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《保安业务管理体系　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、北京华远测评国际认证有限公司、方圆标志认证集团江苏有限公司、苏州恒东员物业管理有限公司、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、吴笑朗、管旭晖、刘旺、秦智鑫、王晓、陶中河、吴杰、胡庆、胡永明、曹春华、刘立生、郭立志、许磊、王峰、朱伟、毛朝南、李军、姜茂鸿、张蕾、朱毅云、杜群雄、刘守道、张素祥、王建峰、张宇、孔肖雷、刘福强、唐庆华、王亚飞、许敏宜。

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)　证实能够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(3.38)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描述)、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)，或可以是多体系审核(包括两个或两个以上专业)。

注2：组织(3.38)自身可进行内部审核，或请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

由其管理层或计划委托一个组织(3.23)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订包的情况。

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(3.31)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(3.211)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风险管理的存在、性质、形式、可能性(3.50)、严重性、评价、可接受性和应对或其他事方面。

注2：咨询是组织与其利益相关者及其他方为作出对某一问题做出决策或确定方向而针对该问题进行的有限沟通过程，不同于：

——通过影响力而不是通过权力来影响决策的过程；

——可获得的输入，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(3.31)、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：后果可以是定性或定量表述。

注4：一个事件引发一连串伴随后果的结果可能通过累积效应升级。

注5：后果也影响到等级或严重程度进行计值。

[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(3.61)人群，非预期事件(3.73)或非预想危害(3.42)对组织实现预期的影响性，系统识别和评估信息(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，且该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(3.62)。

3.15

干扰性事件 disruptive event

预所规划的活动，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(3.25)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(3.62)；

——为使组织运行产生的信息(一组文件)；

——结果实现的证据[记录(3.45)]。

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(3.42)方案，指挥团队成员和人员角色，测试组织(3.31)系统(如技术，设备规程，管理等)以证明保安业务管理能力(3.5)的活动。

注：演练包括培训相关组织工作人员的活动，以确定组织实现最高绩效(3.20)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(3.58)和后果(3.10)不可能完全已知。

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"(3.59)。

[来源：GB/T 23694—2013，4.2.1.3，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(3.24)的合法权益和基本自由产生不利影响的情景(3.60)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，将会造成生命威胁或严重人身伤害的物品。

示例：枪支、弹药、炸药、核辐射物质、生物制剂和毒素，感染或放射性物质等。

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(3.141)。

注 1：标准者可以是利益相关方。

注 2：受影响的社会群体和当地居民都视为价值利益相关方。

注 3：本文件中对条文"利益相关方"的使用应与保安服务(3.81)保持一致。

3.24

关键绩效指标 key performance indicator;KPI

组织(3.55)为完成其战略和服务目标(3.42)而采用量或比较绩效(3.45)的可量化数值。

3.25

防卫装备 defense equipment

依据国家有关规定，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

事件事发生的机会。

注 1：无论是以客观的或主观的、定性或定量的方式来评定、度量或确定，或是用一般词汇或数学术语来描述(如概率，或一定时间内的概率)，在风险管理术语中，"可能性"一词都与事件发生的机会。

注 2："可能性"(likelihood)在一些语言中没有直接与之对应的词汇，而此概念常用"概率"(probability)这个词代替。然而，在英语中，"概率"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常规的"概率"一词相同的解释，而不局限于英语中"概率"一词的狭义。

[来源：GB/T 23694—2013，4.6.1.1]

3.27

管理计划 management plan

具有明确规定所记录的行动计划，通常包含执行事件(3.133)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(3.55)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(3.103)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(3.76)采取以下方式实施：

——规定人员岗位、职责、权力等级和职能结构；

——实现依目标和指标的系统过程和相关管理(3.87)；

——针对绩效目标和指标按照下列要求进行评定和测量(3.29)和评价方法等，结果的反馈将作为改进体系计划；

——确保风险等级的正、或成有机会获得确认和实施附件等(3.48)应用。

3.29

质量 assessment

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(3.31)]。

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条件一致，以实现特定的结果。

3.33

组织 organization

为实现目标(3.42)，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、慈善机构或种研机构，或前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(3.20)包括外包功能或过程(3.42)，但不包括供应组织。

3.35

绩效 performance

可测量的结果。

注1：绩效可能表现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)的意图和方向。

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(3.46)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(3.38)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(3.30)或利益相关方(3.23)的惯例或一般做法，所考虑的需求或期望是不言而喻的。

注2：规定要求通常明示的方法，如，在成文信息(3.14)中做明示。

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：剩余风险也被称为"留存的风险"。

[来源：GB/T 23694—2013，4.5.1.4]

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—2013，4.5.1.7]

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(3.37)的活动。

3.49

风险 risk

不确定性对目标(3.32)的影响。

注1：影响总是临界限制，可以是正面的和/或负面的。

注2：不确定性是对事件(3.45)及其后果(3.13)或可能性(3.58)等信息缺乏理解或了解的状态。

注3：通常以参考"事件"(GB/T 23694—2013,3.5.1)和"后果"(GB/T 23694—2013,3.5.1.3)或两者的组合来描述风险。

注4：通常对事件(包括情形的变化)的后果和事件发生的相关"可能性"(GB/T 23694—2013,3.6.1.1)的组合表示风险。

注5：目标可以有不同方面(如会计目标、安全管理、遵守法律、财务、健康和安全、环境等)，也可以按照在不同层面(例如战略、组织范围、项目、产品和过程(3.10))。

注6：风险可分为纯粹、及意外自然损的来源。

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(3.80)，也可以在风险应对过程(3.42)中发生。

注2：接受的风险需受到监视(3.28)和评审(3.18)。

[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(3.53)和风险应对(3.80)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(3.36)、风险分析(3.51)和风险评价(3.53)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—2013，4.4.1.3]

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(3.80)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(3.10)及其原因和潜在后果(3.11)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(3.5)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—2013,4.1]

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、分析和评估过的所有风险的汇总，包含可能性(3.36)、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)、法律和监管、组织规章制度(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(3.36)；

——改变后果(3.10)；

——与其他各方分担风险(包括合同和风险融资)；

——慎重考虑的决定保留风险。

注2：针对负面后果的风险应对有时称“风险减轻”“风险消除”“风险预防”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internal人员从事的本单位门卫、巡逻、守护等安全防范工作；以及物业服务企业受用人单位委托为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性管理一般应包括建立方针(3.37)、集结(3.35)的目标(3.33)、指导运行过程(3.62)和持续改进(3.41)。

3.63

保安服务目标 security operation objective

保安服务管理(3.62)的结构。

注1：保安服务目标通常根据组织(3.34)的保安服务方针(3.64)制定。

注2：保安服务目标通常在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(3.34)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

使高管理者(3.72)支持的持续运行的管理和合理过程(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(3.45)直接或间接从事保安服务(3.61)的人员。

注：根据GA/T 1279—2015的规定，保安员特指依法取得保安员证，为企业、个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：同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：组织的子公司可被视为分包组织(4.33)。

3.69

供应链 supply chain

组织(3.34)、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、内部配送中心、分销商、批发商及其他供应运营管理职责的实体。

3.70

指标 target

为实现目标(3.42)而制定的适用于组织(3.34)的详细(或部分)绩效(3.30)要求(3.44)。

3.71

威胁分析 threat analysis

对可能危害人身、资产(3.11)、体系或组织(3.34)、环境或社会群体(3.7)的非预期事件(3.75)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(3.34)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(3.12)的权力。

注2：如果管理体系(3.25)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供审者。

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) 标准、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（包括服务区域内当地社会团体）；

h) 业务能力及组织绩效。

4.1.4 供应商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，以及是否可能对风险管理产生影响，并有可能引发应对预案或卡线处置的分包方，组织的整体保安服务管理方案中应包括识别有能引起重大预期事件或下游在事件的重大风险的供应链风险要素。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角色。

4.1.5 确定风险准则

组织应确定并持续评价风险准则。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) 业务活动、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从内在的不确定性；

c) 与重要事件、干扰性事件相关的潜在影响；

d) 适用法规要求及组织承诺的其他要求（如合同义务、合法权益）；

e) 组织的保险风险管理方针；

f) 对资产、业务造成威胁和后果的性质与类型；

g) 风险可能性、后果及需要权衡的方式；

h) 对相关方的需求和所受影响——尤其是人身、安全和合法权益（见下G.1.2）；

i) 信誉风险和恐怖风险；

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。

应对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，应持续或按相应评审其适宜性。

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。

为了履行合同与相关风险降到最低、最高管理者应识别、评价并记录的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（如地方社会团体、客户及其他保安从业单位）的相互影响；

f) 服务交付和合格供方变化记录要求。

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、或其一个或多个明确和评审的职能部门）。组织应考虑环境、性质、复杂性和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应予处理的风险和机遇。

组织应形成文件并可追溯。组织应确定适用信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。

适用性说明应按照风险评估和合法权益影响分析（见 6.1.1）定义适用于组织的应用，法律法规符合义务以及运行环境的附录 A 的相关参数。这些参数一经确定，组织应予以处置和执行。具体的免责条款和其说明应有记录。

4.4 信安服务管理体系

组织应按照本文件要求，建立、实施、保持并持续改进信安服务管理体系，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非价值和活动进行外包或参与时，应确保在信安服务管理体系中对这些外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信安服务管理体系并持续改进其与信息方面的领导作用及承诺：

——确保制定信安服务的方针和目标，并与组织的战略方向相一致；

——确保将信安服务管理体系要求融入组织的业务运行过程；

——确保信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、保持和改进信安服务管理体系；

——沟通有效开展信安服务管理并符合信安服务管理体系及此项应履要求的重要性进行沟通；

——确保信安服务管理体系实现预期结果；

——指导并支持员工对信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信安服务管理体系进行管理评审。

最高管理者应通过应用其信安服务管理体系的建立和执行，以及践行个人诚信安服务与尊重合法私益相结合为组织使命和其文化的组成部分，从而为在信安服务管理体系所起的积极预防作用提供证实。

5.1.2 符合性声明

最高管理者应制定符合性公开声明声公开发布，表明组织承诺并遵守信安服务管理体系和相关法律应履规定的责任，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) 传达到组织内外影响利益相关方，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，

——包括满足适用的处理及其他要求的承诺，在防范犯罪的自愿承诺，

——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意图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，

——可获取并根据成文信息，

——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4.1.3和4.1.5所描述的因素和要求，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，

c) 识别与保安服务相关的法律法规、合同、共同及其他要求和承诺；

d) 识别法律法规及规定以外与其业务和保安服务相关的合法权益责任；

e) 确定如何将上述要求应用于组织的运营中，以及分级、外包的保安服务业务。

组织应记录上述信息并持续更新，应将相关信息和相关方沟通有关法律法规和其他要求。组织和其客户将在签订上述评估表和维护要求的义务。

6.1.3 风险评估

组织应当建立保安服务管理体系，应当考虑到的组织内部和外部环境以及相关的法律法规，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、资产和现有控制措施，组织识别商人为和自然事件可能引起组织业务流程和组织的损失，资产、业务、职能影响和相关方故障，以及知识管理风险；

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、合作方、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估和优先级排序，以便实施对组织之前风险偏好可接受的水平的；

组织应：

a) 记录、保持更新上述信息，并确保信息的安全；

b) 实施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) 在组织内部和组织的运营环境、流程、职能、服务、合作关系和供应链发生变化时，重新进行风险评估；

d) 评价风险管理和缓解可靠性，所发生的直接和间接的收益与成本；

e) 确定现有的习管理风险应对方案的实际有效性；

f) 确保在将主、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，确定应包括：

a) 形成包含风险应对方法的风险优先级排序记录；

b) 风险接受过程准则；

c) 关键控制点（CCP）的识别；

d) 外包和外包方控制要求。

组织应建立与保安服务一致的监视、评估、评价和应对风险管理变化的过程。

组织应确定：

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，组织应与内部和相关相关方建立、实施和保持文件化的沟通和协调过程，以确保：

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

b) 风险被充分识别和传播；

c) 明确内部和利益相关方的利益；

d) 风险和风险应对方法已与合适的利益相关方沟通；

e) 明确与外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流程可对接；

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。

8.2 保安服务目标及实现策划

8.2.1 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；

——所需什么资源；

——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、利用于软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沟通、为组织的指标完成、产品和服务交付、职能运作和关键作用的分包方和供应链建立内部和外部控制。

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) 基于质量成本视角保障合法权益；

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量值和/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等三方，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。

8.2.2 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。组织应确定、实施和保持文件化的风险应对过程，考虑以下因素：

a) 降低潜在风险重要性；

b) 减少和降低某个事件及其后果发生的可能性；
c) 消除、降低或减缓改善性后果；
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) 规避或暂停产生风险的活动。

最高管理者应：

a) 评估用以消除、减少或控制风险的各方案的收益和成本；
b) 评价其接受服务方案，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、必施、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。

可利用资源应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) 明确其服务管理体系范围内的任一合资企业或合伙人关系的实体。

7.1.2.3 保险

组织应证明其有保险（能承担业务和活动）与其风险评估一致）引起的风险和相关责任。组织应确保组织已充分处理或购买了其外包或分包服务、运行或职能活动。

7.1.2.4 分包和分类

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、沟通和监督行为准则特定条款中就服务和事项合法权益方面对分包方和外包执行规定的要求。

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的同样认可且在本文件中所述的法律法规、道德以及合规性层的承诺与

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防和应对中提供有效的保安和风险管理。程序应：

a) 确保可以加强财政决策的制定；

b) 遵循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获得认可和合同义务一致，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于列各方面都要具备相适应的能力水平：

a) 保安职能的履行；

b) 风险评价；

c) 管理风险评估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、知识和宗教等；

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，包括适当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) 通过培训的处理志，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所需和定制在岗的理论、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，为使用防卫装备携带反复消耗和提高培训效果，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、记录和响应内外部利益相关方的沟通；

c) 定义并确保在紧急事况或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有效测试。

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、运行和问题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。还应包括向政府、其他保安团队和紧急医疗支持请求互助援助的程序。

组织应确保所有层级的人员熟悉接受和理解以未成当前形式的沟通，并且应有使用特定的沟通渠道或方式予以回应，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

根据法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。若决定向外部传递，应建立和实施一套或多套方案，用于外部沟通（包括警告、预警和通报媒体等）。

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，并尽可能确保语言、教育水平或对客户报复及考虑保密性和隐私等引起的访问障碍。

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、角色说明、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策划、运行和控制所必需的成文信息。

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、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、软件版本、图表）和载体（如纸质品、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) 人员简历；
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缴；
p) 管理体系会议记录；
q) 保安、保安服务和合法权益维护信息；
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) 随时更新和获取的文件；
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，以保护记录的可追溯性、检索性和完整性，包括识别、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。根据服务记录应至少保留3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、目标和绩标的活动，以确保这些活动在规定的情况下进行，策划并管理：

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导；

c) 遵守相关的法律法规以及本文件规定的其他义务；

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，以尽量降低下发生事件或非预期事件发生时可能带来的后果；

g) 实现其保安服务运行目标和指标。

组织应建立、实施和保持支持化程序，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，必要时应采取措施减轻任何不利影响。

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) 关事重大时，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，包括对交服务的要求；
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、实施及记录的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) 确定保安服务的持续、持续时间和复杂程度；
c) 确认客户的需求和期望及组成保安型考核团的要求；
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验证进行评审；
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) 确定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) 确认客户的需求并制定；
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，评审活动可以单独进行或合并进行。

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) 能应实施方案计进行评价；
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问题施的保护，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；

e) 其他应考虑环境的特定问题。

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) 为过程的运行应用适宜的基础设施，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) 采取措施防止人为差错事件不应有发生；

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，以尊重所有人员的财产和合法权益，并避免任何不合格情况。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 非预期事件应对处理事件的预防与管理

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

a) 保安职责的履行；

b) 保护生命、组织机构内外部利益相关方人员的安全；

c) 尊重生命和人的尊严；

d) 需要考虑对非预期事件的预测和预防；

e) 应对非预期事件，启动上报升级；

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（包括临时、合同方和外部分包代理）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受适当重视的权益。该道德准则应确保所有代表组织工作人员理解其职业和社会责任和维护合法权益的责任。

组织应向所有代表其工作的人员和客户传达该道德准则，并提供相关信息。

8.3 防卫装备使用

8.3.1 总则

组织应建立并形成支持的程序，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服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完成勤务所必需的，为保护自己和他人免受伤害而配备的非致命装备，如警用防卫装备及执行武装守护、押运任务配备的防弹衣等。

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) 防暴盾使用；

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) 如形势和环境允许，警告相应人员并给其留出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管制，以及监督控制授权的撤销。

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后，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) 法律应规定予以正当防卫权利；

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，授权应仅给予被组织确定适合执行任务、且经管理毕业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相关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至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。组织应保留涉及关系所属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求：

a) 适用于特定保安服务中应当配备的装备；

b) 从事武装守护押运保安服务以及特殊保安服务时应当配备的装备；

c) 对使用警卫警犬等人员死亡或严重伤害到应承担责任的责任；

d) 对合理确定使用防卫装备的指令明确清晰，以避免上级指令为滥用防护应用无效；

e) 防卫装备使用前培训。

组织应开发员工可随身携带的培训资料，以概括其员工职责、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

服务管理者应提供建立、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、管理下属和人力资源（包括具有专业技能和知识的人员）及财务支持、基础设施、记录和符合指南、预算和权限。以保证有效的保安服务管理，包括具有承接业务控制、协调及监督责任。

为有效地处理未预期条件或干扰性事件，组织应设立具有资格的位置，适当期限和充足资源（包括安全有效的设备和资源）的作业计划及指挥（协调员、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）来履行合约义务。应向人员提供适当的培训和资源，包括保密、组织应根据具体情况保护上述信息的机密性，并以协议要求经授权提供相关文件。

组织应当给有人员保持或文档备：

a) 能够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) 处于在事故发生时的个人医疗；

d) 向于重要家属具伤亡信息。

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审核或或文信息，以使可代表其工作的每个人员进行背景审查，确保组织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）。在确定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) 执照、从警经历和相关服务从业记录审查；

e) 无犯罪记录的评审；

f) 无吸毒和药物滥用评审；

g) 特定活动进行体能和心理健康的适合性评价；

h) 要求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，符合程序或本文件条款的个人承诺书，有无犯罪或发生变化时及时报告机制。

组织应确定适当的程序，以确保背景审查所涉及或被确定为在各内外部组织过程中予以处理，并根据确定对象保存记录。

应按照岗位管理要求的能力（包括知识、技能、服务和资质）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，明确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详细记录。

8.4.3 制服、标识和可追溯性

为确保客户、公众安全要求得到，履行合同或适当法律法规要求而能识别其人员和交通工具的服务标识，该标识在一定距离内可见，并区别于那些和警察所用的标识。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。组织在在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，以合理的预防措施，提供安全、健康的工作环境，以预防与风险源及生产作业的人员，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) 提供环境和培；

c) 提供个人防护及其他适当的保安设备；

d) 医疗和心理健康监护培训，治疗和支持；

e) 识别和处置工作场所暴力、胁迫、欺诈、骚扰等不当行为的指导方针。

8.6 事件管理

8.6.1 原则

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、合法权益及资源的非预期事件和干扰性事件，明确如何对其做预防、缓解和应对上述事件，考虑以下原则：

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) 防止下级控事件的进一步升级；

d) 尽量减少并适行的干扰；

e) 通报有关部门；

f) 保护（按照相关客户的）指定财产；

g) 对正常活动的破坏。

8.6.2 事件处理、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、敏感信息或装备的损失、超物质用等不合规情形的，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。

应将每个合格项和事件的记录并保留以定时收集等。

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。该程序应考虑内外部利益相关方，以便于个人报告在组织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) 防止举证人或证明收集证据；

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及时反映。

组织应确定：

——[illegible]需要监视和测量什么；

——需要[illegible]什么方法进行监视、测量、分析和评价，以确保结果有效；

——[illegible]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。

组织应保留实施评价的成文信息，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最关键特征[包括软件关系，涉及合同和供应链关系]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和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)维护系统、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规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兼顾风险评估和风险管理程序确定能力测试中发现的问题，以识别潜在的问题或薄弱环节，演练内容和执行方式不应影响运行，且应考虑人员、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，或在新的指标、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的信息，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、合同执行和分包商报表。

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，以确定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) 是否有效改进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，以确保其持续适宜性、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) 风险管理准则和机制。

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) 监视和测试的结果；

f) 以往风险评估中未充分解决的风险；

g) 审计报告；

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 管理输出

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化有关的决策和措施，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) 对不合格做出反应，并在适用时，
——采取管理控制和纠正不合格；
——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而防产生不合格的原因，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，管在避免不合格发生，
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变改。
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，以确保对影响组织组织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当明确需要批准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。

应维持已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
3.62、3.63—、3.75	3.63、3.64—、3.75
—	3.76
3.76	3.77
5.1.2	5.1.1 自第二段至结束
5.1.4	5.1.3
5.1.2	—
5.1.3	—
5.1.4	5.1.2
5.1.5	5.1.3
5.1.6	5.1.4
5.3.2	5.3.3、5.3.4、5.3.5 合并调整
5.3.3	5.3.2
—	5.3.6
5.3.6	5.3.7
—	5.4
—	5.5
5.4	5.6
5.4.1	5.6.1
5.4.2	5.6.2
5.4.2.1、5.4.2.2、5.4.2.3	5.6.2.1、5.6.2.2、5.6.2.3
—	5.6.3
5.4.3	5.6.4
5.5	5.7
5.6	5.8
5.6.1、5.6.2、5.6.3	5.8.1、5.8.2、5.8.3

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 第四段至末
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 18788:2015 的技术差异及其原因的一览表。

表 B.1 本文件与 ISO 18788:2015 的技术差异及其原因

本文件的结构编号	技术差异	原因
1	删除了 ISO 18788 中关于采购标准的适用范围	既符合从国际角度表达，我国不适用于法律表述
2	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"人权影响评估"(HRIA)	适应我国管理
4.4.1	更改"市场竞争"为"同业竞争"	符合我国相关法律及行业现状
4.4.2	更改"私营安保研究"为"保安从业单位"	适应我国行业现状
5.4.1	更改"安保业务"为"保安服务"，并确定其内容	符合我国相关法律及行业现状
8	删除了 ISO 18788 中 8.4.5"安保"	3.41 定义中已包含相关含义
	删除了 ISO 18788 中 8.10"武力使用原则"	符合我国相关法律及行业现状
9.2.3	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《联合国文件(09/2008)》(16.1.1、8.8.1 等原则的处理)； ——删除了《私营安保服务提供国际行为守则(ICoC)》(11.2018)； ——删除了《汇报准则与人权合法权益(金融稳定理事会)"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
9.3.3	将 ISO/DIS 18788 第 8.3.3 条款中关于风险评估的内容更改为 8.3.3 风险评估	单独成一节进行规定合理
9.3.4.4	将 ISO 18788 中"受雇人员"更改为"受雇企业职员"，并全文做相应处理	适应我国管理
9.3.5	删除了 ISO 18788 中"在遵守适用的联合和国际法律、标准情况下，人权适用国际法	适应我国管理
9.5	增加了"——相关的保险服务目标"	保持内容的完整性
9.6.1	删除了 ISO 18788 的 9.6 中遵守国际人权和管理合法管理设，修改为遵守相关国际法律法规	符合我国相关法律法规
9.6.2	删除了 9.6.2 保险服务的要求	综合我国行业现状，增加相关内容
9.6.3	增加了 9.6.3 保险服务的设计和开发	综合我国行业现状，增加相关内容

表 B.1　本文件与 ISO 18759:2005 的技术差异及其原因（续）

本文件结构编号	技术差异	原因
5.1.4	增加了“组织所提供的保密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密服务的提供准则应的受控条件	适应国内保密服务的需要，更具有可操作性
5.3	删除“或为”改为“防卫装备”	适应我国国情
5.5.1	增加了我国有关保密服务范围的相关说明	适应我国国情
5.5.2	将 ISO 18759 中 5.5.1 武力使用预案、5.5.4 录像命方、5.5.5 指命方合并整改为 5.5.2 防卫装备使用预案	适应我国国情
5.5.3	将 ISO 18759 中 5.5.3 武器装收重改为防卫装备授权	适应我国国情
5	删除了 ISO 18759 中 5.5.6 使用武力风险的承诺	适应我国国情
	删除了 ISO 18759 中 5.6 调查和遵循	适应我国国情
	删除了 ISO 18759 中 5.5 文援执后的业务	适应我国国情
	删除了 ISO 18759 中 6.6.1 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，保密标准中涉及的相关内容不宜细广
5.4	标题改为“人财物资”	内容中未提到人下岗位，附录规定的具体要求
6.4.2.2	删除了 ISO 18759 中“根据法律应视和根据客户要求，进定最小年龄，然而在任何情况下，存利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
6.4.3	删除了 ISO 18759 中“以及建立确定和论文培训标准与本基础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，保障内容的完整性
8.7	增加了 8.7 保安服务质量检查	增加国内保安服务的要求，更具有可操作性
8.1.4	增加了 8.1.4“客户满意”	保障内容的完整性，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的内容旨在帮助组织理解和支持此要求，组织在执行本条款时，还需根据自身风险评估及客户合同和法律法规要求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了审核的依据，以证明其有能力满足相关要求，与此小组的不当、非法及过度行为的发生。

对于从事及承担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处置，组织应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。这就需要确定一个持续、动态及基础的管理过程，以保证建立并维护合适的控制，还要让规和基本目标的文化氛围，同时为客户提供一个本质的服务，助其完成预期。

从事或承担保安服务的组织及其客户在义务等级内外和对影响其方的生命及企业权益，通过使用本文件，组织可以更好地理解其所面临的风险，并能更加灵活对策，以便：

a) 对其所维护的合约客户遭受的生命及财产风险进行管理；

b) 证明其履行等级合法权益，法律法规和承诺及义务；

c) 降低风险对支持业务和运行；

d) 通过组织维护其在与其客户及利益相关方间建的战略及行动计划来对影响事件作予以积极事件进行有效管理。

针对潜在影响事件和一致性事件回顾以及预先规划响应各项措施并及时检讨能性及其影响。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。

本附录为组织建立了管理框架，以改善识别和评估实施以下活动的最佳实践方法：

a) 降低其运行和供应链（包括分包方）的风险；

b) 保障客户权益，遵守法律法规要求和合同，确定管理方针和目标；

c) 鉴定和评估对其业务能否长期成功至关重要的风险；

d) 降低各种危害对组织和环境造成的影响；

e) 理解、遵循并进行关于遵守法律法规和客户合同义务的培训；

f) 增加业务维护资产和进一步完成任务为目标而实施的作用及重视的证据；

g) 管理事故响应措施及预案；

h) 开发、测试及维护事故预防和响应计划以及相关的运行程序；

i) 开展培训和演练，以支持与评估、预防、保护、准备、缓解、响应、恢复及运行程序；

j) 确定和执行消防方案，为正确使用防卫装备提供支持；

k) 确定内外沟通管理程序，包括媒体或公众信息和管理响应程序；

l) 建立和维护监测成功的绩效；

m) 记录此标准和产品作为组织的重的关键职责，基础设施，持续及职责；

n) 确定确保信息共享可管理，时效性，并确保能及工作环境安全的变化的程序。

管理体系的成功取决于组织中各级部门及职能的领导和承诺管理层的投入。为实现这一目标，高层者应为必要资源和适当的责并确保其安全。有必要建立适当的行政结构以有效地进行策略、规划和管理。这一结构将确保所有各方了解该要求为何人、决定如何执行、以及组织各下所有工作人员的职责与责

是一个动态的持续保安服务文化建设。

对于从事或承担保安服务的组织来说，如果其行动直接或间接地影响其客户的利益（或客户的利益对其组织至关重要），则其客户有权期望组织遵守本文件的规则。组织的不当、违法和过度行为的后果可能会导致客户流失、争议诉讼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发展闭环过程，每个要素作为一项管理及时功能单元进行实现。其组成要素主要包括：与组织策略相适应的一个体系的组成部分基于五级架构和与其他体系架构的兼容性进行规划时，对其理解得到加强。要完全理解并实施管理体系要素，统一方法及组成该功能单元与整个元素或对其进行规划。这就产生了一个迭代过程，这个过程中体系和政策的建立、风险评价、实施、操作、审核和审查形成一系列管理的步骤，也是一个互动的闭环。

管理相关概念的层级如下：

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) 了解体系各元素之间的动态交互作用。

管理体系方法强调通过整体战略利益导向，这些战略将支持并在组织运行和复杂的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，建立风险和机遇评价准则为基于过程的战略和决策提供反馈环路。

C.3 组织环境

C.3.1 理解组织及其环境

C.3.1.1 总则

为了管理风险，促进合适组织的文化氛围，组织需要识别和理解可能影响其保安服务目标实现的内外部因素。

当组织策划保安服务管理体系时，首先应该理解其运行环境及组织内外部影响因素和其运行环境，通过理解环境，组织可以确定其保安服务管理体系的范围，作为保安服务管理设计一个适应框架，这有助于确保组织确定内外部对成就其目的目标、需求和期望，这种环境既与组织、客户和受影响群体感知风险管理的范围，从而为风险评价和处理过程，确定风险准则和重新运行提供基础。

在建立内外部环境的过程中，组织应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在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管理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

确定组织的外部环境时，需考虑以下几点：

a) 当行业和运行环境相关的风险因素；

a) 影响组织的保安服务和运行环境的外部因素；
b) 作为风险制造者的风险承担者的外部利益相关方；
c) 受保安服务相关风险影响的外部利益相关方；
d) 影响外部利益相关方考虑风险的因素。

C.3.1.4 明确组织分配方信息的数据和分析

组织在管理保安服务的风险时，要了解业务组织的文化和环境以及供应链结构，供应链包括合同签约方和分子公司条件。组织的供应链的每个节点都涉及一些需要管理的风险和管理责任。

供应链和采用分包方是保安服务不可分割的一部分。业务供应链中没有明显好标准或存在差异，组织供应链的每个单独节点在特定方面都是独一无二的，这种独特性可能需要定制组织对其业务管理带来的风险。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级每一成员的相对个人的作用；
b) 了解对持续成功交付重要的相互依存因素和商业连续性；
c) 每个节点的信息技术网络能够支撑作用程度的信任等其他部分的表现；
d) 确定每个节点受损或丢失风险消费的可能性；
e) 评价每个节点如何在管理体系实施过程中影响影响，成功降风险最小化。

当进行节点分析时，组织应认识到在各个节点做出的决定可能影响整个供应链。因此，在设计保安服务管理体系，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

组织应了解评价风险重要性的准则并对其进行定义。风险准则应反映组织的价值观、目标、资源以及其保安服务的状况。风险准则将确保评估风险因素和风险应对需求的管理。

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收记录，同时记录与利益相关方的互动。组织宜考虑利益相关方的需求、理念、价值观、规型、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) 供应链和价值合作伙伴；
d) 负责确定服务许可、授权和监管的法定上管部门；
e) 适用范围内的社会群体；
f) 相关行业协会和标准组织；
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以是个组织，特定业务单位，并要对范围定义的适用性范围中选择进行实施。这些范围将反映了保安服务管理体系的最高管理层和从其组织及其活动的视角，性质和复杂性。一旦确定管理者确定了保安服务管理体系的范围，范围内的所有要素，活动，产品和服务都将成为管理体系中重要的考虑。

组织应采用风险评价方法来证明范围涵盖在保安服务管理体系范围之外的任何情况。排外情况可包括组织无法控制的某些服务或者设施件，后备/额外情况对下决定该组织建立哪些业务应最终

文件，作为适用范围内及其客户业务的完整性。保安服务管理体系的范围应作为组织可用性的一项声明提供，例如以适用性声明的形式。

组织在各种环境中可能不同地开展保安服务。根据保安服务和风险评价的情况，"适用性声明"应记录本附录中适用于在组织范围内建立和实施保安服务管理体系的相关条款。

单独和分包活动的责任组织的责任，其应当在保安服务管理体系范围内。如果外包或分包的产品、服务、活动或组织流程的一部分仍然在组织的风险责任和管理控制之下，那么适用管理体系应确保这些在保安服务管理体系的范围内。组织应确保适当的协议并达成适当的沟通渠道与其合约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实现所提供的保安管理体系的证明有效性等考虑，当组织评估特定要求在适当文件时，可使用组织活动和分析它的过程方法，计划和规定实现本文件的要求。

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基础目标是：

a) 提高保安服务水平；

b) 保障内外部利益相关方的安全；

c) 形成基于合法权利和义务平衡基础的文化氛围。

本文件规定的范围是，组织将选择，评审和评价其保安服务管理体系，以确定不断适应和正确预防错误的对应。组织面临不断变化的风险环境，应特别注意其预期保证保安特别改进的程度的范围，范围和时间，本文件要求组织：

a) 建立适当的保安服务管理方针；

b) 评估和管理因及组织保安服务的各种风险；

c) 明确适用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、目标和指标所需要的方案；

f) 实施策划、控制、监视、预防和纠正措施以及内部审核和管理评审相结合，确保方针得到遵守，保安服务管理体系保持有效；

g) 随情况应予修改的环境。

C.4 领导作用

C.4.1 管理承诺和承诺

C.4.1.1 总则

组织的最高管理者应承诺并下决心在组织中实施保安服务管理体系。具有最高管理者的承诺，任何管理体系都无法成功。最高管理者应与其内外相关利益相关方沟通承诺，并提供保安服务时遵守适用法律和要求合法权益。为了保证最高管理体系工作动计划与构建，最高管理者应自己或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) 遵守适用法律法规和要求合法权益的利益相关方的期望；

c) 将保安服务管理要求纳入整个的组织业务；

d) 将问题视为改进的机会。

最高管理者应证实其对建立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；

j) 制定和传达方针的风险策略；

k) 确保在各级各部门确立保安服务目标；

l) 确保在建立内部和沟通相关管理体系时明确职责和权限；

m) 为管理体系持续运行的管理；

n) 确保代表该组织工作的人员的能力，并对其进行培训；

o) 组织和开展管理体系和风险要求化工作；

p) 确保全组织知悉实施管理体系要求的认识和风险意识；

q) 认证准备；

r) 新加坡和其他管辖权的过程。

组织的最高管理者负责必要的资源，并为建立、实施、保持和改进一个总体目标，旨为达到确保组织内各级管理层和工作人员知晓和实施各管理体系要求和预期的组织管理优先事项。最高管理者应针对保安服务管理体系制订"自上而下"的方法，使得组织各级管理层对体系的维护责任作为企业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，开展与其业务相关的一切的保安服务。

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，制定方针应从最高管理者的以下承诺：

a) 把考虑人的生命和财产作为重中之重；

b) 减少、预防和减少事故和其他事件的发生及其影响；

c) 符合适用法律法规的要求和适当要求；

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绩效提供框架。保安服务方针应明确，能够被内外部利益相关方理解，并定期进行审查和修订以反映不断变化的环境和情况。其适用范围/界限应可明确识别，应反映职能、产品和服务活动风险的特性质，明确和影响。

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，特别方和社会群体的相关成员，使其分包方和外部其他各方对，可采用书面声明的形式，例如张贴，张贴和展示，明显地向所有预期的更广泛的社会群体传播保安服务政策；向最高管理者定义和授予承担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，为了提高保安服务管理体系的有效性，需要将其承担的代表组织工作的每个人身上，应下体系是一种自上而下、自下而上的方法，保护合规性最和管理风险将成为组织文化和习惯的一部分。所有风险制造者和风险承担者都应是风险管理者。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。

管理体系在组织内的人员进行实施。因此，宜任命一名或多名合格人员，并授权实施实施，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，可考虑一个包括所有主要组织职能部门和后勤工作组的高级管理团队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

从事或寻求保证安全服务的组织从运行环境来确定其有风险，这些组织需要管理客户、组织本身业务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，组织需要实现预期结果、运行安全并持续改进，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，要求保证处理依法合规相关问题来实现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，确定的挑战是评价、评定及处置风险，以便有效地控制风险和其不确定性。通过风险评估可确定了解风险环境，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。

通过风险评估应识别潜在外部利益相关方的风险，应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，来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奠定了基础，并能识别组织的安全服务管理体系宜处理解决的风险。风险评估为实施管理体系内部设定目标和程序及测量安全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

组织应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符合法律规定，避免争议，减少罚金，改善组织的形象及增强组织的能力，从而为客户和尽可能的保护服务。

组织应建立和实施管理体系所需流程中应识别、遵守和评价适用的法律法规和监管要求。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) 适用的强制性标准法律规定；

c) 本文件的，从原始或现有要求的强制性行为的增加；

d) 安全服务运行采用的有关的卫星系统使用是否符合法律法规要求。

组织可采用要求的其他要求包括：

a) 建立及其他合同义务；

b) 与公共机构、社会群体的协议；

c) 与客户的协议；

d) 非法规指南；

e) 自愿原则或行为守则；

f) 产品或服务管理审核（无须图例）；

g) 相关社会协会的要求；

h) 组织或其上级组织的公开承诺；

i) 非约束性协议；

j) 组织保健要求；

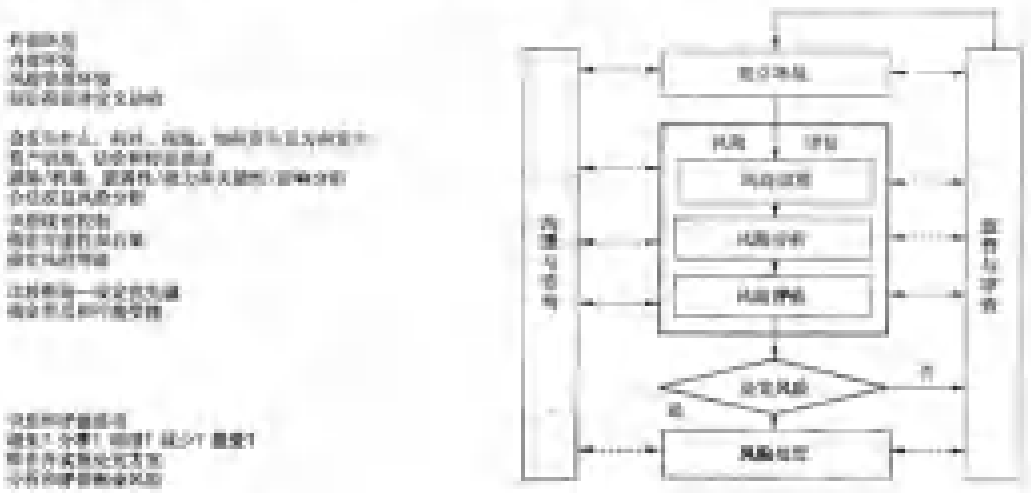
k) 捐赠义务；

l) 社会责任组织要求；

m) 与组织、结果性有关的私有性。

C.5.1.2 风险评估

C.5.1.2.1 ISO 31000 中风险评估过程



注：摘自 ISO 31000:2018。

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：通过感知分析、危害性分析、偏离性分析和合法权益风险分析对风险进行识别，分析和威胁的过程，还应考虑风险成因，来源是可能影响组织及其利益相关方合法权益，给组织带来风险的事件，包括组织管理层没有可能的明显原因完成其业务，影响和运行目标的所有风险事源，包括客户、组织代表人员及其他内部影响相关方的权利的安全。

b) 风险分析：理解风险和风险程度的过程，确定被当做确定合法权益的风险及分析风险的最适当的方法。确定了预期，预测事故风险或损失事件，风险后果(包括产生损害)及事故和后果发生的可能性，识别影响结果和事实时，事件对利益相关方造成的后果，风险导致随着可能性，严重程度以后果变化，为风险处置的优先顺序提供了依据。

c) 风险评价，支持决策点时，在管理风险需要和风险准则相对比的过程，风险评价确定了风险本质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，以做出风险处理，风险处理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

合法权益风险分析的目的是确定、评价与合法权益相关的风险发生影响的过程，主要包括：其目的是控制风险，减少或防止危害合法权益的影响，造成任务。企业权益风险分析主要集中于合法权益风险评估"或"合法权益影响评估"，合法权益风险分析是同时评估风险和消极影响的基础，消极影响指风险管理活动的严重程度分级和考虑。进行风险识别和后果可以为管理和组织相关资产的风险环境提供依据，合法权益风险分析为组合风险评估过程的一部分。

进行全面合法权益风险分析与识别，评估、管理及文件化风险或损了记录，可以跟踪，减少及记录得

[illegible]

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、业主方、外包合作伙伴、供应链及其他业务关系相关的风险；

b) 可受风险和相关活动影响的内外部利益相关方进行沟通并有意义的协商；

c) 识别和确保必要的合规权益与实现组织能力，以进行企业保安风险评价，并证明合规和风险程序实施的合理性；

d) 为降低风险评估过程从实施到评审、监控、检测直至单个活动或整个程序的风险，并确保适当的组织和特定保护。

C.5.1.3.3 风险评估过程注意事项

风险评估可根据管理风险定义风险包括但不限于：实物性、严重程度和位置，组织应在风险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人与产品（有形和无形的）：

a) 资产的、产品和服务；

b) 与环境和社会群体的相互作用；

c) 与内外部和监管机构的关系；

d) 公共建设和相互依赖性。

风险评估宜包括但不限于识别导致或预防不确定因素的评审分析和评价，及确定各种利益相关方过程的组织责任，单纯包括但不限于：

a) 为使命和运行的关键特性风险；

b) 与组织及其资产的声誉有关的风险；

c) 财政、法律和社会影响；

d) 对组织工作人员的威胁和脆弱的后果；

e) 对社会群体及其他利益相关方的威胁和脆弱后果及运行对他们价值权益的影响；

f) 与业务关系相关的风险，比如外包合作伙伴以及与参与保安服务运行的其他组织的潜在影响；

g) 策略和运行风险的相互关系及要素生命和价值损益的内在关系。

风险评估有方法很多，组织宜建立、实施并维护成文的且可重复使用的正确方法，通常要求或定义和评审标准包括：指标、评价准则和结果。

一个组织可能存在很多风险，因此，有建立和文件化确定重大风险的准则和方法，单一方法无法确定每个风险。组织所用的方法宜提供一致结果，且宜包括评价准则的建立和使用，比如关于生命和价值权益保护、环境影响的严重程度、预防或减缓不良影响的作用、运动和功能的能力和程度、法律和组织及对内外部相关方的关注等评价准则。组织宜分析与预期事件或干涉有关的可能性和严重程度及对运行和组织产生的后果，并识别和对照目标之间关系和实施的关键运行。

评估后果时，组织宜考虑以下各点：

a) 人力成本，如客户、组织工作人员、供应商，社会群体及直接利益相关方造成的身体和心理伤害；

b) 财务成本，包括财产重置、停工、罚款费、赔偿索赔、销售/业务损失、诉讼、行政处罚等；

c) 物质成本，声誉、社会响应、负面曝光、业务关系等；

d) 环境影响，特别是对环境内、对特定人员和部件（尤其是珍贵野生体或濒危群体）的实际损害和负面环境影响。

——社会影响：对区域经济及区域经济所应减少的影响。

——环境影响：环境质量或潜在的影响。

风险评估是组织在决策过程中综合考虑组织开展业务和管理活动的过程，包括与内外部各相关方（个人、组织）之间的沟通、咨询、评估和管理风险的活动，以及对决策和行动过程的监督和评审的一系列活动。风险评估应考虑内外部环境，法律法规及其他要求。

为保证风险识别的准确性和全面性，组织应建立合格的组织机构，组织由管理和具有丰富理论与实践经验的专家、学者参与风险评估的全过程，并选择恰当的管理、财务、技术、社会和管理数据的获得技术，以及适宜的比较标准。风险评估有不受程序约束，因此组织的信息可能比较主观。收集数据前，应明确组织安全管理体系所涉及的相关业务单位的范围，风险评估的结果应当能够帮助决策者做出决策，以确定保安服务管理目的、目标及范围，组织应考虑以下因素确定风险评估的选择：

a) 保安服务管理体系的范围、产品、服务和活动；

b) 组织的义务；

c) 法律法规及合同要求；

d) 保安合同构成的要求；

e) 受影响社会管理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。

风险评估应根据事故和异常运行状态及合理预测等干扰性情况，以便更好的制定预测事件和干扰性事件，但由于无法预测所有事件情况，组织应该在不考虑事件本质的情况下，评估其特定关键资产，活动和功能及受影响社会管理和利益相关方造成的后果，以便作出管控风险。

风险评估宜：

a) 用表明关键支持的定量和/或定性方法来理解识别到的潜在风险的可能性或系统及单位变动对后果的严重性；

b) 基于合理和明确的准则；

c) 充分考虑对组织采行准则的所有潜在风险；

d) 考虑风险与其他各方的相互依赖性，包括资产、社会群体、需求关系和供应链的依赖和约束；

e) 评估法律义务和其他义务的结果及管理组织活动的注意事项；

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或后果严重性难以确定的风险；

h) 分析和评价管理风险后果的成本、效益和原则；

i) 评估组织可通过针对性举措和管理对到风险和影响。

注：为组织决定对风险做出、风险规避、风险管理、风险最小化、风险转移以及基本/适当的风险处理方案提供参考。

在某些地区，采取新的设施，社会群体资产和文化遗产可能受到的运行所有影响的重要性或后果评估，组织应考虑新建组织所面对风险并适当影响风险管理决策的考虑。

在开发与此相关的潜在风险的信息时，组织宜考虑记录相关的数据信息，这对相关决策者管理体系的改进。

风险识别和评价应考虑有助的范围，适当分析组成本和时间以及可能获得的可与性，该范围宜涵盖为业务策划、需要或其他目的而考虑的信息。

组织宜在活动的整个预期中定期进行重新评估，以完成不断变化的组织运行、运行环境和对组织的影响。导致重新评估的重要可能包括：

a) 合同与行业的变；

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) 组织环境；
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安保事协商流程，以收集风险评估输入信息和控制假设结果，在风险沟通事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"是通常事项，例如将意外最小化的目标。保安服务的"指标"即相关绩效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、执行情况并能实现的目标。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和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有效性的、及时的、确定和恢复事件的信息。

在建立目标和指标时，组织宜考虑：

a) 政策承诺；
b) 与战略目标保持一致；
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) 绩效监视；
h) 基础建设要求和相互依赖关系；
i) 相关相关方的利益；
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、具有成本效益和被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、间接和固定成本。

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、基

略和预算协调实施一、行动计划可能涉及为实现组织运营的具体要素。

为了成功管理保安服务运行，战略和行动计划应明确：

a) 实施目标的要素（谁将负责？在哪里实现？）；

b) 实施目标的手段和资源（如何实现？）；

c) 实现这些目标的时间表（何时完成？）。

战略运营部分应基于组织运行的具体要素，以简洁每个成文的策略和实施战略确定责任、策略步骤、资源需求和时间表，组织应可采用若干行动计划。

在适当和切实可行的情况下，战略应包括与重启、设计、建造、试运行、运行、改造、服务、销售，并征询关键运行有关的组织活动各阶段需考虑的事项。战略开发可为应急活动和新活动，新产品和/或新服务进行战略开发。

组织的策略中应考虑活动、合同关系、员工和社会群体以及运行连续性优先事项的必要性。

战略应是动态的，可重复使用修改，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支持性进展；

e) 活动、产品、服务、过程或运营发生变动出现其他问题。

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。最佳选的单个（或多个）战略应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) 不确定的后果。

最高管理者应在考虑文件化的战略类确认已确定的保安服务运行策略已经适当地实施中，考虑战略已经解决了影响事件或于发生事件的可能或预有影响，且与选择战略适合组织确定的组织目标。

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。组织宜独立和保护以保护利益相关方生命和安全为宗旨，同时兼顾合法的业务运行所提供的产业利益务完整的战略。此外，宜确定与公共机构和社会群体其他方的互动和协调，并将其纳入战略实施中。当外部组织相关方的运营战略实施应支持应急准备和保安服务运营目标，且要得到证明并形成文件。

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智能、场所、内部基础设施、技术、信息和财务资源。最高管理者宜确保在实施和管理体系和增资源的确定、提供和维护。

C.6.1.2 能力要求

C.6.1.2.1 总则

合同为客户和供应方之间关系的主要法律依据，订立合同的组织者宜为成人实体，并且组织宜确保授权代表签订合同。

C.6.1.2.2 组织结构

组织宜建立一个管理结构，明确界定履行合同及各所必需的角色、责任和职责。

C.6.1.2.3 保险

组织宜寻求充足的保险类型，以满足对任何人关于符合其风险评估的人身伤害、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) 在合同中规定限额和限制；

b) 按事故管辖区域及争议发生情况；

c) 免赔额；

d) 除外限制；

e) 所有设备，包括使用的工装备；

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) 分包商的活动；

h) 保护客户。

宜考虑的保险类型包括（但不限于）：

a) 债券；

b) 工伤赔偿；

c) 雇主责任；

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保证且宜规定承包方、分包方履行的责任条款和条件。组织采取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，也宜解决组织的财务风险。

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，并代表其执行任务，包括：

a) 为可能受事项影响并成为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、分包方提供其雇员具备必要的能力和接受适当的培训；

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) 宜持续开展监控和业绩评估活动的水平，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。宜在现行其职责的情况下，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，并按照培训要求的一致性和标准化。培训宜包括保护合法利益的内容。

C.6.2.2 能力认定

组织应识别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) 选择适当的方法和资料；
d) 将企保安服务管理体系培训要求的验证方法；
e) 培训目标群；
f) 记录和监控受训的培训；
g) 根据培训需求与要求评定受领的培训；
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) 严禁泄露个人隐私或者依据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) 严禁实施其他法律、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的人员进行培训，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、种族和文化问题，以及重点地区等；
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、调查和报告相关犯罪的措施。

特殊和特定状况主题的实例可包括：

a) 技术运用；
b) 谈话技术；
c) 路线引导；
d) 电子沟通；
e) 医疗救护；
f) 社会媒体使用；
g) 协议调查；
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，试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。

培训和监控方案可包括：

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；

h) 应组织的对事故调查、预报、入门方案或期刊(包括新员工入职培训)中涉及关于保安服务管理的讨论；

i) 保安业务管理政策和相关网页或内联网上；

j) 本组织学习管理体系中加入在线培训模块；

k) 通过组织活动报告从内外部事故中学习；

l) 将保安服务管理作为管理小组会议中的一项；

m) 会议及课堂培训；

n) 紧急救护及其他实际操作培训。

所有人员都应接受培训，来履行其个人与保安服务管理体系相关的责任。他们应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个人信息相关法律法规，并接受相关培训。这种培训可包括关于预防和管理暴力袭击、闯监、文件编制和回答要求以及处理社会群体、客户和媒体咨询的程序。

应为装备使用培训，包括使用软皮的培训。培训宜包括指导性培训、基于情景的培训和防卫装备复习培训。

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)。新成员在进入团队时宜接受培训，应急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纳入设计人员能力、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) 能力鉴定及检测结论；

b) 培训方案；

c) 对组织工作人员绩效及评估的相关记录。

C.6.3 意识

组织宜在其内部建立、发扬和维持安全服务管理文化，这种文化宜：

a) 确保保安业务管理方针和意图合适且益于与组织核心价值观和管理的一致性；

b) 使相关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) 有利于提高个人健康。

C.6.4 沟通

C.6.4.1 总则

有效沟通是预防、管理和汇报潜在预期事件或下发性事件最重要的措施之一。宜与内外部利益相关方进行积极的沟通和协调，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信息，可能需要对受众进行分区管理。通过这种方式，可将消息发给员工、客户、社会群体或特定群体。

沟通程序宜解决以下考虑：

a) 组织各个层级和功能之间以及与承包方、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) 将媒体与外部利益相关方(包括媒体)的沟通；

e) 与相应利益相关方根据实行的关于响应和避险计划的沟通，并根据预期响应；

f) 促进与受益响应人员的结构化沟通；
g) 在干扰事件下沟通重建的可用性；
h) 信息的敏感性和管制规范；
i) 工作环境。

组织应实施接收、记录和回应内外部利益相关方有关应急的程序。这一程序可包括与利益相关方管理层探讨其相关顾虑的考虑。在一些情况下，利害相关方照虑的回应可包括与组织沟通和减轻重要有害的风险、影响和/或程序相关的信息。应确保协调员与专责部门就应急计划履行和沟通相关问题进行的必要沟通。

C.6.4.2 媒体沟通

需要业务沟通计划，以对正在进行的恢复及服务提供予以控制，协调和关注。业务沟通计划宜包括对恢复服务工作人员、客户与监管主体如何分享相关威胁信息。

C.6.4.3 风险沟通

组织应与包括媒体在内相关事件有关的事件情况、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。组织应正式规划其协同、缓解和响应沟通战略，同时考虑到针对相关社会群体的特定、适当的信息和方案以及平段的选择。

组织宜建立与内外部利益相关方沟通和协调的程序，其内容关于具体组织风险、风险影响和优先顺序。这些程序宜考虑具体的利益相关方、沟通的信息类型、干扰性事件的等级及通报、沟通方法的可用性以及组织的干预情况，如适用还宜予包括：

a) 新闻或新闻稿；
b) 媒体；
c) 群发邮件；
d) 网站；
e) 社交媒体；
f) 电话，电子邮件和短信；
g) 社会媒体会议。

组织宜对干扰性事件进行初步短期沟通。宜为响应评估中识别出的直接受影响的利益相关方、监管机构、媒体和公众制定沟通计划。计划宜包括负责识别出的一个或多个利益相关方、也宜建立确保计划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员，发言人宜管理并协调媒体和其他人宣传应急响应，宜按照关于媒体关系、危机应对和在多时区响应上的培训，所有信息宜通过一个单独的小组汇编，以确保消息的一致性，最终管理者宜监督，以减少和所有组织工作人员关于应对应急响应与媒体的互动，并且只有获授权的发言人可接受媒体采访。在一些情况下，组织要确定适当的组织领导人。

C.6.4.4 沟通投诉和申告程序

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，程序宜确保服务机构要性，考虑应目标受众的文化、语言、教育和技术要求。宜建立程序，为改进和纠正沟通汇报机制。

C.6.4.5 沟通举报政策

举报由关于组织工作人员实际内外部影响他人的负面、不道德行为或违法行为。组织工作人员可能有份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作为内部利益相关方的玩忽职守和不当行为的关注。举报为针对有助于组织以适当的方式处理问题，同时也可对那些可

和非道德行为，不当或不道德行为的人最初或随后报告。良好的举报方针将有助于识别减少问题，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，以服务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，以及需要树立的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.8.5 成文信息

C.8.5.1 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，说明在何处参照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，不必拿是手册的形式。

不同组织的保安服务管理体系文件编制范围不同的范围，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，一般性声明和遵循规范；

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) 内部和外部规则；

h) 事故响应，战略，应急和危机计划；

i) 记录。

文控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) 较文和确定访问而减少；

d) 记录可靠性和重复性。

最初创建以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.8.5.2 创建和更新

C.8.5.2.1 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（无限）：

a) 符合性记录；
b) 培训证；
c) 对序列化和敏感设备的业务责任；
d) 燃料和其他易消物资报告；
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

组织应创建和保持文件，并使其满足保安服务管理体系的实施、维护，组织的主要重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。

保证正确的密信息，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和生命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。运行管理含保安服务运行的所有内容，包括计划方、供应链和维护活动等。

保安服务管理体系发如何将体系要求应用于其业务组织指导，因此，宜应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不良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，组织宜在实施这些变动之前考虑相关或新的风险降至最低。

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。参见 8.1.2.1 的 a)～d)，组

组织：

a) 沟通招揽供给保险服务的详细情况，出售客户投保所选择的保险服务，签订保险服务协议书、投保单、批单、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险服务的联系方式；

——提供客户相关更改信息；

c) 提供适当的途径，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，其方式包括但不限于直接交流电子邮件或打电话、座谈调查、客户支持热线（如适用）；

d) 确保在适当时将组织向客户财产的处置有关的方式通知客户；

e) 确保主动参与客户沟通可能采取的应急措施，即需要采取应急措施，则宣传先可能对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、人员短缺或应急预案时方不足等情况的应急措施。

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

8.7.1.2.2 保险服务要求的确定

组织在确定保险服务要求时，宜考虑：

a) 客户提出的保险服务的内容与要求；

b) 客户未明确保险服务的要求，但组织了服务的对象（如金融购点、重点区域等），组织满足对服务客户的保险服务要求；

c) 与保险服务相关的适用法律法规要求及相关文件的要求；

d) 组织认为必要的附加要求。

组织需要确保能够对所提供保险服务做出的声明。此声明是组织关于保险给客户的保险服务及其特点与技术方案的描述。例如组织可能对其提供的保险服务等会客户的项目投承要求做出声明，比如特别针对人员要求，保密协议，廉洁协议等做出声明。

适时宜考虑以下因素：

——可获得性；

——服务能力；

——服务时间；

GB/T 19580 提供了组织行为规范指南，包含了做出声明的相关内容。

8.7.1.2.3 保险服务要求的评审

组织应对客户作出承诺前，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保险支付服务问题的风险。

针对 8.7.1.2.2 的 a)—g)，组织宜评审：

a) 支付前支付后的保险要求，如人力资源保险、客户培训、现场服务、客户支持单；

b) 是否满足隐含的要求，即保险服务最终满足客户的期望（如服务人员着装规范的银行柜员，服务人员应耐心细致地关于保险帮助，人员销售应适时要求）；

c) 组织选择的为能够客户需要，增强客户满意度所合内容及各项方面的服务要求；

d) 适用保险实施步骤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，则组织服务与客户沟通并确认后选择；

g) 若客户未能其服务的保险要求的说明，如仅通过电话或口头保障进行确定，则组织需要在选择保险服务之前与客户确认这些要求（如在服务过程中，增加人员或提供额外人员服务）。

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，包括任何时正或更改，并准确地满足客户要求。

对附录A.3.2中第二段组织保留成文信息中的(b)：

a) 评审结果可通过适当的载体予以保留，如组织可选择保留包含与客户之间作为于确定满足要求可保留评估的风险评估报告；

b) 组织应说明存在新产品要求的更改，组织应保留或增补成文信息，以确保新要求已被知晓(如更改订单或接受新产品要求的电子邮件)。

组织成文信息应当包括与客户沟通有关产品和服务要求的信息以及组织的投标要求。

8.2.3.2 确定服务要求的更改

本条要求确保组织对特定的相关人员知晓对提交服务要求的任何更改。组织宜保持适宜的沟通方法，并保留适当的成文信息，如沟通的邮件、会议纪要、补充协议等。

8.2.3.3 服务的设计和开发

8.2.3.3.1 总则

本条旨在确保组织建立、实施和保持设计和开发过程，以确保其提供服务满足要求，并确定服务提供。组织在确定服务管理体系的范围时，宜考虑包括所有关键相关方在内的组织环境，因为该范围决定了8.1.2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。如设计开发是完成客户指导。

产品按照客户的要求的组织，只有在客户对设计方案做出了批准或其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，由于服务管理体系范围，客户或相关组织要求或新法规行事调，组织可能决定将设计和开发要求用于运行过程。

8.2.3.3.2 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阶段和控制。这些要求宜包括考虑组织确定所需的资格(见附录A.7.1)。这些措施可能对策划后续的实施、资源需求以及潜在和新型相关产生影响。

本条的要求包括了在设计和开发策划期间应考虑的一些关键要素。附录A.3.2的a)~j)，包括考虑：

a) 保交服务的复杂性(如重复设计、新设计、保证服务正常，服务的策划范围和适用要求计划等)以及实时要求等因素；

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(验证服务设施要在技术方案进行了适当的确定)和确认(如进行认证考核和测试)；

c) 确保确定满足输入要求所需的验证活动，以及确保最终获得实现参考要求规定的使用目的和特定要求的确认活动；

d) 从事设计和开发的人员，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、人为资源、设备、技术、能力、客户或外部供方的支持、编制工作人员、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，参考参与人员的数量和参考的信息共享方式，如会议、流程流程、会议纪要等；

g) 在设计和开发适当时，客户财物损失或者信息泄露（如客户的视频监控、客户病历、客户健康）；

h) 组织内人员提供服务无法或支持服务的紧急事件（如技术方案、应急预案、人力资源、接收准则）；

i) 客户或其他相关方在过程所确定的期望控制水平（如应急管理、残障残疾的安全已完成的质量服务的专业检查），若客户未确定预期的控制等级，组织制定且考虑在安全者承担治理下的实际情况的控制等级；

j) 所需的成文信息（以证实服务已满足设计和开发要求）以及有效审、验证和确认所需实施、过程和服务的主要要求，测试和应、作业指导、方法和全场指南。

C.7.1.3.5 设计和开发输入

本条要在确定组织规模适设计和开发项目的输入并与设计和开发要求的编制一致适当，应确输入应确、完整并与预期目的要求的一致。（见附录A.7.1.3.5）应考虑：

a) 客户、应场所要求或组织确定的功能和质量要求，如适应的预测结果，理解特定服务的标准，应特定和预期的服务；

b) 适应法律和设计和开发活动直接的信息，如法律文件、应适应场所的要求，适应质量管理体系的要求（如组织要管理）及环境或避免由规管理；

c) 与以前类似设计相关的信息（如在实服务管理条例），或与前实服务施所相关的运行适应要求（如前实服务中对犯罪嫌疑人的记录，在前后阶段的适护服务时不适人规程）；

d) 组织承诺遵守的产品或适应标准（如行业规范、道德准则）；

e) 因前实服务失败或其他原产生的潜在后果（适外实现的影响范围可能应由先前的失败所以承担额外责任要求等法规可能导致诉讼）；产生投客户不满意的各种问题（如人员损伤或下游后失败）。

应用于设计和开发的输入应能为成文信息予以提供。这些输入可能来源于策略中所明确的其他要求或适用法律。

在输入要求获得中，或以提供或实现的情况下，组织有采取行动措施（解决以下内容）：

C.7.1.3.6 设计和开发控制

本条要在确保输入一旦确定之后，即可根据策划在施设计和开发活动并加以控制，并证确保过程符合：

a) 确定设计和开发过程的阶段及其应实施的评审、验证和确认活动，以确确认其适应了输入要求，确定了问题并确定了输出方案；评审与设计和开发过程相关的职责和人员对参与活动评审，验证参与确保评审人员以及相关部门，确确保产物和预期一致，并发现和产生的不知道措施；

——复杂设计的评审可能先后进行或上进行，其次证应当对应为相关记录；

——简单设计的评审可能不需要那么正式，其记录可简单地计划上表明已满足评审的程度，评审人员可签名和注明日期；

b) 进行验证，以确保输出在设计和开发过程中满足相应的所有要求，对于输入的要求，应该和当前行为或下个步骤阶段，在每个关键阶段结束时验证或确认活动，确证活动可包括：

——实施替代计算；

——将设计与已实现的规格设计进行比较；

——开展测试和演示；

——查阅检查或计划阶段的成文信息。

d) 进行确认，以确保组织按服务需求满足客户或外部用户的预定要求或使用要求。确认活动可包括：

——试运行；

——实行测试；

——按照用户的预期条件进行模拟或测试；

——部分验证或测试（如概念类发布前的验证）；

——客户或最终用户测试，并提供反馈。

e) 评审、验证和确认活动暴露出存在问题，则应确定相关变更问题的处理方法，并记录确认有效性评审结果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，以及满足规定、按照标准试验方法以及客户批准文件。

8.3.3.5 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、服务提供过程或活动）提供必要的信息。这步信息需足够清晰，以确保参与者理解将采取的措施和其相关职责。

依据 8.3.3.2 的 a）—d），设计和开发输出应：

a) 与 8.3.3.3 所规定的输入要求保持一致；

b) 考虑预期的使用者和使用条件，足以确保所有提供安全服务的后续过程得到实施；

c) 提供有关监视测量要求（如适用）和验收准则，指导外部提供的过程，确定服务的恰当提供细节，以及保证服务实行的监督；

d) 规定有关保证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，并明确说明以下提供服务（如门卫对入驻记录）。

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（包括维护细节、人力资源说明、质量计划、控制计划）；

——过程规范，必要的人员未能到场情况；

——服务计划；

——工作指导书册；

——与基础方案所确定的岗位设计以及所要使用设备的规格说明；

——以计划形式呈现的，对营销活动的广告代理设计。

8.3.3.6 设计和开发更改

本条旨在建立和保持一个评审和控制在设计和开发过程期间或后续的提供期间的更改。组织宜确定何时实施与开展过程或相关方（如客户或外部供方）达成新的或修改的设计和开发过程的临时协议，并宜在确定设计和开发更改时予以考虑。

更改可在服务管理体系内的任何活动期间提出，包括但不限于：

a) 在实施设计和开发过程期间；

b) 在完成初步设计和开发输出之后；

c) 得客户或直接外部听方的情况作为验证结果时。

有关设计和开发更改问题的成文信息，可包括更改问题实际考虑因素以及已实行的发展或外部产生影响的评价结果，以防止产生不利影响。评审、验证和确认过程需要时产生影响服务设计和开发

[illegible]文信息，成文信息应当详细说明对受到影响的后续过程（如采购、培训、售后服务等环节）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当事人对应执行更改、这种授权有时是来自客户或监管机构的要求。成文信息可以是处理单的更改单或电子签证更改单。

C.7.1.4 售后服务的提供

C.7.1.4.1 总则

服务过程宜按照合同文本和相关适合性权益的要求，提供保护人身安全以及有形和无形资产安全的相关活动。

C.7.1.4.2 售后服务提供过程控制

本条旨在规范组织对售后服务提供过程进行控制，通过确定适用于合格服务的可测量、确保实现预期结果。

组织宜建立售后服务绩效考核机制，以确保与合格交服务行为相关、遵循承诺和与客户签订的合同要求。

直接监管客户什么进行检测时，组织宜考虑售后服务提供的哪个环节，监控对交付后的活动要求（如质保处理）。组织宜考虑以下所有适用方面。

a) 确定和监控服务或进行活动的绩效的成文信息的可获得性，由此在向客户提供或过程的人员提供基于经验的成文信息，如行为规范或操作指导书，以及获得有关于确保售后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、准确识别的测量设备，或在交付要求中使用的测量方法。

c) 确保满足客户要求所确定的任何监视和测量活动，如在验证阶段进行的产品检测或对客服电话的监听。

d) 任何有关通知或跟踪过程环境的必要条例。

e) 确保人员具备开展工作的能力的要求（如适当的岗位护理），包括考虑任何必要的资格。

f) 确保其输出不能或过程验证被随后的监视或测量证实的过程所有的确认（确认是指通过提供客观证据，证实已实现了对特定预期用途或应用的要求），示例可包括仿客事件经验总结或、或员生跟踪事件等重点范围。

g) 组织宜实施售后的让人为错误，利用相关的工作时间二采取适当措施完成或改进的工作环境，最终应为的活动和操作，过程自动化，并关键信息要求应由电子签人、选择与周围设备以避免错误输入，避免人员信息重力分散（如个人电子设备等），确保输入要求能完整填写信息。

h) 对执行一定时间范围的活动实施控制，重要包括有形资产和无形资产交付前的验证、维护、检查客户投诉等。

C.7.1.4.3 售后服务提供过程的更改

本条旨在确保组织对售后服务期间发生的更改进行评审和控制，以符合售后服务期间的持续性要求。组织宜重点关注与处理这些更改所需的措施，以确保服务持续满足适用的要求。

本条特别关注在售后服务期间实施的影响服务符合性的更改，包括但通过控制这些更改，维护所采取的措施，以及评审这些措施如何影响特定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。

在实施所建议的要点之前，宜在运行的各个阶段对其进行审查。

更改前后的理由（如适用）；

更改的原因可能来自外部因素，内部原因素，如新的或已修订的职业健康法律法规要求）。

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。

组织应确定投标前的成文信息有效管理方式，其示例包括：

a） 评审活动的记录和结果；

b） 投标和确认的结果；

c） 结果的通知；

d） 受权进行更改的人员的详细情况（如适时考虑顾客）。

C.7.1.4.4 激素和生长因子

组织人员在接受急救和医疗等护理人员的培训和经验强化前，建立和维护管理程序，以评估和记录事件发生后心理是否为保证激素等和激素护的处理。培训应适合特定职责，并应包括护理管理流程，确保内容符合组织；建立和维护受控区安全，包括锁定、准备和清洁隔离，其中包括根据适用的人员职业健康要求和要求规定管理程序。此外，组织应根据每个客户要求的优先顺序，及时准确地与相关利益相关方沟通，个人保留在服务团队起作用于及时的行为和其他确定的必要材料（表明相关适应证管理）。

C.7.1.5 维护合法权益

组织有义务根据适用法律法规的要求维护合法权益，同时应建立、实施和保持保护个人财产的程序并形成文件，应制定预案并与相关方沟通，报告和解决不合规情况。

C.7.1.6 处理紧急状况干扰性事件的预防和管理

服务过程有强烈时间的导致造成的事件和干扰性事件的风险进行预防性和前瞻性管理，并应减少事件发生后的响应，恢复和补救措施。

突发事件指干扰性事件发生的事前，事中和事后，组织应建立合适的行政和财务体系以有效支持应急管理体系。应建立程序并形成书面化文件，确保权责清晰，资金调用和日常财务管理规范。此外，组织应明确管理结构，决策权限和责任（如组织主要领导、执行权限和责任）。

C.7.2 建立行为规范和道德准则

组织应与员工、分包方建立、实施和维持“道德规范”，“道德规范”宜清晰说明基本合法权益，严禁贿赂，利益冲突，虚假和其他欺骗行为（如使用企业或非比赛品来间接影响影响）。“道德规范”宜确保所有代表组织工作的人员了解基本合法权益，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地传达“道德规范”内容并提供相关培训。传达和培训宜定期更新。

C.7.3 防止服务使用

C.7.3.1 总则

防卫装备使用不当可能导致人员的死亡或严重伤害，组织和组织的领导负有责任，这会影响保护方的利益。防卫措施使用不当还会给未能有效使用已有防卫装备的企业和人员带来，保护组织人员和管理及附近区域的其他保护对象。

组织的防卫装备使用程序应控制防卫装备使用不当风险和防止武器工具，确定防卫装备使用程序要求：

a） 清晰且被所有配备枪支的专职守护，保安人员及监督人员了解；

b) 适用于复杂情况；

c) 有效实施。

当解决程序、责任的追溯和产品利益行为导致的决策或行为，并确保适当考虑或防止对相关人员的不利影响。

C.7.3.2 防卫装备使用原则

组织可制定在执法部参与合作应下使用防卫装备的总体指导方针，方针宜明确组织的使用理念、原则：

a) 仅在自卫、保护他人、或经授权、防止特定财产遭破坏等时使用防卫装备；

b) 将防卫装备使用控制在消除威胁的必要且合理范围内；

c) 尊重生命，保证人员在执行任务时，只有在避免死亡或严重人身伤害且没有其他合理选择时，才能使用致命性防卫或强制手段。

组织指定的防卫装备使用原则应适用于所有人员在各种情况下的防卫装备使用场景。

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面临攻击时，可使用枪械和非枪械防卫装备予以自卫，保卫特定人员（包括其他执法人员）财产的情形宜形成文件；

指导人员将防卫装备使用、确保防卫装备使用符合组织的防卫装备使用原则，同时也符合相关法律和行为准则。

如可能，程序制定时应与组织的保护对象协议，确保保护者与被保护者之间达成共识，同时确保防卫装备使用得到落实。

C.7.3.4 尊重生命，降低业务活动装备的一般通用原则

防卫装备使用的具体细则条件因不同地区和不同运行环境而存在差异。组织应根据防卫装备使用原则至少确定如下一般通用原则：

a) 在执行任务时，只有在其他较温和的方法失败、可能失败或无法合理使用时（例如下，专职保护特定人员才可以使用致命性武器作为最后手段。在执行任务时，只有在避免生命威胁、或财产遭受任何暴行与威胁生命或人身伤害的合理必要情况下，专职保护特定人员才能使用致命性武器或防卫他人）；

b) 当确定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，可选择与武力水平、程度要求、预警等相应措施等非致性的防卫装备使用。不论是否有意为之，在使用防卫装备使用都有可能造成意外严重人身伤亡。当决定的潜在的风险会随着装备显著增加时，以及他们者，使用指令及防卫装备使用的培训标准平衡考虑不断增加；

c) 防卫装备使用原则在任何企图用防卫装备实现合法目的，但目的和防卫装备使用的任何预防卫装备使用实施单独进行说明。若指定允许，组织应考虑使用重复测试的防卫装备或降级作业装备使用的方式加以应对。尽管如此，显著地且有效的降对有非常紧急使用的防卫装备或在极端危险防卫装备使用，基于情况下，组织应预先确定防卫装备的使用可能会增加的有关人员风险。

组织的防卫装备使用程序应考虑到个人、团队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法庭诉讼的风险。该程序不能为组织或组织人员提供绝对保护。组织和人员可通过程序证明在合理情况下，防卫装备使用程序和培训对组织合理的，并在不经意或有意的疏忽，或违背于对他人安全的重视和漠视方面程序的缺陷行为。

组织的防卫装备使用程序与适用法律的要求相互严格。应注意第5.7.3.3条组织的防卫装备使用

保护相关安全措施法律赋予的正当防卫权利。

C.7.3.5 防卫装备使用登记

从事专职守护、押运的组织应制定程序，确定需要配备防卫装备执行的相关职责守护、押运任务的人员，以及适格人员可配备防卫装备的情形，防卫装备使用权应限于适用法律法规和本组织确定的人员，专职守护、押运人员执行守押任务时，依法享有法律赋予的法律权限，组织应记录相关施行的重要事项信息，以证明该人员在合法授权范围内及依照本组织的使用管理、立专职守护、押运人员的资质和本组织之前申领其配发防卫装备。防卫装备使用授权应随时接受或知道适当、防卫装备使用登记标识物合格的人员使用防卫装备。

对于代表组织工作的授权配备防卫装备的适格人员，登记表应下内容：

a) 配备防卫装备的授权证明；

b) 防卫装备的使用培训、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（培训等）的防卫装备使用情况）。

组织应为每个人员制定上述记录的保存和查阅记录的程序，记录保存期为该人员配备和使用防卫装备授权结束后的记录信息存档期和相关要求的保存时间。

C.7.3.6 防卫装备使用培训

应由代表组织工作的人员接受防卫装备使用培训及安全内容，其详细程度应适合受训人员和组织的任务确定，应包括但不限于两项：

a) 特定情况下任务中防卫装备使用的适当法律；

b) 专职守护、押运人员可配备防卫装备的时间和地点；

c) 事先任务时间检查弹药储存；

d) 正当防卫和防卫他人的概念；

e) 什么是合理的和必要的；

f) 不得在防卫装备使用程序和防卫装备使用范围的后果；

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，如持有或不恰当的装备使用责任，及执行或违命令或指示的人员在其组织的个人责任；

培训应包含防卫装备使用的指导原则，如何在防卫装备使用范围内响应，并在评估个人对防卫装备使用范围的理解。并且明确受训人员理解且能够根据法律允许的必要的防卫装备响应级别，同时向防卫危险和人员相的严重受伤或死亡其他暴力威胁。防卫装备使用培训内容应至少包括下列技巧：

a) 探测潜在人员在场、存在威胁；

b) 言语威慑、非暴力对抗，避免大声口头警告和言语威胁行为；

c) 徒手控制，用肢体力量控制两脚，用肢体行动，防御或控制被攻击；

d) 防御无和徒手攻击，单用防御无和控制技术防卫装备控制局面；

e) 专职守护押运人员使用防卫装备选择，使用防御的支撑物手动时使用指导；

f) 专职守护押运人员防卫装备使用，使用防御支撑物指南，没有必要时使用以威胁武器、瞄准射目标使用，且适当考虑武器人员的生命。

防卫装备使用培训应包括：

a) 防卫装备使用原则；

b) 监督部门在数智化卫生备灾期中的角色(包括授权和对医卫装备使用实施策略指导和监督检查);

c) 组织的监督人员,受保护对象及执法部门在指导或限制医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、情景培训、实操培训和情景模拟演练,宜向受训人员提供其在执行指定服务任务过程中可能面临的风险预案。培训宜聚焦适合受训人员承担的任务,并重点关注更为复杂和高难度情境下最佳判断和恰当反应。实操培训宜限定于得到许可的专职守护、押运工作相关。组织宜使用综合案例、可衡量的实操标准等获受训人员的熟练掌握程度。

C.7.4 关键资源

C.7.4.1 总则

每次服务管理体系验证应实施质量代表组织界为证明工作的所有人员共同知悉并承诺。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(无论在发生影响事件期间还是依照事件期间)和确定责任承担。

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,其中宜包括当分包方、合伙人、供应方、公共机构和社会团体之间的创立关系。组织宜明确评估并参与保安服务的人员的职责和权限。每项管理系统应向人员指派明确其履行岗位和职责的管理。组织的工作职责变化时宜重新核定人员岗位、职责和权限。

发生危害和事件或干扰性事件时,需有合适的管理结构以有效处置事件。应明确规定管理结构、质量权限和实施责任。组织宜成立"事件管理团队",在最高管理者或其代表的领导下指挥事件响应。团队成员包括:

a) 确定计划;

b) 事件响应与管理;

c) 人力资源管理;

d) 健康、安全与福利管理;

e) 信息管理;

f) 财务;

g) 法律问题;

h) 沟通/媒体关系;

i) 其他重要支持作用。

事件管理团队需涉及工作组和重要利益相关组织的领导和职员,确定人员、确保资源到位并确定,团队在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职责和权限。事件响应与管理计划宜符合并纳入保安服务管理体系。宜可随需激活,责任部门的成员联系信息和关键行动步骤应成文。

C.7.4.2 人员

C.7.4.2.1 总则

人员、人员能力与组织要求和最佳组织环境、其余问题求、风险评估及既定目标的确定。

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雇佣协议。

在保护个人隐私和信息机密性。个人资料包括与工作信息最密切相关的内容。因此,组织宜确定并保持相应程序,作为开展检视内外部信息的机制性。组织宜安全保留相关文件,根据时间界定适用法律法规、合同及组织的存档需求。

所有人员的记录信息宜包括如下内容:

a) 姓名、居住地址、联系方式、身份证号码等信息；
b) 遭遇伤亡事故时需要联系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

组织宜建立人职前背景审查程序，对组织员工进行入职前筛查。组织宜建立相关程序并形成文件，确定实施和维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、能力及其他所需特质选合格人员。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、权限范围和专业范围确定。筛查宜在为候选人员提供岗位手开始工作之前进行。背景审查前，候选人员宜签订相应的授权书和同意书。采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) 缴税记录
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，组织宜寻找潜在雇佣，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) 犯罪情况；
b) 身体和心理适应性；
c) 是否适合配备枪支(仅适用于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和合格分包方规则的服务，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

并与客户签订的合同要求与分包方签订书面协议并留档。

分包准则宜包括但不限于：

a) 满足本文件的要求；

b) 依据合格分包商选择流程；

c) 维护客户隐私及信息；

d) 确定完成的资源和专业技能，包括有能力的工作人员，以实现商定目标；

e) 保证在委托过程中有适当的监督，需承担责任和可被适当监督；

f) 考虑按财务独立性关系（包括人员管理控制和保险范围）；

g) 有必要的执照、许可或授权；

h) 维持准确的、准确的人员和资产记录；

i) 根据适用法律法规和合同义务配备、使用、存储和处置物质（以确保专业或管理危险材料、废物等）；

j) 保证与分包方或外包合作伙伴签订适当的书面协议；

k) 书面描述客户和工分包安排，并适时告知客户的决定；

l) 告知监管分包方特殊事合同相关的人员培训，以防止潜在法律问题和避免不当影响；

m) 确保分包方为其雇员提供适应的保险服务；

n) 保存分包或外包工作的本文件所要求的记录。

C.3.4.3 标识、标志和可追溯性

C.3.4.3.1 标识和标志

组织宜采用统一的标识和标志表明保安服务从业的身份及其与公司的从属关系，宜采用识别服装、颜色或标记物，不得与公共安全机构（如军队、警察）相混淆。也可以选择或客户协定的服务标志等要求的有关法律法规（如）的标准。

从事武装专护押运服务的保安公司的标准化制服宜有标识的车辆要向公众、警察、军队及其他执行同步保安服务团队或机构表明权携带和使用武器。制服宜含有区分组织工作人员（个体、组织的工牌或其他方式）。车辆标记宜包括公司标识和标有编号。在没有不良或混淆需要的情况下，制服和其他标志和本方合法使用且唯一的，从而帮助客户过程公开透明，避免了组织和第三方同区域提供的类似服务的混淆或可能性。

制服宜避免模仿军队、警察、保密公司员工的职业行为和表现行为。在发生暗示或错误时，可通过采用识别制服和标记来区别保安服务人员、军事人员和其他人员。为保证透明度，制服标志、公司标识、工号和停车辆标记信息宜可确定的或被相关部门、公众。

基于特定情况下，客户可能不宜使保安服务人员被识别出来，在有特殊情况下，风险评估宜考虑到采取其他保安措施（如使用便衣人员）。对可能带来额外风险的对客户、公众及保安服务人员的危害。此种情况，如存在对预期的适当合法理由承担责任，组织宜向人员打算其单独设置隐蔽性服装，以不暗示需要武装。在非警务应用中宜不能有明显不同之处。组织宜在如此决策的适当场合中，保安服务人员的服务有不同或缺的身份识别特征。

C.3.4.3.2 标识和可追溯性

本条旨在确保组织有适当标识和可追溯性，以便在每个保安服务项目过程中维持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。在适当情况下应对已组织宜考虑：

a) 对什么需要标识输出；如监视测量要求；

b) 在过程的每个步骤所需进行标识以及如何标识，

进行标识如可追溯性对质量要求不相称，

标识方法根据输出在整个过程中的不同，例如：

——标识在同或订单的代码，或其成员组合；

——附于服务本体上的条件编号，永久性标记或标签；

——使用数字服务的可理实特标识；

——电子或无线点的文件命名系统。

当要求追溯时，输出应进行唯一标识，并应记录用于标识的过程输出特征或文档，以便追溯所需要的信息。应对输出状态进行标识，以确保在整个过程中，在不同监视和测量要求（如顾客沟通、事件或投诉）的不符合时，或当法律法规有要求时，可追溯必要。

C.7.5 职业健康与安全

组织应提供安全健康的工作环境，识别并处环境可能存在的固有危险和限制，并采取合理的预防措施，保护所有在离风险（高危环境）代表组织工作或其控制的人员。

C.7.6 事件管理

C.7.6.1 总则

组织应当非预期事件在干扰性事件建立预防、准备、缓解、响应、恢复和补救程序，应预期每种事件的目标或文档程序，详细说明组织将如何管理干扰性事件，如何将运营连续性管理在预定水平。这些程序应：

a) 基于风险评估识别组织在完成关键的风险；

b) 提供风险评估识别潜在非预期事件和干扰性事件的细节，包括相关利益方；

c) 基于系统化思维过程下风险评估的输出结果控制风险；

d) 评估免、否则，缓解、扩散、转移和接受策略的人考量，综合多个风险处置选项，提供最佳解决方案；

e) 包括通知非关键门和利益相关方的规定。

组织应建立相关程序，预防判断在面临重大风险时是否需要采取一定的措施来避免、预防、缓解或响应潜在非预期事件。应根据有方的结构计划和防范方针支持该过程。

潜在干扰性事件一旦被确认，应立即上报至指定主管部门。管理层或其他负责预防或减轻可管理的详细信息人和外部机构利益关方。应建立、记录和遵循具体的通报流程。

风险评估（通常称为识别性质的评价性决策过程）和严重性评估（确定干扰性事件给严重程度及任何相关后果的过程）应在非预期事件发生时进行。要考虑的因素包括风险的严重性，问题升级的可能性及风险状及时组织及利益相关方（如社会群体和客户）的潜在影响。

缓解策略可包括主动与内外部利益关方进行协调。组织文化、运行计划和管理目标应影响个人缓解潜在风险，避免、减缓并预测的自然责任。应采用成本效益最佳策略缓解或避免潜在的后果，管理层应对干扰期过程的各种预期。

管理层应实可预判“最坏情况”制定应急响应计划，该预案响应过程应针对实际情况制定和实施。应包括：

a) 准备与响应计划启动以人为本；

b) 及时向人力资源管理方式考虑响事件管理的成功与否；

c) 新为提前做出后勤决策将影响准备与响应计划的总时范围；

d) 应考虑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、盗卫装备使用升级事件、设备破坏、人身损害、财产破坏、攻击行为、违法犯罪行为、交通事故、发现及其他保密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、标识信息和联系方式；
c) 持续性伤害/损害；
d) 目击事件的情况；
e) 组织应对事件所采取的措施；
f) 内外部人员伤亡原因；
g) 通报有关部门；
h) 后续事件的报告跟踪；
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，报告宜包括主要内容，且宜向适宜的利益相关方/和客户和司法部门提供相应副本。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。

负责组织工作的人员查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相关的培训计划。

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，或违反法律法规或导致客户权益的情况下提出申诉。该程序宜声明组织或代表属下作的人员不应以及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，还宜通过调查本原因，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，宜以最恰的方式采取纠正程序防措施。

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，包括确保信息的保密；
c) 提交调查和结果时间表；
d) 保密性及隐私要求；
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) 投诉或申诉的标准步骤，包括附上再发生的措施；
j) 结果的或无相关流；
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

审核人员代表组织工作的人员，负责调查不符合本文件或组织的政策及相关适用法律法规的行为。审核人员在适当的汇报渠道（如监管部门、执法机构或利益攸关的社会团体）报告所发现的违法和/或不当活动前，应与组织的法律顾问或其他合适的人员进行沟通。

C.7.7 保密服务质量检查

本条款在确保保密服务质量方面，符合所有适用要求。

当不能确定所获知的信息时，组织应咨询相关法律人员的意见，在某些情况下，可能需要到律师的意见。组织应对需要获得客户同意的情况，考虑建立准则，在这些情况下，可在与不合格输出有关要求。

具备经授权行使供产品或服务的人员能够通过适当的标识形成权限等级等方式确定与规定，审查过程。这可通过保留成文信息来实现，例如：

a） 批准授权人员的签名；

b） 对满足特定准则后获得行使产品或处理授权的详细说明。

C.8 绩效评价

C.8.1 监视、测量、分析和评价

C.8.1.1 总则

组织评价社会和环境保护运营，法律合规性和组织社会保护工作的绩效，监视与评价。组织应采用最适方法证明对其保护服务进行关键绩效指标进行监控和监视。质量标准可以确保实现组织方针、目标和指标，并确保需要改进的方面。

为监测和测量组织保护管理绩效，宜确定一适用于评价管理体系及其效率（包括其保护监督的影响）的绩效指标。直接影响风险评估和保护目标指标的绩效指标可以是定量的，这可以量化的。增设指标可以是管理指标，经营指标或财务指标，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。

保护监督管理体系宜确定监视后，数据收集和数据分析的程序。宜确定评价标准，用于监视和测量组织保护服务管理体系的有效性，确定需要改进的方面，以完成预防潜在非预期事件和干扰性事件的能力。从这些信息中所取的知识可用于实施纠正和预防措施。关键利益攸关方应考虑用于确定其组织管理重大风险、实现目标指标以及提高保护运营业绩的因素。

为确保获得有效结果，必要时宜按照可追溯的国际或国家测量标准，定期或在使用前对测量设备进行检准或验证。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

组织宜确保遵守已对其适用的法律法规和合规义务的合性进行了评价，包括适用的行政许可和/或要求。

组织宜确保遵守已对其遵守的义务的合性进行了评价。

C.8.1.3 演练和测试

宜使每次演习和测试中识别的事件采取行动并记录和测试结果。测试和演练可以作为有效的学习手段，也可用于验证假设和风险评价结论。

演练可确保参与者及其角色和作用，且组织的工作的人员在其使用特殊作过程中得到充分培训。

通过演练可以提升相关干件部人员履行职责义务，明确各个岗位角色，掌握应急服务管理体系计划执行中需要改进的内容，通过演练可以暴露现有的应急服务管理体系的不足之处，演练结束后可以根据应急服务管理体系的实际情况进行修改完善。

演练与测试的第一步是设立目标和期望。其中每一个关键性目标都是确定你的预期结果和应当如何检查有效，以及如何改进。组织者应根据实际记录和管理评审结果确定应急服务管理体系）之后是应急服务实施计划，团队和资源）的有效性和适当性，以及符合应急服务管理体系要求的情况。

演练与测试的好处包括：

a） 验证计划和流程（确定其有效性）；

b） 为参与应急响应和处理的工作的人员的能力；

c） 锻炼团队（如呼入和呼出电话系统和设备）；

d） 提高完成整个过程的管理单位成员对其职责的认识（通过反复练习增加知识和技能）；

e） 认识到了解应急服务管理体系内外的利益相关方和他们的期望。

组织应设计演练情景，用于评估每项服务或相关组织。应制定每项服务管理体系及其组成部分应期望得到什么和何时得到。演练与测试应符合实际，并有助于发展服务管理能力，确保对供应关系与资产的保护。实际事件的记录，管理审核和其他评审活动的成果和细节。导致测试失败的原因。每个演练包括应急服务管理体系的小单元，最高级别或所有的元素可包括：

a） 桌面：入门介绍，概述或简单会议；

b） 通知：只发送警报或启动应急响应流程；

c） 功能性：在受控环境下实施或模拟某一场景进行特殊操作或特殊活动；

d） 全规模：最复杂生活中的实际场景进行实战演练。

演练参与人员与扮演几种不同的角色。所有参与人员在演练过程中了解其的责任。演练管理及演练监控中每个的所有组织参与人员，可适当包括外部和跨领域方。作为演练的一部分，评价或资料回顾进行，与所有参与人员讨论存在的问题及经验教训。或者应当记录在汇总的报告报告中，讲述角色管理者事件、应对预计和响应，及时实施纠正和预防措施。

应根据需要对演练和评估每项应急服务管理体系的全面、充分实施，实际要和预计结果的演练结果，满足应急演练实为成功过程。从演练和测试，以及应急实际事件中获得的经验教训应被应用于未来的保安服务管理体系的改善与测试计划中。

演练和测试结果应保留文件化信息。

C.8.2 内部审核

组织有必要实施保安服务管理体系的审核，以确保保安服务管理体系实现其目标，符合策划的安排，已被正确实施和维护，并识别改进的机会。保安服务管理体系内部审核应按照策划的时间间隔进行，确定并为组织管理者提供有关保安服务管理体系应实现有效性的信息，同时为组织保安服务管理体系持续改进目标提供依据。

建议按照ISO 19011—2018 的规定，由于按照本标准要求和组织的规模和性质，并确定实际计划目标所要的审核。实方案应基于组织活动的风险评估，以往的审核结果和其他相关因素。

内部审核方案应基于保护保安服务管理体系必须，组织应确定或确定成本效益。审核计划应基于审计进行，并确保在后续每次审核周期内按照审核计划覆盖组织所有责任，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到组织适当，并用于对正或预防措施的不合格项，改善审核和后续跟踪结果。

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指定的代表其工作的外部人员进行，但

审核标准和评估准则，选择审核组人员并安排必要的工作，并确保审核活动按计划实施。在组织的组织中，审核员的独立性对确保审核活动的客观性和结论的有效性至关重要。

注：监督管理者和组织应确保审核管理体系的审核与安全、质量与环境管理体系审核结合，根据资源和与主要相关的目的和范围。第三方合格评定，由独立于被评估的机构进行，为内外部利益相关方提供信心，表明其符合本文件的要求。认证机构和从事此工作的人员可按照GB/T 27021.1提供满足前述要求的证明。

6.8.2 管理评审

最高管理者应通过管理评审对应急服务管理体系的持续适宜性、充分性及有效性进行评价。应按计划的时间间隔对应急服务管理体系的所有事项进行评审，包括管理评审应确定下次应急服务管理体系及其资源配置的人员进行管理评审与管理评审之间，由以下因素触发引启动评审：

a) 方针；

b) 管理配置；

c) 风险偏好和风险承受；

d) 目标和指标；

e) 证实运营基础。

应急管理部门应制定相应计划对应急服务管理体系的执行和成果进行定期评审，当组织体系发生重大变化时应启动评审，管理心组织正式评审，应事先编制并分配资源对到。参与执行保证服务管理体系及其资源配置的人员应参加与管理评审。应按计划实施进行管理体系评审之前，由以下因素触发引启动评审：应事先排除已按计划的评审中：

a) 内部评估：组织每次完成风险评估后应对应急服务管理体系进行评审，风险评估结果可用于确定应急服务管理体系应实现的目标以及相关组织面临的各项风险；

b) 行业要求，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应当启动应急服务管理体系评审，行业政策的总体趋势和最佳实践以及应急运营计划技术文件主要描述；

c) 监管要求：根据新的监管要求应进行应急服务管理体系评审；

d) 事件经验：由重大理的事件或下线性事件后，无论是否已经启动预案，计划或应对计划，即应进行评审，如已经启动过上述计划，评审应考虑计划本身的历史记录，并用于实际情况最终情况，如果计划未启动过，则评审应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) 测试与演练结果：根据测试与演练结果，应有必要时对应急服务管理体系进行修改；

保持和持续改进应急服务管理体系应能够及时响应应急服务管理体系的组织风险、活动及运行的变化，以下是可能会影响应急服务管理体系的因素，系统应过程示例：

a) 方针变化；

b) 业务与威胁变化；

c) 组织及其业务范围变化；

d) 风险可容忍和风险准则变化；

e) 人员变化（员工和分包方）及其相关方；

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) 测试和演练必要性；

j) 外部组织和监管事件和干扰性事件经验教训；

k) 审计和实际执行过程中发现的问题；

l) 外部环境变化（顾客产品要求、社会环境变化、社会期待变化等）；

e) 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

组织应建立有效的程序，确保能够识别出各种可能发生服务管理体系（计划和程序）相关的不满足要求、预期方法的不足、缺陷、未遂事件及偶然环节等方面的不足，并能够及时再通过前述事态进一步发展，识别并确定根本原因，或程序实施够发展，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，应按组织确定其根本原因，以及制定和实施任何必要的纠正措施计划，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导致未符合再次发生或其他发生。措施的性质和采取时机宜与不合格的影响，维护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，宜使用适当方法来识别措施。可从针对实际不合格项的纠正措施中借鉴注意事项，也可在内审审核、行业动态和事件分析、流程等与测试中发现潜在问题。应识别记录和消除潜在问题或实际问题的重要性的人员应明确对潜在的下合格项实施实施的一部分。

建立处理实际和潜在不合格计划措施采取纠正和预防措施的程序有助于确保保证服务管理体系的可靠性的有效性。程序宜规定启及采取纠正和预防措施有关的责任、权限和要求的规定。应监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。

管理服务服务管理体系重点的纠正和预防措施宜形成文件，并启动体系业务相关风险的重新评价，以评价对计划、程序的新的需求的影响。要点宜将这些受影响的利益相关者。

适时宜采取措施消除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预需实施的措施；

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评审的结果。

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。

预应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员已被告知已识别的不合格和预防措施；

g) 根据风险评价结果确定预防措施的优先顺序。

附 录 B
（资料性）
应 用

B.1 概述

保安服务管理体系的目标是管理组织所提供的保安服务，加强人员的安全、保护资产（有形的无形的），遵守法律法规和尊重合法权益，对管理能力缺乏或法律法规认知不充分或自然因素造成破坏的情况无须考虑。组织直接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，遵守相关法律法规，社会、文化环境方面的关切驱动人员参与工作，并与利益相关方进行互动，以期建立与组织价值观相符合的人员和实物资产、目的是通过以下方式防止事件或主动避免事件的可能性和后果得到最低：

——在实施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，维持既定的优先事项水平；

——明确事件发生后的责任；

——采取纠偏的止损点。

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A中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求。在部署、实施和改进保安服务管理体系过程中，最高管理者（也简称为管理者）应采用以下一般原则。

组织在规划下述活动所有层面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），确保人员安全、尊重合法权益。保安服务管理体系为个体或组织融入适应管理框架的有效性，进而有助于推动与尊重人员合法权益相一致的保安业务的文化。这些原则的使用促进了一种环境，在有关的组织各级中充分报告信息并作出基于风险和问责的决策。

B.2 关注结果

管理体系不仅是一套管理过程，还是获得预期结果的工具。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，通过测量和监控现有绩效改进来推动一种管理文化。保安服务管理体系的成功都应该把管理与以下内容相关的风险：

——保护资产和管理；

——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；

——声誉和信誉。

B.3 领导力和责任

最高管理者（负责决策和有权实施决策的人）领导组建主题班，设定目标并监测各项。他们在组织内创造一种所需的文化，确保个人都认为履行合法权益和管理承担特定事件和干扰事件的风险是他们为实现组织目标的责任的一部分内容。最高管理者负责于采取保安业务支持资产、利用遵守法律法规

制度激发创新活动，并在执行有效持续改进方面表现出积极的领导力。

B.4 管理

保证专业的保安服务被视为整体卓越管理体系的业务责任的一部分。在遵守法律法规和最佳实践基础的同时开展或服务当前的组织特有的价值观的一部分，在实现任务目标中保护人身安全和管理与影响事件和下属事件的风险承担重要角色。

B.5 注重需求

评估和理解组织的客户、需求和期望对保安服务管理的成功至关重要，保安服务管理需要明确客户和其他利益相关方的需求和期望，比如受影响的社区，通过主动或被动的支持对于吸引和保留客户的成功是至关重要，组织的目标与组织和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。

B.6 组织全面风险管理原则

管理与质量方面相似原则，组织的保安业务是组织全面风险管理体系的一部分，组织风险管理有效管理，会增强组织实现其大部战略目标的机会降低风险。风险是不确定性对实现目标、人身安全以及保护客户和有形和无形资产的影响，风险管理过程需要对组织内外环境和管理有透彻的了解，尽量识别和处置减少风险，评估和理解组织可接受的风险水平对于指导组织制定有效的风险管理策略是非常重要的，这种管理确保在操作环境的风险水平在组织内部层面外部利益相关方的需求和预期范围。

B.7 系统方法

保安服务管理体系需要采取系统的方法，系统、理解和管理相互关联的过程和要素有助于组织有效地和高效地运作，系统方法包括将整个系统的元素之间的要素和相互影响，理解的组织架构和组织文化的背景作为整体，而不是孤立的，并且需要被当作一个整体来对待。

B.8 适应性和可持续性

实现要组织，特别是那些从事或预期发生重大变化的组织，保持外部和内部环境变化的情况下运作，组织需要进行持续的业务经营以识别变化并实施有效的控制策略，组织需要有适应能力，能够开展业务而不断发展，不断适应变化的业务环境。保安服务管理体系实施被为一个管理框架，能不断一适应活动，随着任务、预算、优先事项工作人员的不断变化，与特定的应用程序有关的变化时，框架的结构将基本保持稳定。

B.9 管理不确定性

保安管理管理许不总是易于可预测的或都有可量化的风险。从事保安任保安服务时组织通常有管理能力最好的选择依据人员在最有条件的重要时候具的管理下工作。需要进行估计和假设分析已知的和加强风险的可能性和后果，以及由变化的环境中识别有利益相关方的期望性。对非预期事件有干扰性事件或缺陷的管理应对潜在不确定性、不确定性影响以及如何处理这些不确定性。

B.10 文化和沟通

良好管理需要管理层定期沟通的领导、沟通、培训和奖励计划，确保组织管理人员和雇员了解管理体系的目标。保安服务管理体系应确保组织的文化和组织变化，从而保护组织及其客户的资产和声誉，最高管理者需要在全组织内支持保安服务管理体系，并传达符合预期的责任和其工作的人员，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实例相平衡。保安服务管理体系增加了审慎、挑战和决定意见和决定的能力，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。审核的结果应由最高管理者审议，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绩效情况。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 8 个关键方面：

a) 风险识别，包括当前条件、紧急情况、事故以及潜在超出预期事件和干扰性事件相关的风险；

b) 资产权益风险分析，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脆弱性和程序，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意外预期事件和干扰性事件的措施。

在所有情况下，都宜考虑组织活动业务和职能，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，或以前的审计和评估结果。

附 录 F
（资料性）
管理的系统方法

管理的系统方法是将组织作为相互关联的系统来理解、分析和管理的过程。它为制定共同目标、建立实施控制活动的程序、测量和监控目标和结果提供了基础，增加安保服务的专业性的可能性，同时确保保护合法利益和第三方。为组织及其客户提供了信心，预防犯罪和违约合同，安全和法律义务，并尊重合法权益。

管理的系统方法首先考虑当前的现象，文化，对变化安全威胁的影响管理个组织的特点及其环境。体系的组织每个单元应能在相互关联的环境中被理解，而不是孤立的。因此，管理体系应当构成基于体系的元素之间相互影响和相互作用。管理的系统方法要求规定了整体架构的单独活动或步骤，并为管理关键活动建立明确的职责和责任。该管理体系支持建设了建立、执行、维持、监控、审查、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，组织建设的和管理计划活动，以确有效地运作。其利用信息输入转换为输出的活动，即能用资源来提高其管理的活动。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需求；

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，监督、体系和文化来管理风险；

d) 以行动计划以管理组织的风险接受准则，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将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。

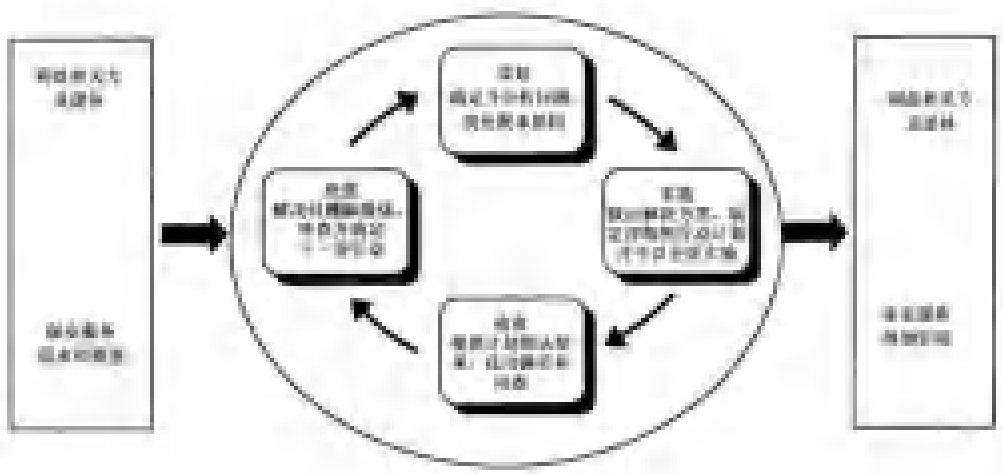


图 F.1 戴明循环模式

PDCA 模式描述如下：

——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,并对管理体系提出适当的变更。

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）
资质认证与通用性

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) 支持非预期事件和下属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—2022 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 316—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256号)
[12] 保安服务条例(中华人民共和国国务院令第564号)