录(3.43)]。

3.17

有效性　effectiveness

完成策划的活动并得到策划结果的程度。

3.18

演练　exercises

用以评估保安服务管理(3.62)方案，排练团队成员和人员角色，测试组织(3.33)系统(如技术、报告规程、管理等)以证明保安业务管理能力(3.5)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(3.35)的目标。

3.19

事件　event

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(3.20)。

[来源：GB/T 23694—2013，4.5.1.3，有修改]

3.20

事故　incident

造成伤亡、资产(3.1)损害、对内外部利益相关方(3.23)的合法权益和基本自由产生不利影响等后果(3.10)的事件(3.19)。

3.21

固有危险物　inherently dangerous property

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。

3.22

完整性 integrity

保障资产(3.1)准确性和完整性的特性。

3.23

利益相关方 interested party;stakeholder

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(3.33)。

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(3.61)保持一致。

3.24

关键绩效指标 key performance indicator;KPI

组织(3.33)为完成其战略和服务目标(3.32)用来测量或比较绩效(3.35)的可量化措施。

3.25

防卫装备 defense equipment

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。

3.26

可能性 likelihood

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。

注 2：“可能性”(likelihood)这一英语词汇在一些语言中没有直接与之对应的词汇，因此经常用“概率”(probability)这个词代替。不过，在英语中，“概率”常常被狭义地理解为一个数学词汇。因此，在风险管理术语中，“可能性”应该有着与许多语言中使用的“概率”一词相同的解释，而不局限于英语中“概率”一次的意义。

[来源：GB/T 23694—2013，4.6.1.1]

3.27

管理计划 management plan

具有明确规定和记录的行动计划，通常包含执行事件(3.19)管理过程(3.42)所需的关键人员、资源(3.47)、服务和行动。

3.28

管理体系 management system

组织(3.33)建立方针(3.37)、目标(3.32)和实现目标所需过程(3.42)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(3.36)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(3.70)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(3.47)；

——针对该目标和指标用于对绩效(3.35)进行评定的测量(3.29)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(3.48)过程。

3.29

测量 measurement

确定数值的过程(3.42)。

3.30

监视 monitoring

确定体系、过程(3.42)或活动的状态。

注：确定状态可能需要检查、监督或密切观察。

3.31

不合格 nonconformity

未满足要求(3.44)。

3.32

目标 objective

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(3.42)]。

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(3.64)，或使用其他有类似含义的词[如宗旨、指标(3.70)]。

注 4：在保安服务管理(3.62)环境中，组织(3.33)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。

3.33

组织 organization

为实现目标(3.32)，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。

3.34

外包 outsource

安排外部组织(3.33)承担组织的部分职能或过程(3.42)。

注：虽然组织的管理体系(3.28)包括外包功能或过程(3.42)，但不包括外部组织。

3.35

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(3.42)、产品(包括服务)、系统或组织(3.33)的管理。

3.36

策划 planning

管理的一部分，致力于制定保安服务目标(3.63)并规定必要的运行过程(3.42)和相关资源以实现保安服务目标。

3.37

方针 policy

由最高管理者(3.72)正式发布的组织(3.33)的宗旨和方向。

3.38

预防 prevention

能够使组织(3.33)避免、杜绝或限制非预期事件(3.73)或潜在干扰性事件(3.15)的措施。

3.39

预防措施 preventive action

为消除潜在不合格(3.31)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。

[来源：GB/T 19000—2016，3.12.1]

3.40

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(3.66)单位的统称。

3.41

程序 procedure

为进行某项活动或过程(3.42)所规定的途径。

注：程序可以形成文件，也可以不形成文件。

[来源：GB/T 19000—2016，3.4.5]

3.42

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。

3.43

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(3.39)和纠正措施(3.12)提供证据。

注 2：通常，记录不需要控制版本。

[来源：GB/T 19000—2016，3.8.10]

3.44

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(3.33)或利益相关方(3.23)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(3.16)中阐明。

3.45

剩余风险 residual risk

风险应对(3.60)之后仍然存在的风险(3.49)。

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"。

[来源：GB/T 23694—2013，4.8.1.6]

3.46

恢复力 resilience

组织(3.33)对复杂变化环境的适应能力。

[来源：GB/T 23694—2013，4.8.1.7]

3.47

资源 resources

有潜在价值并可以被利用的资产(3.1)、设施、设备、材料、产品或废弃物。

3.48

评审 review

确定管理体系(3.28)及其组成要素实现规定目标(3.32)的适宜性、充分性或有效性(3.17)的活动。

3.49

风险 risk

不确定性对目标(3.32)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(3.19)及其后果(3.10)或可能性(3.26)等信息缺乏理解或了解的状态。

注 3：通常以潜在“事件”(GB/T 23694—2013，4.5.1.3)和“后果”(GB/T 23694—2013，4.6.1.3)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”(GB/T 23694—2013，4.6.1.1)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(3.42)]。

注 6：风险可分为故意、无意和自然性的来源。

3.50

风险接受　risk acceptance

接受某一特定风险(3.49)的决定。

注 1：风险接受可以不经风险应对(3.60)，还可以在风险应对过程(3.42)中发生。

注 2：接受的风险要受到监视(3.30)和评审(3.48)。

[来源：GB/T 23694—2013，4.7.1.6]

3.51

风险分析　risk analysis

理解风险(3.49)性质、确定风险等级的过程(3.42)。

注 1：风险分析是风险评价(3.55)和风险应对(3.60)决策的基础。

注 2：风险分析包括风险估计。

[来源：GB/T 23694—2013，4.6.1]

3.52

风险偏好　risk appetite

组织(3.33)寻求、保留或接受风险(3.49)的准备。

[来源：GB/T 23694—2013，4.7.1.2，有修改]

3.53

风险评估　risk assessment

包括风险识别(3.56)、风险分析(3.51)和风险评价(3.55)的全过程(3.42)。

[来源：GB/T 23694—2013，4.4.1]

3.54

风险准则　risk criteria

评价风险(3.49)重要性的依据。

注 1：风险准则的确定需要基于组织的目标(3.32)、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(3.44)。

[来源：GB/T 23694—2013，4.3.1.3]

3.55

风险评价　risk evaluation

对比风险分析(3.51)结果和风险准则(3.54)，以确定风险(3.49)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(3.60)的决策。

[来源：GB/T 23694—2013，4.7.1]

3.56

风险识别　risk identification

发现、确认和描述风险(3.49)的过程(3.42)。

注 1：风险识别包括对风险源、事件(3.19)及其原因和潜在后果(3.10)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(3.23)的需求。

[来源：GB/T 23694—2013，4.5.1]

3.57

风险管理　risk management

在风险(3.49)方面，指导和控制组织(3.33)的协调活动。

[来源：GB/T 23694—2013，3.1]

3.58

风险登记　risk register

已识别风险(3.49)的信息记录。

注：风险评估(3.53)过程(3.42)中对已识别、分析和评价过的所有风险的汇编，包含可能性(3.26)、后果(3.10)、应对和风险所有者等信息。

3.59

风险容忍　risk tolerance

组织(3.33)或利益相关方(3.23)为实现目标在风险应对(3.60)之后承担风险(3.49)意愿。

注：风险容忍会受到客户(3.4)、利益相关方、法律法规要求(3.44)的影响。

[来源：GB/T 23694—2013，4.7.1.3，有修改]

3.60

风险应对　risk treatment

处理风险(3.49)的过程(3.42)

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(3.26)；

——改变后果(3.10)；

——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。

[来源：GB/T 23694—2013，4.8.1]

3.61

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。

[来源：GA/T 594—2006，3.2，有修改]

3.62

保安服务管理　security operation management

指导和管理组织(3.33)关于保安服务(3.61)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(3.37)、策划(3.36)和目标(3.32)，指导运行过程(3.42)和持续改进(3.9)。

3.63

保安服务目标　security operation objective

保安服务管理(3.62)的目的。

注 1：保安服务目标通常根据组织(3.33)的保安服务方针(3.64)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。

3.64

保安服务方针　security operation policy

组织(3.33)关于保安服务(3.61)的总体意图和方向，由最高管理者(3.72)正式发布。

注：一般保安业务方针与组织的总体方针(3.37)一致，并为保安服务目标(3.63)的制定提供框架。

3.65

保安服务方案　security operation programme

最高管理者(3.72)支持的持续进行的管理和治理过程(3.42)，确保采取必要的步骤来协调各项工作，实现保安服务管理(3.62)体系的目标(3.32)。

3.66

保安服务人员　security operation personnel

为组织(3.33)直接或间接从事保安服务(3.61)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。

3.67

自卫　self-defence

保护自身或财产免受他人侵害。

3.68

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(3.33)。

3.69

供应链　supply chain

组织(3.33)、人员、过程(3.42)、物流、信息、技术和资源(3.47)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。

3.70

指标　target

为实现目标(3.32)而制定的适用于组织(3.33)的详细(或部分)绩效(3.35)要求(3.44)。

3.71

威胁分析　threat analysis

对可能会损害人身、资产(3.1)、体系或组织(3.33)、环境或社会群体(3.7)的非预期事件(3.73)的潜在原因进行识别、限制和量化的过程(3.42)。

3.72

最高管理者　top management

指导和控制组织(3.33)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(3.47)的权力。

注 2：如果管理体系(3.28)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。

3.73

非预期事件　undesirable event

可能造成人身伤亡、资产(3.1)损失或对内外部利益相关方(3.23)的合法权益造成负面影响的事件。

3.74

脆弱性分析　vulnerability analysis

对可能造成后果(3.10)的风险(3.49)来源产生敏感性的识别和量化的过程(3.42)。

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（见 6.1），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附录 C 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：

——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。

7.4 沟通

7.4.1 总则

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。

附 录 A
（资料性）
本文件与 ISO 18788:2015 相比的结构变化情况

表 A.1 给出了本文件与 ISO 18788:2015 结构编号对照一览表。

表 A.1 本文件与 ISO 18788:2015 结构编号对照情况

本文件结构编号	ISO 18788:2015 结构编号
—	引言
—	3.20
3.20，3.21，3.22…，3.76	3.21，3.22，3.23…，3.77
—	3.62
3.61，3.62…，3.73	3.63，3.64…，3.75
—	3.76
3.74	3.77
6.1.3	6.1.1 自第二段至结束
6.1.4	6.1.3
8.1.2	—
8.1.3	—
8.1.4	8.1.2
8.1.5	8.1.3
8.1.6	8.1.4
8.3.2	8.3.3、8.3.4、8.3.5 合并调整
8.3.3	8.3.2
—	8.3.6
8.3.4	8.3.7
—	8.4
—	8.5
8.4	8.6
8.4.1	8.6.1
8.4.2	8.6.2
8.4.2.1，8.4.2.2，8.4.2.3	8.6.2.1，8.6.2.2，8.6.2.3
—	8.6.3
8.4.3	8.6.4
8.5	8.7
8.6	8.8
8.6.1，8.6.2，8.6.3	8.8.1，8.8.2，8.8.3

表 A.1　本文件与 ISO 18788:2015 结构编号对照情况（续）

本文件结构编号	ISO 18788:2015 结构编号
8.7	—
9.1.4	—
附录 A	—
附录 B	—
附录 C	附录 A
C.6.2.1	A.7.2 第一段和第二段
C.6.2.2	A.7.2 第三段
C.6.2.3	A.7.2 第四段至结束
C.6.2.4	—
C.7.1.1	A.8.1.1
C.7.1.2	—
C.7.1.3	—
C.7.1.4.1	A.8.1.2.1
C.7.1.4.2	—
C.7.1.4.3	—
C.7.1.4.4	A.8.1.2.2
C.7.1.5，C.7.1.6	A.8.1.3、A.8.1.4
C.7.2	A.8.2
C.7.3.1，C.7.3.2、C.7.3.3、C.7.3.4	A.8.3.1，A.8.3.2，A.8.3.3，A.8.3.4
—	A.8.3.5
C.7.3.5	A.8.3.6
C.7.3.6	A.8.3.7
C.7.4.4.2	—
C.7.6.5	—
附录 D～附录 G	附录 B～附录 E

附 录 B
（资料性）
本文件与 ISO 18788:2015 的技术差异及其原因

表 B.1 给出了本文件与 ISO 18788:2005 的技术差异及其原因的一览表。

表 B.1 本文件与 ISO 18788:2005 的技术差异及其原因

本文件结构编号	技术差异	原因
1	删除了 ISO 18788 中关于采用国际标准的适用范围	该内容从国际角度叙述，我国不适用于这种叙述
3	增加了 GB/T 19000—2016 的引用	与相关标准协调一致
	删除了 ISO 18788 中 3.20“人权保护分析”(HRRA)	适应我国国情
3.25	更改“非致命力”为“防卫装备”	结合我国相关法律及行业现状
3.40	更改“私营安保供方”为“保安从业单位”	适应我国行业现状
3.61	更改“安保业务”为“保安服务”，更改定义内容	结合我国相关法律及行业现状
3	删除了 ISO 18788 中 3.62“安保”	3.61 定义中已包含相关含义
	删除了 ISO 18788 中 3.76“武力使用层级”	结合我国相关法律及行业现状
5.1.2	删除了 ISO 18788 中关于遵守联合国人权文件的内容，包括： ——删除了《蒙特勒文件(09/2008)》(8.3.1、8.8.2 中做相同处理)； ——删除了《私营安保服务提供商国际行为守则(ICoC)(11/2010)》； ——删除了《工商业与人员合法权益：实施联合国“保护、尊重和补救”框架指导原则 2011》	符合我国相关法律法规要求，及适应我国行业现状
6.1.3	将 ISO 18788 的 6.1.1 总则中关于风险评估的内容更改为 6.1.3 风险评估	单独设一节使结构更合理
7.1.2.4	将 ISO 18788 中“尊重人权”更改为“尊重合法权益”，在全文做相同处理	适应我国国情
7.2.2	删除了 ISO 18788 中 d)遵守适用的地方和国际法律，包括刑法、人权法和国际法	适应我国国情
7.3	增加了“——相关的保安服务目标”	保持内容的完整性
8.1.1	删除了 ISO 18788 的 c)中遵守国际人权和惯有的法律部分，修改为遵守相关的法律法规	符合我国相关法律法规
8.1.2	增加了 8.1.2 保安服务的要求	结合我国行业情况，增加相关内容
8.1.3	增加了 8.1.3 保安服务的设计和开发	结合我国行业情况，增加相关内容

表 B.1　本文件与 ISO 18788:2005 的技术差异及其原因（续）

本文件结构编号	技术差异	原因
8.1.4	增加了“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”； 增加了组织应确保在受控条件下进行保安服务的提供及相应的受控条件	适应国内保安服务的需要，更具有可操作性
8.3	更改“武力”改为“防卫装备”	适应我国国情
8.3.1	增加了我国有关保安服务范围的相关说明	适应我国国情
8.3.2	将 ISO 18788 中 8.3.3 武力使用层级、8.3.4 非致命力、8.3.5 致命力合并更改为 8.3.2 防卫装备使用原则	适应我国国情
8.3.3	将 ISO 18788 中 8.3.2 武器授权更改为防卫装备授权	适应我国国情
8	删除了 ISO 18788 中 8.3.6 使用武力执法的条款	适应我国国情
	删除了 ISO 18788 中 8.4 调查和逮捕	适应我国国情
	删除了 ISO 18788 中 8.5 支援执法的业务	适应我国国情
	删除了 ISO 18788 中 8.6.3 武器、危险物品及军需品的采购与管理	适应我国国情，我国枪支弹药管理严格，有相关法律法规。国际标准中涉及的相关内容不宜推广
8.4	标题更改为“关键资源”	内容中未提到关于岗位、职责和授权的具体要求
8.4.2.2	删除了 ISO 18788 中“根据法律法规和根据客户要求，设定最小年龄。然而在任何情况下，任何从事需要使用枪支或其他武器工作的人员不得小于 18 周岁。”	国内已有相关法律法规对内容进行规定，本文件无需赘述
8.4.3	删除了 ISO 18788 中“以及建立确定和成文当该标识与本条款要求不一致情况的程序”； 增加了“可追溯性”及相关要求	适应我国国情，保持内容的完整性
8.7	增加了 8.7 保安服务质量检查	满足国内保安服务的需求，更具有可操作性
9.1.4	增加了 9.1.4“客户满意”	保持内容的完整性，更具有可操作性

附 录 C
（资料性）
本文件使用指南

C.1 总则

本附录及附录 D、附录 E、附录 F、附录 G 的内容用于帮助组织理解本文件的要求。组织在执行本要求时，还需根据自身风险评价及客户合法权益考虑并执行本文件适用于其范围、法律法规与合同义务以及运营环境的相关条款。

本文件为组织及其客户提供用于审核的依据，以证明其有能力提供保安服务，有能力预防不当、非法及过度行为的发生。

对于从事及承包保安服务的组织来说，其所面临的挑战不仅仅是事件响应及报告。组织宜制定一个全面及系统的过程，以对其业务的相关风险进行预先管理。这就需要制定一个持续、动态及互动的管理过程，以促进建设尊重合法权益、法律法规和基本自由的文化氛围，同时为客户提供一定水平的服务，助其完成指标。

从事或承包保安服务的组织及其客户有义务尊重内外部利益相关方的生命及合法权益。通过使用本文件，组织可以更好地理解其所面临的风险，并预先制订战略对策，以便：

a) 对其所保护的合约客户遭受的生命及财产风险进行管理；
b) 证明其履行尊重合法权益、法律法规的承诺及义务；
c) 降低风险及支持业务和运行；
d) 通过制订保护其自身与其客户及利益相关方利益的战略及行动计划来对非预期事件和干扰性事件进行有效管理。

针对潜在非预期事件和干扰性事件而制订的适用及预先规划和准备可以降低事件发生的可能性及其影响。全面管理过程有助于避免或降低关键服务及业务中断或中止的可能性。

本附录为组织提供了指导或建议，以助其识别和研发实施以下行动的最佳实践方法：

a) 降低其运行和供应链（包括分包方）的风险；
b) 在尊重合法权益、遵守法律法规要求的同时，确定管理方针和目标；
c) 鉴定和评定对其短期和长期成功至关重要的风险；
d) 降低各种危害和威胁的可能性和影响；
e) 理解、提供并进行关于遵守法律法规和尊重合法权益的培训；
f) 理解其在保护资产和进一步完成任务方面需要发挥的作用及承担的义务；
g) 管理事故响应措施及资源；
h) 开发、测试及维护事故预防和响应计划以及相关的运作程序；
i) 开展培训和演练，以支持与评定、预防、保护、准备、缓解、响应、恢复及运作程序；
j) 制定和执行培训方案，为正确使用防卫装备提供支持；
k) 制定内外部通信程序，包括媒体或公众信息申请的响应程序；
l) 建立衡量及证明成功的指标；
m) 记录支持主要运作功能时所需的关键资源、基础设施、指标及职责；
n) 制定确保信息具有可靠性、时效性，并随风险及工作环境变化而变化的程序。

管理体系的成功取决于组织中各级部门及职能特别是最高管理者的投入。为实现这一目标，决策者宜为必要资源制定预算并确保其安全。有必要建立适当的行政结构以有效地进行预防、缓解和管理。这一结构将确保有关各方了解决策者为何人、决定如何执行，以及组织名下所有工作人员的职责与责

任，推动组织内部保安服务文化建设。

对于从事或承包保安服务的组织来说，如果其行动直接反映其客户（特别是当客户是政府实体时）意图，则其客户有权确保组织遵守本文件的原则。组织的不正当、非法和过度行为的后果可能会令客户难堪、导致信誉风险和承担法律责任。在签订服务合同时，客户有权要求组织执行保安服务管理体系。

C.2 管理的系统方法

管理的系统方法是一个动态的多层面过程，每个要素作为一组结构化的功能单元进行交互。其框架基于以下前提：与孤立地观察相比，将一个体系的组成部分置于互相联系和与其他体系联系的背景中进行观察时，对其理解将更加充分。要完全理解并实施管理体系要素，唯一方法是根据该功能单元与整体的关系来对其进行理解。这就产生了一个迭代过程，这个过程中环境和政策的建立、风险评价、实施、操作、评定和审查不是一系列连续的步骤，而是一个互动功能网络。

管理的系统方法的特征如下：

a) 了解体系运行的环境与状况；

b) 确定体系的核心要素以及系统边界；

c) 了解体系中每个功能单元的角色或功能；

d) 了解体系要素之间的动态交互作用。

管理的系统方法确保能够制定整体战略和方针。这些战略和方针将在组织运行的复杂和不断变化的环境中实施，能够为其制定提供良好的分析基础。战略和方针实施之前和实施期间，建立风险和有效性评定框架可为整个过程的战略和决策提供反馈环路。

C.3 组织环境

.3.1 理解组织及其环境

C.3.1.1 总则

为了管理风险、促进合法依规的文化氛围，组织需要识别和理解可能影响其保安服务和利益相关方的内外部因素。

组织在策划保安服务管理体系时，宜识别和理解其运行所涉及的内外部影响因素和其运行环境。通过建立环境，组织可以确定其保安服务管理体系的范围，并为保安服务管理设计一个适用框架。这有助于确保组织满足内外部利益相关方的目标、需求和期望。这种环境将为组织、客户和受影响群体提供风险管理的准则，从而为风险评价和处理过程，确定风险准则和参数提供基础。

在建立内外部环境的过程中，组织宜确定其重要的有形资产和无形资产，同时确定各种类型的资产对其生存和成功的相对重要性。

C.3.1.2 内部环境

在确定组织的内部环境时，需考虑以下几点：

a) 影响组织的保安服务和运行环境的内部因素；

b) 作为风险制定和风险承担者的内部利益相关方；

c) 受风险影响的内部利益相关方；

d) 影响风险承担的因素。

C.3.1.3 外部环境

当建立组织的外部环境时，需考虑以下几点：

a) 与行业和运行环境相关的风险因素；

b) 影响组织的保安服务和运行环境的外部因素；
c) 作为风险制定者和风险承担者的外部利益相关方；
d) 受保安服务相关风险影响的外部利益相关方；
e) 影响外部利益相关方承担风险的因素。

C.3.1.4 供应链和分包方信息的收集和分析

组织在管理供应链中的风险时，要了解这些组织的文化和环境以及供应链状况，供应链包括合同分包方和分子公司队伍。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。

供应链和采用分包方是保安服务不可分割的一部分。虽然供应链中存在明显的相互依存关系，但供应链的每个单独节点在特定方面却是独一无二的；这种独特性可能需要定制相应的方法来管理涉及的风险。因此，为了管理供应链中的风险，组织需要识别：

a) 在其供应链或供应网上下游的每一层或每一级的组织和个人的作用；
b) 了解对指标成功至关重要的相互依存因素和配套基础设施；
c) 每个节点如何直接或间接地发挥作用提升供应链中其他部分的表现；
d) 确定每个节点促进或阻碍组织风险预测的可能性；
e) 评价每个节点如何在管理体系实施过程中施加影响、成功将风险最小化。

当进行节点分析时，组织宜认识到在各个节点做出的决定可能影响整个供应链。因此，为成功实施保安服务管理体系，需要理解和控制整个供应链的所有风险因素。

C.3.1.5 确定风险准则

组织宜了解评价风险重要性的准则并对其进行定义。风险准则宜反映组织的价值观、目标和资源，以及其保安服务的状况。风险准则将确定评估风险因素和风险应对需求的依据。

C.3.2 理解相关方的需求与期望

组织宜确定与其运行和本文件的要求相关的利益相关方并登记在册，同时记录与利益相关方的约定。组织宜考虑利益相关方的需求、理念、价值观、期望、利益和风险承受能力。

利益相关方包括但不限于：

a) 委托人和客户；
b) 最终用户；
c) 供应链和外包合作伙伴；
d) 负责保安服务许可/授权和监管的法定主管部门；
e) 适用范围内的社会群体；
f) 有关行业协会和国际组织；
g) 组织内的工作人员；
h) 媒体。

C.3.3 确定保安服务管理体系的范围

组织确定保安服务管理体系的范围。保安服务管理体系可在整个组织、特定业务单位、分散的地理位置或明确定义的供应链流程中选择进行实施。这些范围界限反映了保安服务管理体系的最高管理目标以及组织及其活动的规模、性质和复杂性。一旦高层管理者确定了保安服务管理体系的范围，范围内的所有资源、活动、产品和服务都将成为管理体系中重要的要素。

组织宜采用风险评价方法来证明排除在保安服务管理体系范围之外的任何情况。除外情况可包括组织无法控制的某些服务业务或操作；但是，除外情况并不否定该组织遵守法律法规、尊重合法权益的

义务。体系范围宜确保组织及其客户业务的完整性。保安服务管理体系的可靠性取决于体系范围内组织界限的选择。

组织在各种风险因素不同的环境中开展保安服务。根据保安服务和风险评价的情况,“适用性声明”宜记录本附录中适用于在限定范围内建立和实施保安服务管理体系的相关条款。

外包和分包活动仍然是组织的责任,宜包含在保安服务管理体系范围内。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然在组织的风险责任和管理控制之下,那么最高管理者宜将其包含在保安服务管理体系的范围内。组织宜制定适当的协议并采取适当措施确保与其分包方和外包合作伙伴签订有效的保安服务管理协议。

保安服务管理体系的详细程度和复杂程度、所需文件的范围以及向其提供的资源宜对该体系的范围声明有指导作用。当组织评估特定业务单位是否符合此文件时,可使用组织其他部分制定的适用方针、计划和规定来满足本文件的要求。

C.3.4 保安服务管理体系

本文件规定的保安服务管理体系的实施目标是:

a) 提高保安服务水平;

b) 保障内外部利益相关方的安全;

c) 形成尊重合法权利和遵守法律法规的文化氛围。

本文件设立的前提是,组织将监视、评审和评价其保安服务管理体系,以确定不断改进和采取纠正和预防措施的时机。组织根据不断变化的风险环境、经济状况和其他情况来确定持续改进的过程的速度、范围和时限。本文件要求组织:

a) 确立适当的保安服务管理方针;

b) 评估和管理涉及组织保安服务的各种风险;

c) 明确适用的法律法规要求及组织同意遵守的其他要求;

d) 确定优先顺序,设置适当的保安服务管理目标和指标;

e) 建立实现方针、目标和指标的体系和方案;

f) 促进策划、控制、监视、预防和纠正措施以及内部审核和管理评审的进行,确保方针得到遵守、保安服务管理体系保持得当;

g) 能够适应不断变化的环境。

C.4 领导作用

C.4.1 领导作用和承诺

C.4.1.1 总则

组织的最高管理者宜承诺并下决心在组织中实施保安服务管理体系。没有最高管理者的承诺,任何管理体系都无法成功。最高管理者宜向其内外部利益相关方郑重承诺,在提供保安服务时遵守法律法规和尊重合法权益。为了保安服务管理体系工作的开展与持续,最高管理者宜向代表组织工作的所有人员传达以下问题的重要性:

a) 无论组织做什么,始终保持组织与个人提供保安服务的能力;

b) 遵守法律法规和尊重合法权益是所有保安服务的组成部分;

c) 将保安服务管理要求纳入整个组织业务;

d) 将问题视为改进的机会。

最高管理者宜证实其开展与实施保安服务管理体系的承诺,并通过以下方式不断提高其有效性:

a) 在整个组织中传达符合本文件要求的重要性;

b) 制定和传达方针和风险准则；
c) 确保在各级各部门确立保安服务目标；
d) 确保在组织内分配和传达相关管理体系各岗位的责任和权限；
e) 为管理体系分配适当的资源；
f) 确保代表该组织工作的人员的能力，并对其进行培训；
g) 承诺致力于管理体系和风险最小化工作；
h) 增强全组织对保安业务管理体系要求的认识和风险意识；
i) 以身作则；
j) 参加评审并推动持续改进过程。

组织的最高管理者提供必要的资源，并负责保安服务管理体系建立、实施、保持和改进，这一点至关重要。因为这将确保组织内各级管理层和工作人员知晓保安服务管理体系是关键性的最高管理优先事项。最高管理者宜针对保安服务管理体系采用“自上而下”的方法，使得组织各级管理层将对体系的维护责任作为全面管理优先事项的一部分，这一点同样重要。

C.4.1.2 符合性声明

“符合性声明”确立并传达最高管理者的承诺，即通过实施本文件的要求，开展与尊重合法权益相一致的保安服务。

C.4.2 方针

保安服务方针是实施和改进组织保安服务管理体系的驱动力。因此，该方针宜反映最高管理者的以下承诺：

a) 把尊重人的生命和尊严作为重中之重；
b) 避免、预防和减少非预期事件和干扰性事件的发生及其影响；
c) 符合适用法律法规的要求和其他要求；
d) 尊重合法权益；
e) 持续改进。

保安服务方针为组织确立其目标和指标提供框架。保安服务方针宜清楚明确，能够被内外部利益相关方理解，并宜定期进行审查和修订以反映不断变化的环境和情况。其应用领域(即范围)应可明确识别，反映其职能、产品和服务活动风险的独特性质、规模和影响。

保安服务方针宜传达给组织的所有工作人员或代表组织工作的所有人员，包括其客户、供应商合作伙伴、分包方和社会群体的相关成员。传达分包方和外部其他各方时，可采用方针声明的替代形式，例如规则、规章和程序。根据组织所归属的更广泛的社会群体的保安服务政策，由最高管理者定义和记录该组织的保安服务方针，并得到社会群体的认可。

C.4.3 组织的岗位、职责和权限

管理风险不仅仅是高层管理人员的职责。为了保证保安服务管理体系的有效性，需要将其落实到代表组织工作的每个人身上。这个体系是一种自上而下、自下而上的方法。保护合法权益和管理风险需成为组织文化不可分割的一部分。所有风险制造者和风险承担者都宜是风险管理者，因此，宜明确在保安服务管理体系范围内代表该组织工作的人员的岗位、职责和权限，并进行传达。

管理体系由组织内的人员进行实施。因此，宜任命一名或多名合格人员，并授权其实施、监视或实行以及保持保安服务管理体系。最高管理者宜对整个保安服务管理体系进行定期审核和评审。为确保保安服务管理体系被广泛接受，可委派一个包括所有主要组织职能部门和后勤工作组的高层级领导在内的保安服务管理团队。

C.5 策划

C.5.1 应对风险和机遇的措施

C.5.1.1 总则

从事或承包保安服务的组织其运行环境本来就不确定且有风险。这些组织需要管理客户、组织本身及受影响的利益相关方和社会群体的风险。在保证客户、组织代表人员及社会群体的生命及财产安全并尊重合法权益的情况下，组织需要实现其策略、运行及业务目标。尊重合法权益可以创造商业价值，因此，在尊重合法权益和遵守相关法律法规的规定下，要求谨慎处理依法合规相关问题来完成运行指标本质上就是一个业务目标。在满足组织和客户的战略和运行目标的情况下，面临的挑战是评价、评定及处置风险，以便有效地控制风险和其不确定性。通过风险评估可清晰了解风险环境，以便使组织识别风险并按风险处置优先顺序做出明智的决策。

通过风险评估过程可清晰了解内外部利益相关方的风险，而这些风险可能影响组织运行和业务目标的实现。风险评估的目标是为组织创造一个系统过程，来识别、分析和评定风险，从而确定对组织和其利益相关方有重要影响的风险。风险评估为评价现有控制的适当性和有效性及决策最适当的风险管理和处置方法提供了依据，并能识别组织的保安服务管理体系宜优先解决的风险。风险评估为在管理系统内部设定目标和程序及测量保安服务管理体系的效力提供了基础。

C.5.1.2 法律法规和其他要求

组织宜识别和了解影响其实现目标的法律法规和合同要求。识别和了解这些要求有助于确保组织合法依规、息讼止争、减少责任、改善组织的形象及增强组织的能力，从而为客户提供可靠的保护服务。

组织宜建立和实施措施并将措施纳入程序中以识别、遵守和评价适用的法律法规和自发要求，包括但不限于：

a) 适用的法律法规、与活动和运行以及本文件适用范围内分包方有关的其他要求；
b) 适用的劳动和环境法律法规；
c) 有关反贿赂、反腐败或反对类似犯罪行为的措施；
d) 保安服务运行采用的有关防卫装备使用是否符合法律法规要求。

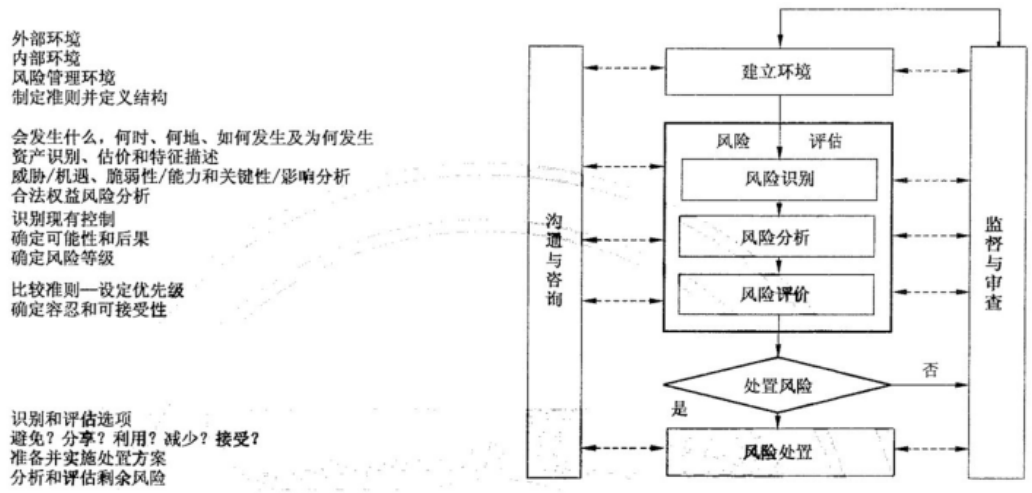
组织可能同意的其他适用要求包括：

a) 商业及其他合同义务；
b) 与公共机构、社会群体的协议；
c) 与客户的协议；
d) 非法规性指南；
e) 自愿原则或行为守则；
f) 产品或服务管理承诺(比如担保)；
g) 有关行业协会的要求；
h) 组织或其上级组织的公开承诺；
i) 非约束性协议；
j) 医疗保健要求；
k) 财政义务；
l) 社会责任和环保承诺；
m) 身份信息、机密性和隐私要求。

C.5.1.3 风险评估

C.5.1.3.1 ISO 31000 中风险评估过程

在执行 ISO 31000 时，组织宜应用的原则和准则如图 C.1 所示。



注：来源：ASIS International。

图 C.1 管理风险（包括合法权益影响风险）流程图

在组织内外部环境中执行风险评估程序。

风险评估指的是风险识别、风险分析和风险评价的全过程，具体情况如下：

a) 风险识别：通过威胁分析、危害性分析、脆弱性分析和合法权益风险分析对风险进行识别、分级和成文的过程。该过程考虑风险成因、来源及可能影响组织及其利益相关方的事件、情形和情况。识别内容宜包括可能妨碍组织完成其业务、策略和运行目标的所有风险来源，包括客户、组织代表人员及其他内外部利益相关方的权利和安全。

b) 风险分析：理解风险和风险程度的过程。该过程为确定宜处置的风险及处置风险最适当的方法提供了依据。同时考虑风险成因和来源、风险后果（包括严重程度）及事故和相关后果发生的可能性。组织宜确定当威胁成为事实时，事件对利益相关方造成的后果。风险等级随着可能性、严重程度及后果变化，为风险处置的优先顺序提供了依据。

c) 风险评价：在环境建立时，在预期风险程度和风险准则间对比的过程。风险评价确定了风险水平和风险类型的重要性。进行风险评价时利用了风险分析中对风险的了解，以做出风险排序、风险控制和风险处置时需要的战略决策。

C.5.1.3.2 合法权益风险分析

合法权益风险分析指的是确立、评价与合法权益相关的风险及其影响的过程，并形成文件，其目的是控制风险、减少或防止危害合法权益的影响、违法行为。合法权益风险分析又被称为“合法权益风险评估”或“合法权益影响评估”。合法权益风险分析宜同时评估风险的消极和积极结果。消极影响按风险事件后果的严重程度分级和考虑。评价风险的积极后果可以为改善利益相关方的风险环境提供机会。合法权益风险分析为综合风险评估过程的一部分。

进行全面合法权益风险分析为识别、评价、管理及文件化风险提供了依据，可以预防、减缓及记录侵

害合法权益和违规违法，成为避免组织卷入侵害合法权益和违规违法行为必要的尽职调查的一部分。组织宜确定与其活动有关或与其业务关系和潜在资源直接相关的潜在和实际合法权益风险，同时宜分析风险的可能性、严重程度及后果以确定风险顺序并采取适当措施来预防、减缓和外置风险。

合法权益风险分析过程为：

a) 评估与组织的保安服务运行活动直接相关和与组织的客户、分包方、外包合作伙伴、供应链及其他业务关系相关的风险；

b) 与受风险和相关活动影响的内外部利益相关方进行沟通和有意义的协商；

c) 识别和取得必要的合法权益专业知识和能力，以进行合法权益风险分析，并证明合法权益风险程序贯穿始终；

d) 文件化风险评估过程，从而进行评审、整合、按调查结果行动、追踪响应的有效性、外部沟通、报告如何消除影响和诉讼保护。

C.5.1.3.3 风险评估过程注意事项

风险评估可帮助理解风险及风险的起因、可能性、严重程度和后果。因此，组织宜在其保安服务运营管理体系范围内进行综合风险评估，并考虑与以下各项相关的投入与产出(有意和无意的)：

a) 其活动、产品和服务；

b) 与环境和社会群体的相互作用；

c) 与内外部利益相关方的关系；

d) 公共建设和相互依赖性。

风险评估宜包括对关于组织使命达成的不确定因素的详细分析和评价，及尊重所有利益相关方权利的组织责任，举例包括但不限于：

a) 与使命和运行相关的策略性风险；

b) 与组织及其客户的声誉有关的风险；

c) 组织活动的政治、经济和社会影响；

d) 对组织工作人员的威胁和造成的后果；

e) 对社会群体及其他利益相关方的威胁和造成的后果及运行对他们合法权益的潜在影响；

f) 与业务关系相关的风险，比如分包方和外包合作伙伴以及与参与保安服务运行的其他组织的相互影响；

g) 策略和运行风险的相互关系及尊重生命和合法权益的内在关系。

风险评估的方法很多。组织宜建立、实施并维护成文的且可重复使用的正规方法。最高管理者宜清晰定义和评审其假设、范围、评价准则和结果。

一个组织可能存在很多风险，因此，宜建立和文件化确定重大风险的准则和方法。单一方法无法确定重大风险。但是，所采用的方法宜提供一致结果，且宜包括评价准则的建立和应用，比如关于生命和合法权益保护、不良权益影响的严重程度、预防或减缓不良影响的作用、活动和功能的危险程度、法律问题及对内外部利益相关方的关注等评价准则。组织宜分析非预期事件或干扰性事件的可能性和严重程度及对组织运行和利益相关方造成的后果，并识别在时间和目标上优先响应和恢复的关键运行。

评估后果时，组织宜考虑以下各点。

a) 人力成本：对客户、组织工作人员、供应商、社会群体及其他利益相关方造成的身体和心理伤害。

b) 财务成本：设备和资产重置、停工、加班费、股票贬值、销售/业务损失、诉讼、行政处罚等。

c) 形象成本：声誉、社会地位、负面舆论、客户流失等。

d) 合法权益影响：特定运行环境内，对特定人员和群体(尤其是弱势群体或边缘群体)的实际或潜在合法权益影响。

e) 间接影响：对区域经济及区域经济利益减少等影响。

f) 环境影响：环境质量或濒危物种的影响。

风险评估是吸收必要的内外部合法权益专业知识兼容并蓄的过程，包括与内外部利益相关方（含受影响的潜在利益相关方）进行有意义的协商。风险和影响识别、分析和评价过程的框架在组织的运行环境内形成，因此宜考虑内外部环境、法律法规及其他要求。

为得到准确反映组织风险预测的结果，宜由受过合格培训的团队（包括合格和得到认可的专家）收集风险评估数据。宜选择收集管理、财务、技术、社会和物理数据的取样技术，以保证取样的代表性。风险评估并不是精密科学，因此假设和信息可靠性宜形成文件。收集数据期间，宜直接向保安服务管理体系范围内的组织运行单位咨询。风险评估的结果宜由最高管理者报告和评审，以确定保安服务管理的目的、目标及战略。组织宜根据以下内容确定风险评估的范围：

a) 保安服务管理体系的范围（产品、服务和活动）；

b) 客户期望和义务；

c) 法律法规及合同要求；

d) 尊重合法权益的责任；

e) 受影响社会群体和利益相关方的期望；

f) 风险偏好；

g) 业务关系、相互依赖性及公共建设要求；

h) 资料/信息要求。

风险评估过程宜考虑正常和异常运行状态及合理地预测干扰性情况，以便更好控制非预期事件和干扰性事件。但由于无法预测所有非预期和干扰性情况，组织也宜在不考虑事件本质的情况下，考虑事件对关键资产、活动和功能及受影响社会群体和利益相关方造成的后果，以便预先管控其风险。

风险评估宜：

a) 用有相关成文的定量和/或定性方法来预估识别到的潜在风险的可能性或概率以及事件发生时后果的严重性；

b) 基于合理和明确的准则；

c) 充分考虑对组织运行有影响的所有潜在风险；

d) 考虑组织与其他各方的相互依赖性，包括客户、社会群体、商业关系和供应链的依赖和约束；

e) 评价法律义务和其他义务的结果及管理组织活动的自愿承诺；

f) 考虑与利益相关方、承包商、外包合作伙伴、供应方及其他受影响方相关的风险；

g) 分析风险相关的信息，并选择可能导致严重后果和/或后果严重性难以确定的风险；

h) 分析和评价管理风险所需的成本、效益和资源；

i) 评价组织可通过杠杆控制和作用的风险和影响。

注：由组织决定对风险接受、风险规避、风险管理、风险最小化、风险容忍的转移和/或处置的控制程度及策略。

在某些地区，关键基础设施、社会群体资产和文化遗产可能是组织运行所在周边的重要组成部分，因此，在理解其组织风险和对周围环境的影响时宜将其考虑在内。

在开发与其相关的重大风险的信息时，组织宜考虑记录为目的保留信息、设计和实施保安服务管理体系的需求。

风险识别和评价过程中宜考虑活动的位置、实施分析的成本和时间以及可靠资料的可用性。该过程中可使用为业务策划、监管或其他目的而开发的信息。

组织宜在活动的整个周期中定期进行重新评估，以应对不断变化的组织运行、运行环境和对事件的响应。导致重新评估的变更可能包括：

a) 合同与行业趋势；

b) 商业关系；

c) 运行上的新活动和重大变更；
d) 法律法规要求；
e) 政治环境；
f) 事件引起的情况；
g) 基于绩效的试验/测试结果。

这种识别和评价风险的过程并不改变或增加组织的法律义务。

C.5.1.4 内外部风险沟通和协商

组织宜与合适的利益相关方建立正式交流和协商流程，以收集风险评估输入信息和控制散播结果。在风险沟通和协商过程中宜考虑信息的敏感性和完整性。

C.5.2 保安服务目标及实现策划

C.5.2.1 总则

确定目标和目的是为了实现组织保安服务运行政策的目标和承诺。通过设定保安服务目标和指标，组织可将政策转换为保安服务运行策略中描述的行动计划。目标和指标宜具体并且可测量，以便跟踪过程，及确定保安服务管理体系在改善整体组织准备方面的表现。

保安服务管理体系的“目标”是重要事项，例如将意外最小化的目标。保安服务的“指标”即根据关键指标对绩效进行具体测量。目标和指标宜依据风险评估适合组织，且宜反映组织的工作、执行情况和想实现的目标。适当的管理层级宜明确目标和指标，同时宜定期评审和修订目标和指标。

当设定了目标和指标后，组织宜考虑建立可测量的保安服务运行关键绩效指标。这些指标可用作保安服务运行绩效评定系统的基础，并且可提供有关保安服务管理体系和具体预防、减缓、响应和恢复策略的信息。

在建立目标和指标时，组织宜考虑：

a) 政策承诺；
b) 与战略目标相一致；
c) 风险评估结果；
d) 风险偏好及风险容忍；
e) 法律法规及其他要求；
f) 内外部环境；
g) 绩效准则；
h) 基础建设要求和相互依赖关系；
i) 利益相关方的利益；
j) 技术选项；
k) 财务、运行和其他的组织考虑；
l) 实现目标所需的行动、资源以及时间节点。

在考虑技术选项时，组织宜考虑在经济上可行、具有成本效益和经判断适当的且可获得的最佳技术。

组织的资金需求并不意味着组织必须使用特定的成本会计方法，组织可选择考虑直接、间接和隐性成本。

C.5.2.2 实现保安服务运行和风险处置目标

保安服务运行战略和行动计划是成文的实现组织目标和指标的方法。战略宜与其他运行计划、战

略和预算协调或统一。行动计划可细分为处理组织运营的具体要素。

为了成功管理保安服务运行，战略和行动计划宜明确：

a) 实现目标的责任(谁将负责？在哪里实现?)；

b) 实现目标的手段和资源(如何实现?)；

c) 实现这些目标的时间表(何时完成?)。

战略也可再细分以落实组织运行的具体要素。只要在每个成文的策划中足够详细地明确了关键责任、策略步骤、资源需求和时间表，组织就可采用若干行动计划。

在适当和切实可行的情况下，战略宜包括与策划、设计、建设、试运行、运行、改进、服务、销售、外包和终止试运行有关的组织活动各阶段需考虑的事项。战略开发可为当前活动和新活动，新产品和/或新服务进行战略开发。

组织的策划中宜考虑活动、合同义务、员工和社会群体以及运行连续性优先顺序的必要性。

战略宜是动态的，可被监视和修改，如：

a) 风险评估结果有变化；

b) 修改或增加了目标和指标；

c) 引入或更改了相关法律法规要求；

d) 已经(或尚未)在实现目标和指标方面取得实质性进展；

e) 活动、产品、服务、过程或设施变更或出现其他问题。

确定保安服务运行策略可使组织能够评价一系列选项。组织可为每个活动选择适当的方法，使其能够在可接受的水平上运行。最合适的单个(或多个)战略宜取决于一系列的因素，比如：

a) 组织的风险评估结果；

b) 实施单个(或多个)战略的成本；

c) 不作为的后果。

最高管理者宜批准文件化的战略来确认已确定的保安服务运行战略已经适当地实施中，这些战略已经解决了非预期事件或干扰性事件的可能成因和影响，且所选择战略适合组织风险偏好内的组织目标。

战略还宜考虑组织与外部利益相关方的关系、相互依赖性和义务关系。利益相关方包括客户、供应方和外包合作伙伴，以及公共机构和社会群体中的其他方。组织宜建立和维护以保护利益相关方生命和安全为先，同时尊重合法权益并保证所提供的产品和服务完整的战略。此外，宜确定与公共机构和社会群体其他方的互动和协调，并将其纳入战略发展中。与外部利益相关方的这些战略安排宜支持实现保安服务运行目标，且要详细说明并形成文件。

C.6 支持

C.6.1 资源

C.6.1.1 总则

保安服务管理体系所需的资源宜得到确认，包括人力资源和专业技能、设备、内部基础设施、技术、信息和财务资源。最高管理者宜确保保安服务管理体系所需资源的确定、提供和维护。

C.6.1.2 结构要求

C.6.1.2.1 总则

合同为客户和承包方之间关系的主要法律依据。订立合同的双方宜为法人实体，并且组织宜明确授权代表签订合同。

C.6.1.2.2 组织结构

组织宜建立一个管理结构，明确界定履行合同义务所必需的角色、责任和职责。

C.6.1.2.3 保险

组织宜寻求充分的保险类型，以满足对任何人关于符合其风险评价的人身伤害、死亡或财产损失的所有赔偿责任。保险类型宜至少为客户规定的类型或得到现有行业惯例认可。保险宜包括雇主和公众责任险。宜提供与人员工资结构和服务风险水平相适宜的健康和人寿保险。

寻求保险范围时，组织宜考虑：

a) 在合同中规定政策和限制；
b) 政策的管辖区域及争议发生情况；
c) 地区限制；
d) 赔偿限制；
e) 所有活动，包括使用防卫装备；
f) 代表组织工作的人员和受影响的有关人员的医疗保险和治疗；
g) 分包方的活动；
h) 保护客户。

宜考虑的保险类型包括(但不限于)：

a) 债务；
b) 工伤赔偿；
c) 意外事件；
d) 财产损失。

C.6.1.2.4 外包和分包

合同宜为承包方和分包方之间的关系提供法律依据且宜规定承包方、分包方履行的责任条款和条件。组织承担外包或分包给另一个实体所有活动的责任。

C.6.1.2.5 财务和管理程序

组织的财务和管理控制程序，除支持提供有效的安全和风险管理外，也宜解决显著的财务风险。

C.6.2 能力

C.6.2.1 总则

组织宜确定任何具有责任和权限的人所需的意识、知识、理解和技能，并代表其执行指标，包括：

a) 为可能受非预期事件或干扰性事件影响的内外部利益相关方制定培训和提高意识方案；
b) 要求为其工作的承包方、分包方能证明其雇员具备必要的能力和接受过适当的培训；
c) 确定必要的经验、能力和培训的水平，以确保被记录的人员有能力执行专门的保安业务管理体系管理活动；
d) 宜持续开展监控和重新评估培训的水平，以确定改进的机会。

为代表其工作的人员提供充分的培训是组织的责任，宜在履行其职责的情况下，在岗前和岗中进行培训。确定的培训目标宜以风险评估为基础，并促进培训要求的一致性和标准化。培训宜包括保护合法权益的内容。

C.6.2.2 能力认定

组织宜识别和评价执行保安业务活动所需的能力与相关个人能力之间的差距。这些差距可通过额外的教育、培训或技能开发方案来弥补，可包括以下步骤：

a) 能力和培训需求识别；
b) 为达到具体能力和培训需求设计与开发培训计划；
c) 选择适当的方法和物料；
d) 符合保安服务管理体系培训要求的验证方法；
e) 培训目标群；
f) 记录和监控受到的培训；
g) 根据培训需求与要求评定受到的培训；
h) 必要时，改进培训计划。

组织的培训宜包括适用的法律法规中明令禁止的行为，如：

a) 严禁限制他人人身自由，搜查他人身体、或者侮辱、殴打他人；
b) 严禁扣押、没收他人证件，财物；
c) 严禁阻碍依法执行公务；
d) 严禁参与追索债务、采用暴力或者以暴力相威胁的手段处置纠纷；
e) 严禁删除或扩散保安服务中形成的监控影像资料、报警记录；
f) 严禁侵犯个人隐私或者泄露在保安服务中获知的国家秘密、商业秘密及客户单位明确要求保密的信息；
g) 严禁有违反法律、行政法规的其他行为。

C.6.2.3 培训及能力评定

培训可包括一般性主题和以指标及特定状况为主题的培训，用于具体合同和具体情况下对人员进行培训，使其履行相应职责。一般主题包括但不限于：

a) 使用枪支和其他防卫装备；
b) 保护合法权益的相关法律法规；
c) 宗教、性别和文化问题，以及尊重当地居民；
d) 处理投诉：具体方法是将其转交给有关部门；
e) 打击行贿受贿、腐败和其他相关犯罪的措施。

指标和特定状况主题的实例可包括：

a) 战术运用；
b) 洽谈技术；
c) 路线引导；
d) 电子沟通；
e) 医疗救护；
f) 社会群体联络；
g) 伤员撤离；
h) 合同条款或组织提供的服务中规定或暗含的指标。

组织宜进行实用的、以情景为导向的培训，这将要求接受过培训的人员在反映保安人员执行任务时可能面对的情况下做出决定，并对所做决定的后果做出反应。

培训和意识方案可包括：

a) 整个组织的工作人员就如何执行保安服务管理方案而进行的协商过程；

b) 在组织的时事通讯、简报、入门方案或期刊(包括新员工入职培训)中进行关于保安服务管理的讨论;
c) 将保安业务管理放在相关网页或内联网上;
d) 在组织学习管理体系中加入在线培训模块;
e) 通过后续活动报告从内外部事故中学习;
f) 将保安服务管理作为管理小组会议中的一项;
g) 会议及课堂培训;
h) 紧急救护及其他实际操作培训。

所有人员都宜接受培训,来履行其个人与保安服务管理体系相关的责任。他们宜简单了解保安服务管理体系关键点,以及直接影响他们行动的保护合法权益相关法律法规,并接受相关培训。这种培训可包括关于预防和缓解措施、回应、文件编制和问责要求以及处理社会群体、客户和媒体询问的程序。

防卫装备使用培训,包括使用枪支的培训。培训宜包括指导性培训、基于情景的培训和防卫装备使用培训。

事件应急响应小组宜接受关于他们责任和义务的教育与培训,包括与现场急救员及其他内外部利益相关方的相互配合。小组成员宜定期接受培训(至少每年一次)。新成员在进入组织时宜接受培训。这些小组还宜接受预防非预期事件的培训。组织宜将相关的外部利益相关方和资源计入其能力、意识和培训方案中。

C.6.2.4 文件编制

组织宜保留以下记录:
a) 能力鉴定及检验指标;
b) 培训方案;
c) 对组织工作人员培训及评定的相关记录。

C.6.3 意识

组织宜在其内部建立、发扬和灌输保安服务管理文化,这种文化能:
a) 确保保安业务管理文化和尊重合法权益成为组织核心价值观和管理的一部分;
b) 使利益相关方了解保安服务管理方针及其在任何计划中的作用;
c) 有利于提高个人绩效。

C.6.4 沟通

.6.4.1 总则

有效沟通是预防、管理和汇报非预期事件或干扰性事件最重要的因素之一。宜与内外部利益相关方进行积极的沟通和协商,以传达日常情况、警报、干扰性事件以及组织和社会群体的响应信息。为了给各个群体提供最好的交流和适当的消息,可适当地对受众进行分区管理。通过这种方式,可将消息发给诸如员工、客户、社会群体或媒体等特定群体。

沟通和协商程序及过程宜考虑:
a) 组织各个层面和活动之间以及与承包方、分包方、客户和合作实体之间的内部沟通;
b) 利益相关方的需求;
c) 接收、记录和回应来自外部利益相关方(包括社会群体)的相关信息;
d) 积极规划与外部利益相关方(包括媒体)的沟通;
e) 与相应利益相关方提前进行的关于响应和报告计划的沟通,并保证规划到位;

f) 促进与紧急响应人员的结构化沟通；
g) 在干扰性事件下沟通渠道的可用性；
h) 信息的敏感性和详细程度；
i) 工作环境。

组织宜实施接收、记录和回应内外部利益相关方有关信息的程序。这一程序可包括与利益相关方的对话和对其相关顾虑的考虑。在一些情况下，对利益相关方顾虑的回应可包括与组织活动和业务有关的风险、影响和控制程序相关的信息。这些程序还宜解决与有关部门就应急计划制订和其他相关问题进行的必要沟通。

C.6.4.2 运行沟通

需要业务沟通计划，以对正在进行的保安服务提供充分控制、协调和关注。业务沟通计划宜包括对保安服务工作人员、客户与政府之间如何分享相关威胁信息。

C.6.4.3 风险沟通

组织还宜与负责潜在非预期事件和干扰性事件情报、警告、预防、响应和恢复的社会群体、公共机构、其他组织确定并建立关系。组织宜正式规划其预防、缓解和响应沟通战略，同时考虑到针对相关目标群体的决定、适当的信息和主题以及手段的选择。

组织宜建立与内外部利益相关方沟通和协商的程序，其内容关于具体组织风险、风险影响和控制程序。这些程序宜考虑具体的利益相关方、要沟通的信息类型、干扰性事件的类型及其后果、沟通方法的可用性以及组织的个别情况。外部沟通方法可包括：

a) 新闻或新闻稿；
b) 媒体；
c) 财务报告；
d) 网站；
e) 社交媒体；
f) 电话、电子邮件和短信；
g) 社会群体会议。

组织宜对干扰性事件进行预先规划沟通。可为风险评价中识别出的威胁事先制定消息模板、脚本和声明草稿，以便传递给风险评价中识别出的一个或多个利益相关方。也宜建立确保信息在短时间内传递的程序。

组织宜指定和公布主要发言人(以及指定的备选人)，发言人宜管理并向媒体和其他人宣传应急沟通，还宜接受关于媒体关系、危机应对和在实时基础上的培训。所有信息宜通过一个单独的小组汇集，以确保消息的一致性。最高管理者宜强调，迅速告知所有组织工作人员关于在何处查询来自媒体的电话，并且只有经授权的发言人可接受媒体采访。在一些情况下，也需要经过适当培训的现场发言人。

C.6.4.4 沟通投诉和申诉程序

组织宜建立并向有关利益相关方传达内外部投诉与申诉程序。程序宜确保隐私和机密性，并适应目标受众的文化、语言、教育和技术要求。宜建立程序，为投诉和申诉创建汇报机制。

C.6.4.5 沟通举报政策

举报出现于组织工作人员关注内外部影响他人的危险、不道德行为或违法行为。组织工作人员可能害怕举报会受到其同事或雇主报复。但是，组织宜鼓励其工作人员表达他们对任何内外部利益相关方的玩忽职守和不当行为的关注。举报方针将有助于组织以适当的方式处理问题，同时也可对那些可

能想做非法、不当或不道德行为的人起到威慑作用。良好的举报方针将有助于组织减少问题、改善工作条件和运行效率。

有效的举报方针为个人提供了除直接管理之外的其他途径，可以提高他们对问题的关注度。因此，组织宜建立和传达举报方针，举报方针可以提供明确的内部机制，以匿名方式汇报在内外部影响他人的危险、不道德行为或非法行为的不合格项和事务。该方针还宜规定外部披露可接受和受保护的情况和条件，以及需要转交给有关部门的情况和条件。只要举报人本着诚意行事的原则并有提出问题的正当理由，就宜受到保护。

C.6.5 成文信息

C.6.5.1 总则

文件编制的详细程度宜足以描述保安服务管理体系和使其各部分协同工作的方法。文件编制还宜提供指导，说明在何处获取有关保安服务管理体系特定部分的操作的较为详细的信息。此文件编制可与组织实施的其他管理体系的文件编制结合在一起，不必非是手册的形式。

不同组织的保安服务管理体系文件编制有着不同的范围，原因如下：

a) 组织的规模和类型及其活动、产品或服务；

b) 过程的复杂性及其相互作用。

文件实例包括：

a) 方针、目标和指标；

b) 适用性声明、一致性声明和道德规范；

c) 重大风险和影响的信息；

d) 程序；

e) 过程信息；

f) 组织机构图；

g) 内部和外部准则；

h) 事故响应、缓解、应急和危机计划；

i) 记录。

文件程序的任何决定宜基于：

a) 不这样做的后果，包括对有形和无形资产造成的后果；

b) 需要证明遵守法律和为组织所认可的其他要求；

c) 确保活动持续进行的需求；

d) 本文件的要求。

有效文件编制的优点包括：

a) 通过沟通和培训更容易实施；

b) 易于维护和修订；

c) 歧义和偏差的风险减小；

d) 论证可能性和明显性。

最初创建目的不是保安服务管理体系的文档可用作此管理体系的一部分，并且(如果使用的话)宜在体系中引用。

C.6.5.2 创建和更新

C.6.5.2.1 总则

程序宜包括控制文件化信息的识别、使用方便性、完整性和安全性。

C.6.5.2.2 记录

除了本文件所要求的记录外，记录还可包括(尤其)：

a) 符合性记录；
b) 持枪证；
c) 对序列化和敏感设备的应负责任；
d) 燃料和其他培训物资报告；
e) 防卫装备使用报告；
f) 合同符合性审计报告；
g) 审计跟踪文件编制；
h) 许可证；
i) 演练和测试结果；
j) 访问控制记录；
k) 分包方的文件编制。

C.6.5.3 成文信息的控制

组织宜创建和保持文件，并使其满足保安服务管理体系的实施。然而，组织的主要焦点仍然是保安服务管理体系的有效实施和保安服务管理的绩效，而不是复杂的文件控制体系。

宜适当考虑机密信息，并建立、传达和保持处理机密资料的程序。宜对机密资料进行明确分级标注以实现对其的以下保护：

a) 资料的敏感性；
b) 个人的隐私、生命和安全；
c) 客户的形象和信誉。

组织宜与其组织内部的权限部门协商，确定文件宜保留的适当时间，并建立、实施和保持有效的过程。记录保留时间应满足相关要求。

C.7 运行

C.7.1 运行策划和控制

C.7.1.1 总则

组织宜对确定存在重大风险的业务进行评估，确保保安服务运行能够控制或降低相关风险及不良后果发生的可能性，以满足保安服务运行管理政策的要求，符合保安服务的目标和指标。评估宜包含保安服务运行的所有内容，包括分包方、供应链和维护活动等。

保安服务管理体系为如何将体系要求运用于日常工作提供指导，因此，要求通过成文程序进行管理，避免因缺乏成文程序导致偏离保安服务运行管理方针、目标和指标。

为最大程度降低非预期事件或干扰性事件发生的可能性，这些程序宜包括行政、运行和技术管理措施。如对现有安排进行修改或重新安排可能对保安服务工作及活动造成影响的，组织宜在实施这些安排之前考虑将相关威胁和风险降至最低。

C.7.1.2 保安服务的要求

C.7.1.2.1 客户沟通

组织在确定拟提供的保安服务要求时，宜确保与客户进行清晰的沟通。针对 8.1.2.1 的 a)～e)，组

织宜：

a) 沟通拟提供的保安服务的详细情况，以使客户理解所提供的保安服务；这些信息可通过会议、宣传单、网络、电话或任何其他适当手段进行沟通。

b) 明确：

——客户向组织咨询或购买保安服务的联系方式；

——通知客户相关更改的内容。

c) 建立适当的途径，以便从客户处获取与问题、关注点、投诉、正面和负面反馈的相关信息；其方法包括但不限于直接发送电子邮件或打电话、在线调查、客户支持渠道、面谈等。

d) 确保在适当时将组织对客户财产的处置和控制方式通知客户。

e) 确保主动地与客户沟通可能采取的应急措施，若需要采取应急措施，则宜避免对满足客户要求产生不利影响，包括对于突发事件、干扰性事件、劳动争议、人员短缺或后备外部供方不足等情况的应急措施。

沟通能使客户理解组织可提供或预期提供的保安服务，使客户理解或确认客户的需求和期望。

C.7.1.2.2 保安服务要求的确定

组织在确定保安服务要求时，宜考虑：

a) 客户提出的保安服务的内容与要求；

b) 客户未明确保安服务的要求，但提出了服务的对象（如金融网点、重点区域等），服务满足对服务客户的保安服务要求；

c) 与保安服务相关的适用法律法规及相关文件的要求；

d) 组织认为必要的附加要求。

组织需要确保履行对所提供保安服务做出的声明。此声明是组织关于提供给客户的保安服务及其特点与技术方案的陈述。例如组织可能对其提供的保安服务符合客户的项目技术要求做出声明，比如特别针对人员要求、保密协议、廉洁协议等做出声明。

组织宜考虑以下因素：

——可用资源；

——服务能力；

——服务时间。

GB/T 19010 提供了组织行为规范指南，包含了做出声明的相关内容。

C.7.1.2.3 保安服务要求的评审

组织在对客户作出承诺前，对履行这些承诺的能力做出评审，可使组织降低在运行期间和交付后发生问题的风险。

针对 8.1.2.3 的 a)～g)，组织宜评审：

a) 交付和交付后的措施需求，如人力资源保障、客户培训、现场服务、客户支持等；

b) 是否满足隐含的要求，即保安服务能够满足客户的期望（如服务人员职责的履行情况，服务人员应有礼仪并乐于提供帮助，人员规模应达到要求）；

c) 组织选择的为超越客户期望、增强客户满意或符合内部方针等方面的额外要求；

d) 适用的保安服务法律法规要求是否已经考虑并做出应对；

e) 合同或协议是否已经做出更改；

f) 若之前规定的要求与合同或协议中的表述存在差异，则组织需要与客户沟通并消除这些差异；

g) 若客户未就其要求提供成文的说明，如仅通过电话或口头说明进行确定，则组织需要在提供保安服务之前与客户确认这些要求（如在服务过程中，增加人员规模或减少人员规模）。

组织宜保留上述内容的成文信息，以证实与客户之间达成的最终协议，包括任何纠正或更改，并表明能够满足客户要求。

针对 8.1.2.3 中第二段组织保留成文信息中的 a)和 b)：

a) 评审结果可通过适当的载体予以保留，如组织可选择保留经筛选的与客户之间的电子邮件信息或者可保留详细的风险评估报告；

b) 若评审表明存在额外或更改的要求，则宜更新或增补成文信息，以确保新要求已被获知（如更改订单或消除误解的邮件沟通内容都应予以保留）。

这些成文信息可为组织与新客户或现有客户在未来签订类似协议时提供依据。

C.7.1.2.4 保安服务要求的更改

本条旨在确保组织内外部的相关人员知晓对保安服务要求的任何更改。组织宜选择适宜的沟通方法，并保留适当的成文信息，如沟通的邮件、会谈纪要、补充协议等。

C.7.1.3 保安服务的设计和开发

C.7.1.3.1 总则

本条旨在确保组织建立、实施和保持设计和开发过程，以确保其保安服务满足要求，并确定服务能力。组织在确定保安服务管理体系的范围时，宜考虑包括有关相关方在内的组织环境，因为该范围决定了 8.1.3 要求的适用情况。

有些组织可能需要考虑所有的设计和开发要求，而另外一些组织仅需考虑某些要求，如设计开发更改或客户沟通等。

严格按照客户的需求的组织，只有在客户对设计方案做出了修改或就人员要求更改进行沟通时，需要考虑设计和开发要求。

在某些情况下，基于保安服务管理体系范围、客户或法律法规要求或最佳运行实践，组织可能决定将设计和开发要求用于运行过程。

C.7.1.3.2 设计和开发策划

本条旨在确保组织进行设计和开发策划，以确定所需的设计和开发活动和任务。这些策划宜包括考虑组织确定所需的措施（见第 6 章和 8.1），这些措施可能对策划活动的实施、资源需求以及岗位和职责的界定产生影响。

本条的要求提供了在设计和开发策划期间需要考虑的一组关键要素。针对 8.1.3.2 的 a)～j)，包括考虑：

a) 保安服务的复杂性（如重复设计、新设计、保安服务目的、服务的预期期限和范围等突出特征）以及交付要求等因素；

b) 必要的阶段，包括适用的设计和开发评审（如初步设计、详细设计）以及验证（如所有服务区域都在技术方案进行了适当地确定）和确认（如进行试运营效果测试）；

c) 确保输出满足输入要求所需的验证活动，以及确保最终保安服务满足规定的使用或预期目标要求的确认活动；

d) 从事设计和开发的人员，即确定设计和开发过程中所涉及的必要职责和权限；

e) 所需的内外部资源（如组织知识、人力资源、设备、技术、能力、客户或外部供方的支持、临时工作人员、提供技术信息的规范或标准）；

f) 设计和开发过程参与人员之间的沟通，要考虑参与人员的数量和最有效的信息共享方式，如会议、远程通信、会议纪要等；

g) 在设计和开发活动中，客户和使用者的潜在参与（如客户的现场监视、客户测试、客户体验）；

h) 组织内人员提供服务人员或交付服务所需的条件（如技术方案、控制措施、人力资源、接收准则）；

i) 客户或其他相关方就过程所确定的期望控制水平（如石油管道、铁路线路的安全巡护或地铁乘客的安全检查）；若客户未确定明确的控制措施，组织则宜在考虑保安服务类型的情况下确定所需的控制措施；

j) 所需的成文信息，以证实是否已满足设计和开发要求，以及在评审、验证和确认阶段过程是否得到适当实施，如项目策划、会议纪要、措施项的完成情况、测试报告、作业指导书或服务流程图。

C.7.1.3.3 设计和开发输入

本条旨在确保组织将确定设计和开发项目的输入作为设计和开发策划期间的一项活动。这些输入宜清晰、完整并与规定保安服务特性的要求相一致。针对 8.1.3.3 的 a)～e)，组织宜考虑：

a) 客户、市场需求或组织确定的功能和性能要求，如设备的使用期限、提供特定服务的装备、在特定时段提供的服务；

b) 从以往类似设计和开发活动获得的信息，如项目文件、规范或吸取的教训，这可提高有效性，并使组织能够基于良好实践或避免出现错误；

c) 与保安服务直接相关的法律法规要求（如保安服务管理条例），或与保安服务提供相关的法律法规要求（如保安服务中对犯罪嫌疑人的处置，在提供铁路巡护服务时不进入线路）；

d) 组织承诺遵守的操作标准或规范（如行业规范、健康安全标准）；

e) 因保安服务性质导致失败所产生的潜在后果；这些失败的影响范围可能从潜在的灾难性后果（如因应急预案不当而可能导致事故），到产生使客户不满意的各种问题（如人员脱岗或不满足数量）。

应用于设计和开发的输入宜作为成文信息予以保留，这些输入可能是项目策划中所列举的特定规范或规格说明。

在输入要求存在冲突、难以处理或实现的情况下，组织宜采取有关措施，解决这些问题。

C.7.1.3.4 设计和开发控制

本条旨在确保输入一旦确定之后，则宜根据策划实施设计和开发活动并加以控制，从而确保过程有效。

评审、验证和确认活动对控制设计和开发过程至关重要，需要得到有效的实施。评审、验证和确认可能共同作为单一过程完成或作为独立活动分开完成。针对 8.1.3.4 中 a)～f)，组织宜确保以下方面。

a) 参与设计和开发活动的所有人员知晓并充分理解客户或最终用户的要求和预期的最终输出；当偏离要求时，如在策划提高服务方面偏离了要求，则需要考虑诸如成本和易用性等因素。

b) 设计和开发策划各阶段及其输出的评审均已实施，以便确认其满足了输入要求、确定了问题并制定了解决方案；不参与设计和开发过程具体阶段的人员可参与其评审，包括参与提供服务的人员以及相关客户、最终用户和外部供方。就复杂性的不同程度而言：

——复杂设计的评审可能在正式会议上进行，其会议纪要将作为相关记录；

——简单设计的评审可能不需要那么正式，其记录可能由计划上表明已得到评审的批注、评审人员的签名和签署日期组成。

c) 进行验证，以确保满足在设计和开发过程之初所识别的所有要求；对于较大的项目，其过程可划分为若干个关键阶段，在每个关键阶段结束时按要求进行验证。验证活动可包括：

——实施替代计算；

——将新设计与已证实的类似设计进行比较；
——开展测试和演示；
——发布前检查设计阶段的成文信息。

d) 进行确认，以确保最终保安服务满足客户或最终用户的特定要求或预期用途。确认活动的示例可包括：
——试运行；
——运行测试；
——按照用户的预期条件进行模拟或测试；
——部分模拟或测试(如模拟突发事件的应急处置)；
——客户或最终用户测试，并提供反馈。

e) 若评审、验证和确认活动显示存在问题，则宜确定解决这些问题的措施；对这些措施有效性的评价宜作为下次评审工作的一部分。

f) 保留评审、验证和确认活动的成文信息，作为证明设计和开发活动已按照计划实施的证据，可包括会议纪要、检验和测试报告以及客户批准文件。

C.7.1.3.5 设计和开发输出

本条旨在确保设计和开发输出为提供预期产品和服务所需的所有过程(包括采购、培训和交付后活动)提供必要的信息。这些信息宜足够清晰，以确保参与者都理解将采取的措施和其相关顺序。

针对 8.1.3.5 的 a)～d)，设计和开发输出宜：

a) 与 8.1.3.3 所规定的输入要求保持一致；

b) 考虑到输出的使用者和使用条件，足以确保所有提供保安服务的后续过程得到实施；

c) 提供有关监视和测量要求方面的明确信息，包括外部提供的过程、保安服务的所有接收准则，以及保安服务放行的细节；

d) 提供有关保安服务特性的必要信息，以确保以安全和适宜的方式提供服务，并详细说明如何提供服务(如门卫出入登记方法)。

设计输出宜作为成文信息予以保留，包括但不限于：

——服务规范(包括防护细节)、人力资源说明、质量计划、控制计划；
——过程规范、必要的人员来源详细情况；
——服务计划；
——工作指导手册；
——由实施方案所确定的岗位设计以及所要使用装备的规格说明；
——以计划形式呈现的，对营销活动的广告代理设计。

C.7.1.3.6 设计和开发更改

本条旨在使组织能够确定、评审和控制在设计和开发过程期间或后续阶段所做的更改。组织宜将如何实施与其他过程或相关方(如客户或外部供方)之间的互动作为设计和开发过程的组成部分，并宜在确定进行设计和开发更改时予以考虑。

更改可在保安服务管理体系内的任何活动和阶段，包括但不限于：

a) 在实施设计和开发过程期间；

b) 在发布和批准设计和开发输出之后；

c) 将客户满意和外部供方的绩效作为监视结果时。

有关设计和开发更改而保留的成文信息，可包括更改对保安服务的组成部分或已交付保安服务所产生影响的评价结果，以防止产生不利影响。评审、验证和确认过程通常可产生清晰地说明设计和开发

更改的成文信息。成文信息也可详细说明对受到影响的后续过程(如采购、培训、保安服务提供)所采取的措施,以及如何沟通这些措施。

成文信息宜表明授权由谁进行更改。这种授权有时是来自客户或监管机构的要求。成文信息可以是经批准的更改单或电子签名更改单。

C.7.1.4 保安服务的提供

C.7.1.4.1 总则

服务过程宜按照合同义务和尊重合法权益的要求,提供保护人身安全以及有形和无形资产安全的相关功能。

C.7.1.4.2 保安服务提供过程控制

本条旨在使组织对保安服务提供过程进行控制,通过减少出现不合格输出的可能性,确保实现预期结果。

组织宜设立保安服务提供的受控条件,以确保符合保安服务行为规范、道德准则和与客户签订的合同要求。

在确定需要对什么进行控制时,组织宜考虑保安服务提供的整个周期,包括对交付后的活动要求(如投诉处理)。组织宜考虑以下所有适用方面。

a) 规定拟提供服务或进行活动的特性的成文信息的可获得性;组织宜向参与活动或过程的人员提供易于理解的成文信息,如行为规范或作业指导书,以及其他有助于确保保安服务符合特定要求的内容。

b) 任何必要的监视和测量资源,这可以是为进行特定测量已校准的、得到识别的测量设备,或在交付服务中使用的规定方法。

c) 确保输出满足服务要求所需的任何监视和测量活动,如在规定阶段进行的产品检验或对客服电话的监听。

d) 任何有关基础设施或过程环境的必要准则。

e) 确保人员具备开展工作的能力的需求(如急救和伤亡护理),包括考虑任何必要的资格。

f) 确保其输出不能通过后续监视或测量加以验证的过程得到确认(确认是指通过提供客观证据,证实已经满足了对特定预期用途或应用的要求),示例可包括伤害事件的应急响应,或发生群体事件等紧急措施。

g) 组织宜采取措施防止人为错误,如限制过长的工作时间、采取适当措施促进形成适宜的工作环境、提供适当的培训和指导、过程自动化、对关键信息要求双重电子准入、提供可用设备以避免使用错误装备、避免人员注意力分散(如个人电子设备等)、轮班制、要求提交前完整填写信息。

h) 对放行、交付和交付后活动实施控制;通常包括有形资产或无形资产交付前的验收、维护、接受客户投诉等。

C.7.1.4.3 保安服务提供过程的更改

本条旨在确保组织对保安服务提供期间发生的更改进行评审和控制,以符合保安服务策划期间所确定的要求。组织宜重点关注为处理这些更改所确定的措施,以确保服务持续满足适用的要求。

本条针对的是在保安服务提供期间实施的影响要求符合性的更改。组织宜通过控制这些更改,评审所采取的措施,以及评审这些措施如何影响保安服务满足要求所实施的控制,确保服务提供的完整性得到保持。

在实施所建议的更改之前,宜在运行的各个阶段对其进行审查。

更改的原因可能各不相同，例如，更改的需求可能来自外部供方、内外部因素（如新的或已修订的顾客或法律法规要求）。

在特定情况下，更改的实施结果可作为设计和开发活动的输入。

组织宜确定拟保留的成文信息和其保留方式，其示例包括：

a） 评审活动的会议纪要；

b） 验证和确认的结果；

c） 对更改的描述；

d） 授权进行更改的人员的详细情况（适当时考虑顾客）。

C.7.1.4.4 急救和伤亡护理

组织人员宜接受急救和伤亡等救护类入门培训和后期强化培训，重点训练遭受攻击、意外伤害或突发事件发生后心肺复苏及伤员救护等初级救护的处理。培训宜达到合格标准，并取得救护员资格证书。培训内容宜至少包括：建立和维护救治区安全、伤情稳定、准备和请求撤离，其中包括保障实施救治的人员安全不会继续受到附近其他蓄意或无意威胁。此外，培训宜包括根据受伤严重程度进行救治的优先排序。组织宜确保等候伤员疏散期间，个人和保安服务团队配有用于及时治疗和维持伤情稳定的必要材料（医药用品或固定器械）。

C.7.1.5 尊重合法权益

组织有义务根据适用法律法规的要求尊重合法权益。同时宜建立、实施和程序保护个人尊严的程序并形成文件。宜制定规程并与相关方沟通，报告和矫正不合规情况。

C.7.1.6 非预期事件或干扰性事件的预防和管理

服务过程宜强调对可能导致非预期事件和干扰性事件的风险进行预防性和前瞻性管理，并宜阐明事件发生后的响应、恢复和补救措施。

非预期事件或干扰性事件发生的事前、事中和事后，组织宜建立合适的行政和财务体系以有效支持保安服务管理体系。宜建立程序并形成书面化文件，确保授权透明、符合通用会计准则和行业最佳实践。因此，宜明确规定管理结构、决策权限和责任（包括开支控制、执行权限和责任）。

C.7.2 建立行为规范和道德准则

组织宜为其员工、分包方建立、实施和维持“道德规范”。“道德规范”宜清晰传达尊重合法权益，严禁贿赂、利益冲突、腐败和其他犯罪行为（如使用合法或非法物品来向绩效施加影响）。“道德规范”宜确保所有代表组织工作的人员了解其尊重合法权益、防止和报告侵犯合法权益行为的责任。

组织宜向代表本组织工作的所有人员清晰传达“道德规范”内容并展开相关培训。传达和培训宜成文并维护。

C.7.3 防卫装备使用

C.7.3.1 总则

防卫装备使用不当可能导致人员的死亡或受到严重伤害，进而损坏组织声誉、为组织带来法律责任，还会影响被保护方的利益。防卫装备使用不当还包括未能有效使用已有防卫装备防止组织人员伤亡、保护目标人员和资源及附近区域的其他保护对象。

组织的防卫装备使用程序是控制防卫装备使用不当风险的关键工具，因此防卫装备使用程序需要：

a） 清晰且被所有配备枪支的专职守护、押运人员及监督人员了解；

b) 适用于复杂情况；

c) 由组织严格实施。

清晰的程序、有效的培训和严格的执行会帮助组织方完成任务，并能够促进法律法规的遵守和组织运营区域的长期稳定。

C.7.3.2 防卫装备使用原则

组织可制定在保安服务工作环境下使用防卫装备的指导方针。方针宜阐明适用的通用原则，包括：

a) 仅在自卫、保护他人，或控制、防止特定财产遭到破坏时使用防卫装备；

b) 将防卫装备使用控制在消除威胁的必要和合理范围内；

c) 专职守护、押运人员在执行任务时，只有在遭到死亡威胁或严重人身伤害且没有其他合理选择时，才能使用防暴枪支自卫或保护他人。

组织制定的防卫装备使用原则是运行范围和任务地点或条件的防卫装备使用依据。

C.7.3.3 防卫装备使用程序

防卫装备使用程序：

——遭受他人不法攻击或蓄意伤害时，可使用枪械和其他防卫装备于自卫、保卫特定人员（包括其他保安人员）或财产的情形宜形成文件；

——指导人员的防卫装备使用，确保防卫装备使用符合组织的防卫装备使用原则，同时也符合组织遵守的行为准则。

如可能，程序制定时宜与组织的保护对象商议，确保保护者与被保护者之间达成共识，同时推动防卫装备使用程序的落实。

C.7.3.4 专职守护、押运业务防卫装备的一般通用原则

防卫装备使用的具体限制条件因不同地区和不同运行环境而存在差异。但组织在制定防卫装备使用规程时宜考虑下列通用原则。

a) 在执行任务时，只有在极度必要且所有其他伤害较小的方法失败、可能失败或无法合理使用的情况下，专职守护押运人员才可以使用防暴枪支作为最后手段。在执行任务时，只有在遭受致命威胁、或在严重违法犯罪行为威胁生命或人身伤害的合理必要情况下，专职守护押运业务才能使用防暴枪支自卫或保卫他人。

b) 当威胁不构成死亡威胁或严重人身伤害时，可使用伤害程度较小的防卫装备，可选择方式众多，包括警告、防暴叉和保安棍器械等非杀伤性防卫装备使用。不论是否有意为之，任何防卫装备使用都有可能造成意外严重人身伤亡。非故意的杀伤性风险会随着装备复杂度和效果以及使用者、使用指令及防卫装备使用的培训和水平降低而不断增加。

c) 防卫装备使用原则旨在用合理防卫装备实现合法目的。组织的防卫装备使用程序宜按防卫装备使用实施原则进行说明。若情况允许，保安服务人员宜尝试使用最低限度的防卫装备或降低防卫装备使用的方式解决问题。尽管如此，处置突发情况和威胁时并不要求延迟使用防卫装备或逐级提高防卫装备使用。某些情况下，逐级增加或提升防卫装备的使用可能会增加所有当事人的风险。

组织的防卫装备使用程序并非法律文件。因此，组织或组织人员因防卫装备使用不当造成严重人身伤亡而遭到公诉时，该程序不能为组织或组织人员提供任何保护。但组织人员可通过程序证明在当时情境下，防卫装备使用程度和持续时间是合理的，并非不经思索作出的反应，而是出于对他人安全的考虑而实施的合乎程序的理性行为。

组织的防卫装备使用程序可能比适用法律的要求更为严格。在任何情况下，组织的防卫装备使用

程序都不宜限制法律赋予的正当防卫权利。

C.7.3.5 防卫装备使用授权

从事专职守护、押运的组织宜制定程序，确定需要配备防卫装备执行组织专职守护、押运任务的人员，以及这些人员可配备防卫装备的情形。防卫装备授权仅限于适用法律法规和合同条款规定的人员。专职守护、押运人员执行守押任务时，若违反适用或相关的法律法规，组织宜记录相关地区的尽职调查过程，以此评估该人员是否被取消防卫装备配备和使用资格。在专职守护、押运人员的背景调查结束之前不宜向其配发防卫装备。防卫装备授权程序宜限制未接受或未通过防卫装备使用特定培训和许可的人员配备防卫装备。

对于代表组织工作的授权配备防卫装备的所有人员，宜记录以下内容：

a) 配备防卫装备的授权证明；

b) 防卫装备的使用训练、资格证明及胜任能力等记录；

c) 防卫装备的发放和归还记录；

d) 防卫装备保养；

e) 防卫装备使用(培训外的防卫装备使用情况)。

组织宜为每个人员制定上述记录的保存和查阅记录的程序，记录留存期为该人员配备和使用防卫装备授权要求的记录留存时间和法律要求的留存时间。

C.7.3.6 防卫装备使用培训

宜向代表组织工作的人员传达防卫装备使用原则及程序内容，其详细程度宜适合受训对象。培训宜包括组织内部防卫装备使用程序和防卫装备使用原则的所有主要内容(根据受训人员等级和要执行的任务确定)。宜特别关注以下内容：

a) 特定保安服务任务中防卫装备使用的适用法律；

b) 专职守护、押运人员可配备枪支弹药的时间和地点；

c) 非执行任务时的枪支弹药储存；

d) 正当防卫和保卫他人的概念；

e) 什么是合理性和必要性；

f) 不符合防卫装备使用程序和防卫装备使用原则的后果；

g) 因防卫装备使用导致个人或组织可能面临的刑事和民事责任(包括作为或不作为的监督性职责，及执行监督命令或指示的人员宜承担的个人责任)。

培训宜包含对防卫装备使用的指导培训，如何在防卫装备使用原则内响应，并宜评估个人对防卫装备使用原则的理解。其目的是让受训人员理解且能够做到仅使用合理必要的防卫装备制止威胁，同时有效且足够保卫人员和财产免受攻击或其他暴力侵害。防卫装备使用的培训内容宜至少包括下列技巧。

a) 保安服务人员在场：存在性威慑。

b) 言语威慑：非肢体对抗；通过大声口头警告阻止威胁性行为。

c) 徒手控制：用肢体力量控制局面；用肢体约束、妨碍或扣留破坏者。

d) 防暴叉和保安棍：采用防暴叉和保安棍等防卫装备控制局面。

e) 专职守护押运人员使用防卫装备威慑：使用防暴枪支威慑并表明使用意图。

f) 专职守护押运人员防卫装备使用：使用防暴枪支控制局面。仅在必要时使用以消除威胁。宜针对目标使用，且适当考虑在场人员的安全。

防卫装备使用培训宜阐明：

a) 防卫装备使用原则；

b) 监督部门在控制防卫装备使用中的角色(包括授权和对防卫装备使用升级或降级指令的授权限制);

c) 组织的监督人员、受保护对象及执法部门在指导或限制防卫装备使用方面的角色和权限。

培训计划宜包括理论(课堂)培训、器械培训、实弹培训和情景模拟演练。宜向受训人员呈现其在执行保安服务任务过程中可能面对的类似情景。这些情景宜适合受训人员承担的任务,并要求其在更为复杂和模糊情境下做出判断和恰当反应。实弹培训只限定于得到许可的专职守护、押运工作相关。组织宜使用切合实际、可衡量的客观标准考核受训人员的熟练掌握程度。

C.7.4 关键资源

C.7.4.1 总则

保安服务管理体系的成功实施需要代表组织和为组织工作的所有人员共同恪守承诺。宜明确各人员的岗位、职责和权限,以确保保安服务管理体系的实施、防止分歧(尤其在发生非预期事件或干扰性事件期间)和避免任务疏漏。

此外,还宜明确与外部利益相关方协作时的岗位、职责和权限,形成文件并传达,其中宜包括与分包方、合伙人、供应方、公共机构和社会群体之间的相互关系。组织宜明确并传达所有参与保安服务的人员的职责和权限。最高管理者宜向人员提供保障其履行岗位和职责的资源。组织的工作背景变化时宜重新审核人员岗位、职责和权限。

发生非预期事件或干扰性事件时,需有合适的管理构架以有效处理事件。宜明确规定管理结构、决策权限和实施责任。组织宜成立"事件管理团队",在最高管理者或其代表的明确指示下指挥事件响应。团队职能包括:

a) 制定计划;

b) 事件响应与管理;

c) 人力资源管理;

d) 健康、安全与医疗措施;

e) 信息管理;

f) 安全;

g) 法律法规;

h) 沟通/媒体关系;

i) 其他重要支持性职能。

事件管理团队需要的工作组数量宜根据组织规模和类型、员工人数、地理位置等因素合理确定。团队宜制定响应计划以处置危害评估与管理、沟通、人力资源、信息技术与管理等各方面的潜在威胁。事件响应与管理计划宜符合并纳入保安服务管理体系。宜可根据技能、责任感和利益关联度招聘相关事件管理团队成员。

C.7.4.2 人员

C.7.4.2.1 总则

人员、人员能力与培训需求都是组织环境、其合同要求、风险评估及既定目标的输出。

组织宜根据劳动法和其他适用的法律法规为其工作人员建立薪酬和福利。

宜保护个人隐私和信息机密性。个人背景资料及工作信息是高度敏感内容。因此,组织应制定并保持相应程序,恰当并严格地保障内外部信息的机密性。组织宜安全保留相关文件,保留时间符合适用法律法规、合同及组织的存档要求。

所有人员的记录信息宜包括如下内容:

a) 姓名、现住地址、联系方式、身份证号码等信息；
b) 遭遇伤亡事故时需要的直系亲属及其他紧急联系人信息；
c) 法律法规及其他要求规定的信息。

C.7.4.2.2 人员筛选、背景审查

组织宜建立入职前背景审查程序，对组织员工进行入职前调查。组织宜建立相关程序并形成文件，通过实施和保持程序筛选出不符合最低岗位要求的人员，并根据知识、技术、能力及其他因素挑选合格人员。筛选程序符合合同要求及其他适用标准和原则。筛选和审查过程宜根据候选人员的计划入职的岗位性质、权限级别和专业范围确定。筛选宜在为候选人员提供岗位并开始工作之前进行。背景审查前，候选人员宜签订相应的授权书和同意书。录用决定宜综合候选人员的资质及背景审查结果而定。

筛选和审查过程宜尽可能包括如下内容：

a) 身份验证；
b) 个人经历审查；
c) 工作经验及资质；
d) 证书审核。

无法获得其有关信息、信息不可靠或不合适的事项宜形成文件。

身份验证宜包括审查个人经历的真实性及候选人员的最低年龄。个人经历宜包括但不仅限于下列各项：

a) 家庭住址；
b) 工作经历；
c) 教育经历；
d) 无犯罪记录；
e) 被处罚记录
f) 服役记录；
g) 机动车辆驾驶记录；
h) 信用报告。

审核候选人员的经验和资质时，组织宜寻找隐性差距，相关信息包括但不仅限于：

a) 教育背景；
b) 工作经历；
c) 许可/认证/注册信息；
d) 自我评价；
e) 主管及同事的面试信息；
f) 服役经历。

组织宜依据下列各项建立明确的员工筛选和审查标准：

a) 吸毒情况；
b) 身体和心理适应性；
c) 是否适合配备枪支(仅适用专职武装守护押运的组织)；
d) 在高压及不利条件下工作的能力。

宜保护个人信息和隐私。例如身份证、驾照等个人资料宜在合理时间内返还给本人。

C.7.4.2.3 分包方的筛选与背景调查

无论临时还是长期，组织宜只采用符合本文件的合格分包方提供的服务，组织承担分包方工作的责任。组织宜为其业务建立、保持明确的分包方筛选和背景调查准则并形成文件。宜根据适用法律法规

和与客户签订的合同要求与分包方签订书面协议并留存。

分包准则宜包括分包方能够：

a) 满足本文件的要求；

b) 依法合规开展各项活动；

c) 保护客户形象及信誉；

d) 提供充足的资源和专业技能，包括有能力的工作人员，以实现运营目标；

e) 保证任务执行过程中有透明度、能承担责任和可被适当监督；

f) 考虑其财务和经济义务(包括人员合理报酬和保险范围)；

g) 有必要的执照、许可或授权；

h) 维持最新的、准确的人员和财产记录；

i) 根据适用法律法规和合同义务配备、使用、存储枪支弹药(仅适用专职武装守护押运的组织)。

组织宜：

a) 保证与分包方或外包合作伙伴签订适当的书面协议；

b) 书面通知客户相关分包安排，并适时获得客户的批准；

c) 负责监督分包方针对本合同提供的人员培训，包括尊重合法权益和避免不利影响；

d) 确保分包方为其业务提供相应的保险保障；

e) 保存分包或外包工作的本文件符合性记录。

C.7.4.3 制服、标识和可追溯性

C.7.4.3.1 制服和标识

组织宜采用统一制服和装备标志表明保安服务队伍的身份及其与公司的从属关系，且采用的图案、颜色或标记宜不易与公共安全队伍(如军队和警察)相混淆。由组织选择或客户指定的制服和标志需要得到有关政府部门的批准。

从事武装守护押运服务的保安公司的标准化制服和有标识的车辆要向公众、警察、军队及其他机构明示保安服务团队成员是否有权携带和使用武器。制服宜含有区分组织工作人员工号、姓名的工牌或其他方式。车辆标记宜包括公司标识和特有编号。在发生不良或破坏性事件的情况下，制服和其他标志有助于公众做出正确判断，从而使得报告过程公开透明，降低了组织可能因另一个同区域组织的不当行为而受到指责的可能性。

制服能够反映组织的正面形象，鼓励公司员工的职业行为和责任行为。在发生冲突的情况下，可通过易辨识的制服和标记来区分保安服务人员、军事人员和其他人员。为保证有效性，制服描述、公司标识、工号和特有车辆标记信息宜可提供给政府部门、公众。

某些特定情况下，客户可能不希望保安服务人员被轻易识别。还有些情况下，风险评估表明如果武装保安随卫被识别，有可能增加暴力威胁和对客户、公众及保安服务人员的危害。此种情况，如存在更为慎重的且符合法律要求的方法时，保安服务人员可穿其他接近便服的功能性服装，但不能公开携带武器，且车辆与民用交通工具不能有明显不同之处。但即便在如此谨慎低调的场合中，保安服务人员仍需具有不可或缺的身份辨识特征。

C.7.4.3.2 标识和可追溯性

本条旨在确保组织利用标识和可追溯性，以便在整个保安服务提供过程中能够确定可能受到潜在不合格输出影响的服务。组织宜根据服务的性质，使用不同的方法标识输出。在选择标识方法时，组织宜考虑：

a) 为什么需要标识输出，如法律法规要求；

b) 在过程的哪个或哪些阶段进行标识以及如何标识。

进行标识和可追溯性的原因各不相同。

标识方法根据输出的性质而有所不同，例如：

——标识合同或订单的代码、名称或其组合；

——防卫装备本体上的部件编号、永久性标记或标签；

——表明提供服务的可视实物标牌；

——电子成文信息的文件命名系统。

当要求能够对输出进行追踪时，组织宜确保已标识的过程输出的相关成文信息得到保留并可获取。这在诸如调查过程和服务（如发生事故、事件或投诉）的不符合时，或当法律法规有要求时，可能非常必要。

C.7.5 职业健康与安全

组织宜提供安全健康的工作环境，识别当地环境可能存在的固有危险和限制。宜采取合理的预防措施，保护所有在高风险、高危环境中代表组织工作或其顾及的人员。

C.7.6 事件管理

C.7.6.1 总则

组织宜为非预期事件和干扰性事件建立预防、准备、缓解、响应、恢复和补救程序。宜根据管理部门批准的恢复目标成文程序，详细说明组织将如何管理干扰性事件，如何将活动恢复至或保持在预定水平。这些程序宜：

a) 基于风险评估中识别到的和优先考虑的风险；

b) 使用风险评估识别潜在非预期事件和干扰性事件的细节，包括预兆和预警；

c) 基于系统化完整过程下风险评估的输出结果控制风险；

d) 将避免、消除、缓解、扩散、转移和接受策略纳入考量，综合多个风险处置选项，提供最佳解决方案；

e) 包括通报有关部门和利益相关方的规定。

组织宜建立相关程序，帮助判断在面临重大风险时是否亟需采取一定的措施来避免、预防、缓解或响应潜在非预期事件。宜用强有力的侦测计划和防范方针支持该过程。

潜在干扰性事件一旦被确认，宜立即上报至指定主管部门、管理者或其他负责危机通报与管理的内部负责人和外部利益相关方。宜建立、成文并遵循具体的通报准则。

问题评估（确定待解决问题性质的评价性决策过程）和严重性评估（确定干扰性事件的严重程度及任何相关后果的过程）宜在非预期事件发生时进行。要考虑的因素包括问题的严重性、问题升级的可能性及问题状况对组织及利益相关方（如社会群体和客户）的潜在影响。

预防措施可包括主动与内外部利益相关方进行协调。组织文化、运行计划和管理目标宜鼓励个人感知有关预防、避免、威慑和侦测的自我责任。宜采用成本效益缓解策略预防或减轻潜在事件的后果。宜识别有助于缓解过程的各种资源。

宜围绕现实可能的“最坏情况”制定准备与响应计划，前提是响应范围恰好与实际危机相匹配。注意事项包括：

a) 准备与响应计划应以人为本；

b) 组织的人力资源管理方式将影响事件管理的成功与否；

c) 能否提前做出后勤决策将影响准备与响应计划的良好实施；

d) 宜考核现有的资金与保险政策。

C.7.6.2 事件监视、调查和报告

组织宜建立事件报告程序，记录事故、防卫装备使用升级事件、设备破坏、人身伤害、财产破坏、攻击行为、违法犯罪行为、交通事故，及涉及其他保安相关事件和客户另外要求报告的事件。组织宜建立内部调查程序，用于确定以下内容：

a) 事件发生的时间和地点；
b) 所有涉事人员的身份，包括住址和联系方式；
c) 持续性伤害/损害；
d) 引发事件的情况；
e) 组织应对事件时采取的措施；
f) 内外部人员伤亡原因；
g) 通报有关部门；
h) 识别事件的根本原因；
i) 采取的纠正及预防措施。

事件调查结束时，组织宜作出书面报告。报告宜包括上述内容，且宜向适当的利益相关方（如客户和司法部门）提供报告副本。事件报告中宜提供充分的信息，以评价对事件响应的充分性。

代表组织工作的人员宜了解事件报告的职责和机制，包括证据采集和保全。事件报告计划宜纳入组织的培训计划。

C.7.6.3 内外部投诉与申诉程序

组织宜建立投诉与申诉程序，由此，内外部利益相关方可在其认为存在不符合本文件的潜在或实际事项，或违反法律法规或侵害合法权益的情况下提出申诉。该程序宜声明组织或代表其工作的人员不可以反对他人提出申诉或配合申诉调查。

投诉与申诉程序不仅是记录申诉，还宜通过识别根本原因、提升责任落实、评价有效性准则和推动不断进步文化来解决争议。投诉或申诉一经证实，宜以最快的方式采取纠正和预防措施。

当启动投诉与申诉程序时，宜委派一名或多名人员协助调查并解决危害他人生命、权利、安全，或者不符合本文件或客户要求的行为。组织宜公布其采用的投诉和申诉程序，为投诉和申诉提供及时公正的解决。

程序宜包括但不限于：

a) 提交投诉或申诉的机制；
b) 提交人的信息要求，包括确凿信息的提交；
c) 提交调查和结果时间表；
d) 机密性及隐私要求；
e) 解决过程的分级步骤；
f) 内外调查程序；
g) 相关文件和记录的维护要求；
h) 纪律处分；
i) 投诉或申诉的解决步骤，包括防止再发生的措施；
j) 结果的成文和交流；
k) 通报有关部门；
l) 评价投诉与申诉程序的有效性。

C.7.6.4 举报政策

举报人是代表组织工作的人员，负责揭露不符合本文件或组织的法律义务和组织自愿承诺的活动和行为。举报人可在组织内外部（如监管部门、执法机构或问题涉及的社会群体）陈述指控。组织宜建立举报人政策，并与合适的利益相关方进行沟通。

C.7.7 保安服务质量检查

本条旨在确保保安服务提供，符合所有的适用要求。

当不能满足所策划的安排时，组织宜得到有关授权人员的批准；在某些情况下，可能要得到顾客的批准。组织宜对需要获得顾客批准的情况，考虑建立准则。在这种情况下，可应用对不合格输出的要求。

具备授权放行最终产品或服务的人员宜通过诸如其岗位说明或权限等级等方式做出适当规定，并可追溯。这可通过保留成文信息来实现，例如：

a) 给出授权人员的签名；

b) 对满足特定准则后自行放行产品的总体授权的详细说明。

C.8 绩效评价

C.8.1 监视、测量、分析和评价

C.8.1.1 总则

绩效评价包括对组织保安运营、法律合规性和合法权益保护工作的衡量、监视与评价。组织宜采用系统方法定期对其保安服务运行关键绩效指标进行衡量和监视。衡量标准可以确保实现组织方针、目标指标，并阐明需要改进的方面。

为监视和测量组织保安运营绩效，宜确定一组用于评价管理体系及其结果（包括其保安运营的影响）的绩效指标。直接影响风险评价和保安运营目标指标的绩效指标可以是定量的，也可以是定性的。绩效指标可以是管理指标、经营指标或经济指标。这些指标宜为识别成功案例和需要纠正或改进的方面提供有效信息。

保安服务管理体系宜提供确定指标，数据收集和数据分析的程序。宜制定评价标准，用于监视和测量保安服务管理体系的有效性，确定需要改进的方面，以提高预防潜在非预期事件和干扰性事件的能力。从这些信息中获取的知识可用于实施纠正和预防措施。关键的是那些组织需要考虑用于确定其如何管理重大风险、实现目标指标以及提高保安运营业绩的因素。

为确保获得有效结果，必要时宜按照可追溯到的国际或国家测量标准，定期或在使用前对测量设备进行校准或验证。如果没有此类标准，则记录用于校准的依据。

C.8.1.2 合规性评价

组织宜能够证明已对其识别的法律法规和合法权益符合性进行了评价，包括适用的行政许可和资质要求。

组织宜能够证明已对其签署的其他要求符合性进行了评价。

C.8.1.3 演练和测试

宜使用风险评价中识别的事件来设计演练和测试情景。演练和测试可以作为有效的培训手段，也可用于验证假设和风险评价结论。

演练可确保技术资源发挥预期作用，且代表组织工作的人员在其使用和操作过程中得到充分培训。

通过演练可以使代表组织工作的人员能有效履行义务，清楚地了解其角色，并能识别保安服务管理体系、计划及程序中需要改进的方面。通过演练可以暴露宜予以纠正的保安服务管理体系的不足之处。演练的承诺可以提高保安服务管理体系的可信度和权威性。

演练与测试的第一步宜设立目标和期望。其中的一个关键性目标就是确定某些预防措施和响应流程是否有效，以及如何改进。组织宜利用演练和记录的演练结果来确保保安服务管理体系(尤其是保安服务实施计划、团队和设施)的有效性和准备状态，以执行并验证保安运营功能。

演练与测试的好处包括：

a) 验证计划范围、假设和策略；

b) 考核并提高代表组织工作的人员的能力；

c) 能力测试(如呼入和呼出电话系统性能)；

d) 提高完成整个过程的效率并减少所需时间(如通过反复练习缩短响应时间)；

e) 认识并了解保安服务管理体系内外部利益相关方和他们的职责。

组织宜设计演练情景，用于评价保安服务运行计划。宜制定保安服务管理体系及其组成部分定期演练的计划和时间表。演练与测试宜切合实际，评价保安服务能力和保安服务管理能力，确保对涉及人员与财产的保护。宜根据组织的经验、资源和能力充分考虑演练的范围和细节。早期测试可包括清单、简单演练和保安服务管理体系的小单元。提高演练成熟度的示例可包括：

a) 定向：入门介绍、概述或教育会议；

b) 桌面：以叙述性格式呈现的实际或模拟演练；

c) 功能性：在受控环境下尽可能逼真地模拟某一场景进行排练预演或特殊演练；

d) 全规模：模拟真实生活中的实时场景进行实战演练。

演练参与人员可扮演几种不同的角色。所有参与人员宜在演练过程中了解其扮演的角色。演练宜涉及演练范围中规定的所有组织参与人员，可适当包括外部利益相关方。作为演练的一部分，评审宜按照计划进行，与所有参与人员讨论存在的问题及经验教训。这些信息宜被记录在正式的演练报告中，供最高管理者评审。宜更新计划和程序，及时实施纠正和预防措施。

宜根据需要对测试和演练的策划进行评定和更改。考虑到保安服务管理体系的变更、人员变动、实际事件和以往的演练结果，演练和测试宜为动态过程。从演练和测试，以及经历的实际事件中获得的经验教训宜被应用于未来的保安服务管理体系演练与测试计划中。

演练和测试结果宜保留文件化信息。

C.8.2 内部审核

组织有必要实施保安服务管理体系内部审核，以确保保安服务管理体系实现其目标、符合策划的安排，已规范实施和保持，并识别改进时机。保安服务管理体系内部审核宜按照策划的时间间隔进行，确定并为最高管理者提供有关保安服务管理体系适宜性和有效性的信息，同时为设定保安服务管理体系持续改进目标提供依据。

组织宜建立审核程序，指导意见宜符合 GB/T 19011—2021 的要求，用于指导审核的策划和实施，并确定实际计划目标所需的审核。该方案宜基于组织活动性质、风险评价、以往的审核结果和其他相关因素。

内部审核方案宜基于全部的保安服务管理体系范围，但每次审核无需覆盖体系全部。审核可分为若干部分进行，只要能够在组织规定的审核期限内按照审核计划覆盖组织所有单位、活动和系统单元以及整个保安服务管理体系。

保安服务管理体系内部审核结果可以报告的形式提交，并用于纠正或预防具体的不合格项，为管理评审的实施提供输入。

保安服务管理体系内部审核可由组织内部工作人员或组织选定的代表其工作的外部人员进行。但

不论在哪种情况下，负责审核的人员宜有能力完成审核工作，并能够做到客观公正。在较小的组织中，审核员的独立性可由免于承担被审核活动的责任的审核员证明。

注：如果组织希望将保安服务管理体系的审核与安全、恢复力或环境审核相结合，则需明确规定每个审核的目的和范围。第三方合格评定，由独立于组织的机构进行，为内外部利益相关方提供信心，表明其符合本文件的要求。认证的价值是由公正、有能力的外部评价所建立的公众信任度。

C.8.3 管理评审

最高管理者通过管理评审可对保安服务管理体系的持续适宜性、充分性及有效性进行评价。虽然不需要立刻对保安服务管理体系的所有要素进行评审，但管理评审宜涵盖整个保安服务管理体系，并且评审过程可能会需要一段时间。通过管理评审，最高管理者可处理保安服务管理体系关键要素是否需要变更的问题，其中包括：

a) 方针；
b) 资源配置；
c) 风险偏好和风险接受；
d) 目标和指标；
e) 保安运营战略。

最高管理部门宜制定相应计划对保安服务管理体系的执行和成果进行定期评审。当现行体系接受评审时，宜精心组织正式评审，妥善记录并合理安排时间。参与执行保安服务管理体系及其资源配置的人员也宜参与管理评审。除按计划定期进行管理体系评审之外，出现以下因素时也可启动评审，或者安排进已经计划的评审中。

a) 风险评定：组织每次完成风险评价后宜对保安服务管理体系进行评审。风险评价结果可用于确定保安服务管理体系是否持续足以解决组织面临的各项风险。
b) 行业政策、合同及社会环境：行业政策、合同及社会环境发生重大变化时宜启动保安服务管理体系评审。行业政策的总体趋势和最佳实践以及保安运营计划技术可用于基准测试。
c) 监管要求：根据新的监管要求进行保安服务管理体系评审。
d) 事件经验：出现非预期事件或干扰性事件后，无论是否已经启动预防、补救或应对计划，均宜进行评审。如已经启动过上述计划，评审宜考虑计划本身的历史记录、作用方式和启动原因等。如果计划未启动过，则评审宜调查计划未启动的原因以及不启动计划的决定是否合理。
e) 演练与测试结果：根据演练与测试结果，宜在必要时对保安服务管理体系进行修改。

保持和持续改进保安服务管理体系宜能够反映将影响保安服务管理体系的组织风险、活动及运行的变化。以下是可能会影响保安服务管理体系的程序、系统或过程示例：

a) 方针变化；
b) 危害与威胁变化；
c) 组织及其业务流程变化；
d) 风险评定中的假设条件变化；
e) 人员变化(员工和分包方)及其联系信息；
f) 分包方和供应链变化；
g) 工艺和技术变化；
h) 系统和应用软件变化；
i) 演练和测试经验教训；
j) 外部组织非预期事件和干扰性事件经验教训；
k) 在计划实际执行过程中发现的问题；
l) 外部环境变化(新客户需求、社会环境变化、社会群体关系等)；

m） 在计划评审中记录的和在风险评价中发现的其他因素。

C.9 改进

C.9.1 不合格及纠正措施

组织宜建立有效的程序，确保能够识别出各种与保安服务管理体系（计划和程序）相关的未满足要求、策划方法的不足、事故、未遂事件及薄弱环节等方面的不足，并能够及时沟通以防止事态进一步发展，识别并解决根本原因。该程序宜能够发现、分析并消除不合格的实际和潜在原因。

对发现的任何不合格，宜组织调查其根本原因，以便制定出相应的纠正措施计划，及时解决问题，从而减轻问题后果，进行必要的更改以纠正这种情况并恢复正常运行，并采取措施通过消除原因来防止问题再次发生。措施的性质和采取时机宜与不合格的规模、性质及其潜在后果相适应。

有时可能会发现有潜在的问题，但是不存在实际的不合格项。在这种情况下，宜按照类似方法采取预防措施。可从针对实际不合格项的纠正措施中推断出潜在问题，也可在内部审核、行业动态和事件分析、或演练与测试中发现潜在问题。意识到记录和沟通潜在问题或实际问题的重要性的人员也可将识别潜在的不合格作为日常职责的一部分。

建立处理实际和潜在不合格并持续采取纠正和预防措施的程序有助于确保保安服务管理体系的可靠性和有效性。程序宜对策划及采取纠正和预防措施有关的责任、权限和步骤作出规定。最高管理者宜确保已采取纠正和预防措施，并有系统的后续跟进来评价其有效性。

导致保安服务管理体系更改的纠正和预防措施宜形成文件，并启动体系变化相关风险的重新评价，以评价对计划、程序和培训需求的影响。更改宜传达给受影响的利益相关者。

组织宜采取措施消除保安服务管理体系实施和运行过程中产生不合格的原因，防止不合格再次发生。纠正措施程序文件宜对以下要求作出规定：

a） 识别不合格；

b） 确定不合格的原因；

c） 评价确保不合格不再发生所需实施的措施；

d） 确定和实施纠正措施；

e） 记录实施纠正措施的结果；

f） 评审已实施的纠正措施和措施结果。

C.9.2 预防措施

组织宜采取措施防止发生潜在的不合格。采取的预防措施宜与其潜在影响相适应。

预防措施程序文件宜对以下要求作出规定：

a） 识别潜在不合格及其原因；

b） 确定和实施所需的预防措施；

c） 记录实施预防措施的结果；

d） 评审已采取的预防措施；

e） 识别变化的风险并确保重点关注显著变化的风险；

f） 确保所有需要了解的人都已被告知已采取的不合格预防措施；

g） 根据风险评价结果确定预防措施的优先顺序。

附 录 D
（资料性）
总 则

D.1 概述

保安服务管理体系的目标是管理组织提供的保安服务，加强人类的安全，保护资产（有形和无形的），并遵守法律法规和尊重合法权益。对管理能力薄弱或法律法规因人为或自然因素遭到破坏的情况尤为重要。组织宜通过管理所有利益相关方（包括代表组织工作的人员、受影响的社区和客户等）的风险来开展业务，并实现客户目标。通过将法律法规、社会、文化环境方面的关切融入业务运作中，并与利益相关方进行互动，以制定适当的优先措施来保护托付给他们的人员和实物资产。目的是通过以下方式将干扰事件或非预期事件的可能性和后果降到最低：

——在可能的情况下采取预防措施；

——减缓事件的影响；

——在发生事件时有效地做出反应，维持既定的绩效水平；

——明确事件发生后的责任；

——采取措施防止复发。

保安服务管理体系将在组织中推动保安服务符合法律法规和尊重合法权益的文化。

通过开发、设计、记录、部署和评估适合于目标的保安服务管理体系，可以达到一致的绩效水平。本文件的第 4 章～第 10 章以及附录详细阐述了与执行和尊重合法权益有关的保安服务的管理制度的要素。在制定、实施和改进保安服务管理体系过程中，最高管理者/决策者宜采用以下一般原则。

组织宜将以下描述的所有原则融入保安服务管理体系的设计和实施中。目标是实现组织和客户目标，保护资产（有形的和无形的），同时确保人员安全，尊重合法权益。保安服务管理将取决于将这些原则融入组织管理框架的有效性，这将在组织的各级中推动与尊重人员合法权益相一致的保安业务的文化。这些原则的使用宜建立一种环境，在有关的组织各级中充分报告信息并将其作为决策和问责的基础。

D.2 关注结果

管理体系不仅是一套管理过程，还是获得预期效果的工具。保安服务管理体系用于实现保安业务目标，尊重合法权益、遵守合同和法律义务等。关键绩效指标是为了支持实现目标，通过测量持续监视和绩效改进来推动一种管理文化。保安服务管理体系的成果都能有效地管理与以下内容相关的风险：

——保安业务和管理；

——保护客户、资产和受保护的人；

——合法权益；

——受影响的社区；

——保安从业单位和人员的安全；

——声誉和信息。

D.3 领导力和愿景

最高管理者（负责决策和有权实施决策的人）为组织建立愿景、设定目标并提供方向。他们在组织内提倡一种所有权文化，即每个人都认为尊重合法权益和管理非预期事件和干扰性事件的风险是他们为实现组织目标所作的一部分贡献。最高管理者致力于促进保安业务文化的推广，同时遵守法律法规

和尊重合法权益，并在执行和保持本文件方面发挥有效的领导力。

D.4 管理

保证专业的保安服务被视为整体良好管理策略和企业责任的一部分。在遵守法律法规和尊重合法权益的同时开展保安服务是组织精神和价值观的一部分。在实现任务目标中保护人身安全是管理非预期事件和干扰性事件风险的首要考虑。

D.5 注重需求

评估和理解组织的资产、需求和期望对保安服务管理的成功至关重要。保安服务管理需要响应客户的需求和期望，同时考虑其他利益相关方的需求和期望，比如受影响的社区，他们主动或被动的支持对于组织和客户的成功是必要的。组织的目标与内外部利益相关方的需要和期望有关。在组织、客户和其他利益相关方（如受影响的社区）的需求之间，系统地管理利益相关方的关系。

D.6 组织全面风险管理策略

管理与尊重合法权益相一致的保安业务是组织全面风险管理策略的一部分。除非风险得到有效管理，否则组织就不能最大限度地利用机会降低风险。风险是不确定性对实现目标、强调人身安全以及保护资产（有形和无形的）的影响。风险管理过程要求对组织的内外部环境有清晰的了解，主动识别机会并减少风险。评估和理解组织可接受的风险水平对于组织预先制定有效的风险管理策略是非常重要的，这种策略能够在操作环境的风险水平范围内满足内外部利益相关方的需求和期望。

D.7 系统方法

保安服务管理体系需要采取多维的、相互作用的方法。识别、理解和管理相互关联的过程和要素有助于组织有效地控制风险。系统方法检查构成整个系统的元素之间的联系和相互作用。体系的组成部分最好能在相互关系的背景中被理解，而不是孤立的，并且需要被当作一个整体来对待。

D.8 适应性和灵活性

大多数组织，特别是那些从事或承包保安服务的组织，在内外部环境可能发生变化的情况下运作。组织需要进行持续的业务监视以识别变化并实施有效的控制策略。组织需要有适应能力，能够并愿意不断发展，不断适应变化的业务环境。保安服务管理体系宜被视为一个管理框架，而不是一系列活动。随着任务、预算、优先级和工作人员的不断变化，当特定的应用程序发生变化时，框架的结构将是可预测的。

D.9 管理不确定性

保安服务管理并不总是基于可预测的威胁和可量化的风险。从事或承包保安服务的组织通常在管理能力薄弱或环境在因人为或自然因素遭到破坏的情况下工作。需要进行估计和假设分析已知和未知威胁的可能性和后果，以及在变化的环境中组织和利益相关方的脆弱性。对非预期事件和干扰性事件风险的管理宜明确考虑不确定性、不确定性的性质以及如何处理这些不确定性。

D.10 文化和沟通

最高管理者有必要制定明确的战略、沟通、培训和意识方案，确保各级管理人员和雇员了解管理体系的目标。保安服务管理体系支持组织中的文化和感知变化，从而保护组织及其客户的形象和声誉。最高管理者需要充分理解和支持保安服务管理体系，并将其传达给所有代表其工作的人员，作为组织核心文化的一部分。

D.11 循证决策

评估管理业务和风险相关问题的保安服务，能驱动决策制定并决定将采取基于事实分析的行动——与经验和公认的行业最佳案例相平衡。保安服务管理体系增加了审核、挑战和改变意见和决定的能力，提高了解决问题的能力，增加了通过引用事实记录来证明过去决策有效性的能力，并确保数据和信息的准确、可靠和及时，并符合公司政策。

D.12 持续改进

管理人员通过监视、测量、审核和在持续改进周期内随后修改保安服务管理的过程、程序、能力和信息，来改进保安服务管理体系。定期开展正式的、记录在案的审核。审核的结果宜由最高管理者审议，并酌情采取措施。

附 录 E
（资料性）
差距分析

组织宜通过差距分析来确定其目前的位置，以管理潜在的风险情境。差距分析让组织能够将比较其实际绩效与实现其目标所需的潜在绩效。分析宜考虑组织的风险（包括潜在的影响）作为制定保安服务管理体系的基础。

差距分析宜涵盖以下 5 个关键方面：

a） 风险识别，包括与运营条件、紧急情况、事故以及潜在的非预期事件和干扰性事件相关的风险；

b） 合法权益风险分析，确定组织保安服务影响的严重程度，并识别改进的机会；

c） 确定组织适用的法律法规和其他要求；

d） 评估现有的风险管理做法和程序，包括与分包活动有关的程序；

e） 评估以前的紧急情况和事故，以及以前采取的预防和应对非预期事件和干扰性事件的措施。

在所有情况下，都宜考虑组织的业务和职能、与其利益相关方的关系以及潜在的干扰和紧急情况。根据活动的性质，进行差距分析的方法包括检查表、采访、直接检查和测量，或以前的审计审核结果。

附 录 F
（资料性）
管理的系统方法

管理的系统方法鼓励组织分析组织和利益相关方的需求，并确定有助于成功的过程。它为制定政策和目标、建立实现预期结果的程序、测量和监控目标和结果提供了基础。管理体系为持续改进提供了框架，增加安保服务的专业性的可能性，同时确保保护合法权益和基本自由。为组织及其客户提供了信心，组织能够履行合同、安全和法律义务，并尊重合法权益。

管理的系统方法宜考虑当地的政策、文化、行动或变化如何影响整个组织的状态及其环境。体系的组成部分最好能在相互关系的环境中被理解，而不是孤立的。因此，管理体系检查构成整个体系的元素之间的联系和相互作用。管理的系统方法系统地定义了取得预期结果所需的活动，并为管理关键活动建立明确的职责和责任。该管理体系文件提供了建立、执行、操作、监控、审核、维护和改进组织的保安服务管理体系的要求，以尊重合法权益。组织需识别和管理许多活动，以便有效地运作。任何允许将输入转换为输出的活动，即使用资源并被正式管理的活动，都可以被认为是一个过程。通常一个过程的输出直接构成下一个过程的输入。

本文件中提出的保安服务管理的系统方法鼓励使用者强调以下内容的重要性：

a) 了解组织的风险、安全和合法权益保护要求；
b) 确定符合合法权益、遵守合同和法律法规义务的保安服务的结果；
c) 制定方针和目标、过程、体系和文化来管理风险；
d) 执行运行控制以管理组织的风险和安全要求，并尊重合法权益；
e) 监视和评审保安服务管理体系的有效性和运行绩效；
f) 根据客观测量，开展持续改进。

本文件采用了戴明循环(PDCA)模式，用于构成保安服务过程。图 F.1 说明了保安服务管理体系如何将保安服务管理需求和利益相关方的期望作为输入，并通过必要的运行和过程产生符合这些要求和期望的保安服务和风险管理结果。图 F.1 还说明了在本文件中提出的过程中的联系。

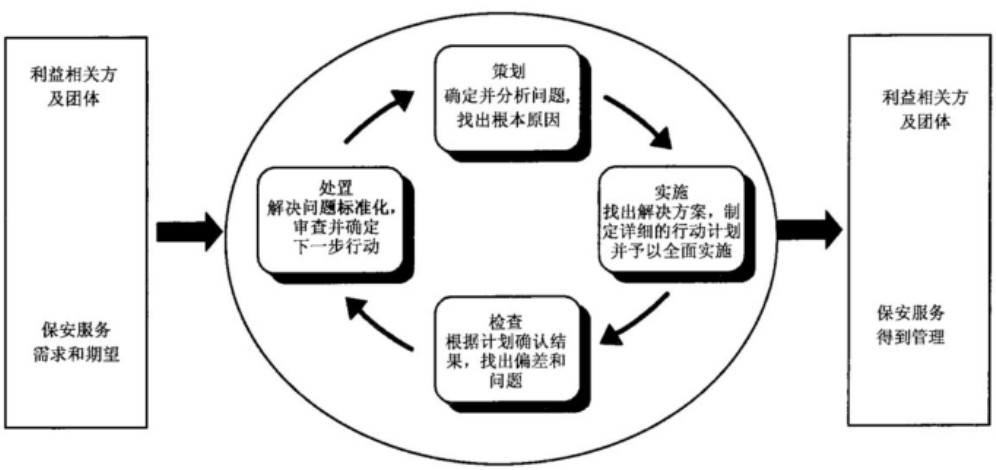


图 F.1 戴明循环模式

PDCA 模式简述如下。

——策划(建立管理体系):根据组织的整体方针和目标,建立管理体系的方针、目标、过程和程序,以管理运营和改进风险管理。

——实施(运行管理体系):运行管理体系的方针、控制、过程和程序。

——检查(监视和评审管理体系):根据管理体系方针、目标和实践,评估和测量过程绩效,并将结果报告给管理层进行评审。

——改进(保持和改进管理体系):根据管理体系的内部审核和管理评审的结果,采取纠正和预防措施,以持续改进管理体系。

PDCA 模式是一种清晰、系统且有记录的方法,可用于:

a) 制定可衡量的目标和目的;

b) 监视、测量和评估过程;

c) 识别、预防或纠正出现的问题;

d) 评估能力要求和培训;

e) 为最高管理者提供反馈回路,以评估过程,并对管理体系做出适当的变更。

此外,它有助于组织内部的信息管理,从而提高业务效率。

本文件是为了使 PDCA 模式能够与组织内的质量、安全、环境、信息安全、韧性、风险、安全及其他管理系统相结合。一个设计合理的管理体系可满足所有这些文件的要求。采用管理体系方法(例如根据 GB/T 19001、GB/T 24001、GB/T 22080、GB/T 45001 等)的组织可将其现有的管理体系作为本文件中规定的保安服务质量管理体系的基础。通过合格评定过程审核符合本文件,并与 GB/T 27021.1—2017 的方法相兼容并保持一致。

附 录 G
（资料性）
资质认证与适用性

系统地采用和实施一系列保安服务管理技术可为所有利益相关方和受影响的各方提供最佳结果。然而，采用本文件本身并不能保证获得最佳的保安服务结果。为了实现目标，保安服务管理体系宜在适当的和经济可行的情况下纳入最佳的实践和技术。这种实践和技术的成本效益宜被充分考虑在内。

本文件不制定超出组织方针承诺的保安服务绩效的绝对要求：

a） 遵守适用的法律法规要求和其他要求；

b） 支持非预期事件和干扰性事件的防御和风险最小化；

c） 推动持续改进。

本文件的主体包含可能被客观审计的通用文件。关于支持保安服务管理技术的指导意见包含在本文件的其他附录中。

如果组织愿意，可通过外部或内部的审计过程认证保安服务管理体系对本文件的遵守情况。可通过认可的第一方、第二方或第三方机构进行认证。

组织可调整其现有的管理体系，以建立符合本文件的保安服务管理体系。然而，管理体系中各种要素的应用可能会因预期目的和利益相关方的不同而有所不同。

保安服务质量管理体系的详细程度和复杂性、文件记录的程度和所投入的资源将取决于若干因素，例如体系的范围、组织的规模和其活动、产品、服务和供应链的性质。尤其针对中小型企业。

本文件为保安服务管理方案提供了一套通用的标准。本文件中使用的术语强调概念的共通性，同时承认在不同学科中术语用法的细微差别。与 GB/T 24353—2009 的一致，风险评估是风险识别、分析和评价的过程。

参 考 文 献

[1] GB/T 19001—2016 质量管理体系 要求
[2] GB/T 19010—2021 质量管理 顾客满意 组织行为规范指南
[3] GB/T 19011—2021 管理体系审核指南
[4] GB/T 22080—2016 信息技术 安全技术 信息安全管理体系 要求
[5] GB/T 24001—2016 环境管理体系 要求及使用指南
[6] GB/T 24353—2009 风险管理 原则与实施指南
[7] GB/T 27021.1—2017 合格评定 管理体系审核认证机构要求 第1部分:要求
[8] GB/T 45001—2020 职业健康安全管理体系 要求及使用指南
[9] GA/T 594—2006 保安服务操作规程与质量控制
[10] GA/T 1279—2015 保安员装备配备与管理要求
[11] 专职守护押运人员枪支使用管理条例(中华人民共和国国务院令第356号)
[12] 保安服务条例(中华人民共和国国务院令第564号)