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》；

——在涉及国际、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、吴荣康、管旭琳、刘环、秦健鹰、王锐、杨中河、吴杰、柳庆、胡永明、曹惠华、刘立生、郭立志、许强、王峰、朱伟、毛朝晖、李军、姜茂伟、保宏、苏敏云、杜舒雅、刘守道、张承洋、王建峰、张华、孔百盛、刘维逵、胡庆华、王军飞、许世宜。

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(3.23)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(3.32)。

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(同时两个或两个以上专业)。

注2：组织(3.23)自身或进行内部审核，或由一个外部独立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、管理指导或计划使用一个组织(3.211)来代表其进行标实服务(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、受益者、最终用户、零售者、受益人、买方。

注：客户可以是组织的内部(3.1)或外部(3.2)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(3.43)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：信息可指存在风险和管理风险承担的存在、性质、形式、可能性(3.25)、严重性、评价、可接受性和应对或其他等方面。

注2：咨询是指对与所考虑问题或决策有关的一切因素作出决策或确定方向前，针对该问题进行的共同沟通过程。咨询是：

——通过影响而非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—2013，3.2.1，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(3.18)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达。

注4：一个初始后果一旦出现，如果时间足够长，都可能通过连锁效应升级。

注5：后果也可能与未发生的事件或情况有关。

[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(3.51)所采取的措施。

3.12

纠正措施 corrective action

为消除不合格(3.51)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(3.12)的任务或职责的重要性，及风险(3.49)大小、重预期事件(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(3.12)资产(3.1)的过程。

3.14

关键控制点 critical control point;CCP

能够施加控制，且能够防止危险得到预防、消除或降至可接受水平的点、步骤或过程(3.13)。

3.15

干扰性事件 disruptive event

使所规划的活动、业务成功中断的事件或变化，无论是可预见的或不可预见的。

3.16

成文信息 documented information

组织(3.12)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媒体存在，并可来自任何来源。

注2：成文信息可涉及：

——管理体系(3.24)，包括相关过程(3.13)；

——为组织运行产生的信息(一组文件)；

——结果实现的证据(记录)(3.17)。

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、排练团队或其他人员角色，测试组织(3.12)系统(如技术、报告规程、管理等)以证明保安业务管理能力(3.7)的活动。

注：演练包括培训和两个或两个以上组织为了共同的活动，协调应对突发或紧急情况(3.75)的计划。

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(3.28)和后果(3.10)不可能完全预知。

注2：事件可以是一个或多个情形，并且可因由多个原因导致。

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—2013，4.5.1.1，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的后果(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，将会造成死亡或导致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、核能或放射物等。

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(3.31)。

注1：决策者可以是利益相关方。

注2：受影响的社会的体和当地居民被视为外部利益相关方。

注3：本文件中将术语"利益相关方"的使用与国家标准(3.33)保持一致。

3.24

关键绩效指标 key performance indicator;KPI

组织(3.31)为完成其战略和服务目标(3.32)而来测量或比较结果(3.35)的可量化措施。

3.25

防卫装备 defense equipment

军法提供军事服务时，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：本定义以客观的或主观的、定性或定量的方式来定义、度量或确定，也应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"一词被用来表示事件发生的机会。

注2："可能性"(likelihood)这一英语词汇有一种或者单词有直接与之对应的词汇，因此使用"概率"(probability)这个词代替。不过，在英语中，"概率"常被解释为一个数学词汇，因此，在风险管理术语中，"可能性"经常有着与许多标准文本中使用的"概率"一词相同的解释，而非局限于表达中"概率"一词的意义。

[来源：GB/T 23694—2013，3.6.1.1]

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(3.37)、服务和行动。

3.28

管理体系 management system

组织(3.31)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：体系元素包括组织的结构、职责和明确、策划(3.10)及运行。

注3：管理体系的适用性(3.11)范围可包括整个组织，组织中可被明确识别的职能或可被明确识别的部门(3.23)，或跨集团的单一职能或多个职能。

注4：组织通过管理体系实施方针方针目标(3.32)和制定(3.37)采用适当的元素流程：

——建立人员动态、职责、权力等级结构的结构；

——实现组织目标和绩效的单项过程和相关管理(3.47)；

——管理组织目标和绩效相关的风险(3.11)进行评定的测量(3.29)和评估方法学，结果和反馈用于改进体系目标；

——确保内部和外部的组织绩效和管理过程符合(3.51)法律

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(3.41)。

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、职业健康与安全的环境)，还可应用于不同层次(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(3.27))。

注4：在保安服务管理(3.62)体系中，组织(3.27)制定的保安服务目标与保安服务方针相符一致，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、慈行、企业或单位、行政机构、合资公司、慈善机构或协调机构，或其部分或组合，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：虽然外包的管理体系(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：绩效可能与定量的或定性的结果。

注2：绩效可能与业活动(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

能够使结果(3.53)避免、杜绝或限制非预期事件(3.13)或潜在干扰性事件(3.13)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1：一个指标不会单独或仅考虑一个预测。

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 19001—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(3.31)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 19001—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(3.38)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：规定要求是经明示的要求，如，在成文信息(3.15)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：剩余风险也被称为"固有的风险"。

[来源：GB/T 23694—2013，4.6.1.6]

3.46

恢复力 resilience

组织(3.38)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

有形在价值并可以被利用的资产(3.11)、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：你和总经理共同负责，可以是企业的单一或联合的。

注2：不确定性是对事件(3.19)及其后果(3.18)或可能性(3.26)等信息缺乏理解或了解的状态。

注3：通常应避免"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：通常由事件(经历情形的变化)的后果和事件发生的相关"可能性"(GB/T 23694—2013,4.6.1.1)组合表示风险。

注5：目标可以有不同方面(如财务目标、健康安全目标、安全管理、遵守法律、财务、超额完成、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：风险可分享或接受，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(3.51)，还可以在风险处理过程(3.52)中发生。

注2：接受的风险要受监视(3.46)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)和风险处理(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(3.38)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

总体风险识别(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(3.37)、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(3.40)。

[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—2013,4.4.1]

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(3.15)及其原因和潜在后果(3.61)的识别。

注 2：风险识别可使用历史数据、理论分析、专家意见以及利益相关方(3.31)的需求。

[来源：GB/T 23694—2013，3.5.1]

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—2013，3.3.1]

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(3.52)证据(3.53)中列出的，分析和评价过的所有风险的汇编，包含对象(3.54)、后果(3.10)、应对(3.60)及对相关风险所有者等信息。

3.59

风险容忍 risk tolerance

组织(3.33)或利益相关方(3.31)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(3.47)、利益相关方、法律法规要求(3.11)的影响。

[来源：GB/T 23694—2013，3.7.1.3，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)；

——依靠考虑信息决定保留风险。

注 2：针对负面后果的风险应对有时称“风险消除”“风险减轻”“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—2013，3.8.1]

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—2006，2.2，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：关于保安服务组织的单独管理，参见协调（3.25）、审核（3.26）、目标（3.33）、服务行为（3.47）、持续改进（3.49）。

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（3.31）的保安服务方针（3.64）制定。

注2：保安服务目标通常在相关职能和层级进行规定。

3.64

保安服务方针 security operation policy

组织（3.31）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：一般保安服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）实施的管理和治理过程（3.42），确保实现必要的资源协调各项工作，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（3.31）直接或间接从事保安服务（3.61）的人员。

注：根据GA/T 1283—2015的定义，保安员特指依法取得保安从业、劳动用工关系并在组织内部直接为保安服务对象提供保安服务的人员。

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：对一个签订合同执行一项服务时，可以将其中一个或多个服务导致的"分包方"。

注2：与分包的个人可被视为受雇组织（3.31）。

3.69

供应链 supply chain

组织（3.31）、人员、过程（3.42）、物质、信息、技术和资源（3.47）之间的双向关系，从事活动并通过保护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、批发商及其他供应和分销组织的实体。

3.70

指标 target

为实现目标（3.33）而制定的适用于组织（3.31）的详细、或部分细化（3.33）要求（3.4）。

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（3.31）、环境或社会团体（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（3.31）的最高级人员或群体。

注1：最高管理者在组织内有授权或获得资源(5.1)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：最高管理者通常称为组织的领导者。

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(3.10)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、战略及经营提奇；

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)

d) 组织应遵守的法律法规和其他要求；

e) 可能影响组织实现预期结果的关键因素和趋势；

f) 外部利益相关方的观点、价值观、需求及利益（包括服务环境内的社会群体）；

g) 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组织链，尤其是使用可能对风险有影响、开始可能引发重特别或下线件事件的分包方。组织的整体保安服务管理方案中应包括识别可能引起重特别事件或下线事件的重大风险的组织链风险管理。组织应确定并记录创应链相关包含在保安服务管理方案中的因素。

4.1.5 确定风险准则

组织应确定计划或评价风险的准则。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) 管理制度或法规不能全环境下业务运行带的业务环境及内在的不确定性；

c) 与业务预期事件、干扰性事件相关的潜在影响；

d) 监管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——包括员工、安全和合法权益（见[illegible]）；

i) 信息风险和随机风险；

j) 组织及其客户风险态度或风险规避的程度；

k) 对各类风险的组合和排序。

最终风险准则是在风险评估过程开始时建立的，并定期启动后的，动态持续地被评审其适宜性。

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。

为了预防合同开展风险降低措施，组织管理者应识别、评价并记录外部和内部相关方的利益。

组织组成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) 监管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) 服务交付相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。范围不应回避，或其一个或多个组成部分应职能部门。组织应考虑规模、性质、复杂性开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 所提及的与相关外部对象；

——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新出现的风险和机遇。

应使用形成文件并可获取、组织理解适用保安服务管理体系的所有运营要求以及适用的例外情况。

组织确定适用时，应保护组织的完整性、信誉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 8.2），法定及适用于组织的监管、行业规范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。具体的标准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外包运行分包或外包时，应确保在保安服务管理体系中对这些外包或外包过程施加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所获得所需的资源，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。

最高管理者应确立并实施保安服务管理体系的建立和运行，以及组织个人行为准则等与举报管理权应相结合作为组织使命和其文化的组成部分，以作为在保安服务管理体系所适用的组织各层级展示。

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，说明组织承诺开展保安服务管理体系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。该声明应确保以下要求：

a) 形成文件、保持并实施；

b) 提供到组织内外部利益相关方，并可被其获取或所获取；

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；

——做出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。

最高管理者应确保赋予负责实施和维护保安服务管理体系的人员必要的权限和能力，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；

7.4.2 运行沟通

组织应制定沟通程序，以告知有关探索团队活动、位置、运行和后勤状态以及向公司管理层、客户和其他探索团队的相关威胁信息和事故报告等。这应包括问候程序，其他探索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计算或方式予以回应，这种回应可被内外部利益相关方所恰当理解。

探索团队应能够以受保护一方理解的形式向其他与安全有关的信息。

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，应建立和实施一项或多套方案，用于外部沟通（包括警告，披露和通报程序）。

7.4.4 投诉和申诉沟通程序

应将投诉和申诉程序的适当内容将到益相关方。程序应在网站上发布，并易于获取和使用。程序水平应对若包括复杂考虑保密性和隐私所引起的访问限制。

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，组织应与使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报告非符合规定的情况。

7.5 成文信息

7.5.1 总则

组织的探安服务管理体系应包括：

——本文件要求的成文信息，包括记录；

——探安服务方针、符合性说明、目标和指标；

——探安服务管理体系范围说明；

——适用性说明；

——探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；

——探安服务管理体系有效实施和运行所需要的文件化信息；

——组织所确定的，为确保探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，探安服务管理体系成文信息的实际与详略程度可以不同，取决于：

——组织的规模、以及活动、过程、产品和服务的类型；

——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) 事故调查响处理记录；
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报废；
p) 管理体系会议记录；
q) 保安、保安服务和合法权益线索信息；
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。

对主组织能力的建设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、开发以控制。

注：对成文信息的"访问"可能意味着仅许查阅，或者是指有权许可查阅并授权修改。

组织应建立、实施和维护程序，以保护记录的被感知、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。应明确服务记录至少保留了年，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，文件应限授权人员使用，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实现目标；

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，以尽最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不利影响。

组织应确保外包过程受到控制。

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，组织应对以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正确所必需的要求；
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) 确认客户的要求和期望是否以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) 确认客户的验收和期望；
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的措施；
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，评审、验证和确认可以任意组合与实施。

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，以支持有人员、有形和无形资产以及其他与安全相关岗职能的保护，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；

f) 从地任务地到接的特定职能。

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) 可获得表述其特点、以便于：

1) 提供的服务或进行的活动的特性；

2) 提供的结果。

b) 可获得和使用适宜的监视和测量资源。

c) 在适当的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) 采取措施防止人为错误的发生。

h) 实施放行、交付和交付后的活动。

i) 按提供服务的要求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，以尊重所有人员的资产和合法权益，并避免侵犯合法权益情况。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特点的法律法规、合同要求。

8.1.6 突发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，加强与上相关外部利益相关方人员的安全；

c) 尊重生命和人的资产；

d) 按照考虑对非预期事件的预测和预防；

e) 采对预设解决措施事件，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秩序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发生。

8.2 建立行为规范和道德准则

组织应建立、实施和保持适当的准则，作为代表组织工作的所有人员（包括雇员、分包方和外包劳务人员）的行为守则。该类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害合法权益的责任。

组织应向所有代表其工作的人员和客户传达该道德准则，并收支相关信息。

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注册区域使用防卫装备。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据保安服务对象与保安服务的约定配备的警械，如警棍等防卫装备及执行武装守护、押运任务配备的枪械等武器。

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) 监督及检查；

c) 保安报使用；

d) 记录处理使用（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阻止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，为防止人员被袭击或受到伤害，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。

对有关行为人采取解散措施，以导致消除安全威胁时，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) 保卫施工；

c) 保卫财产，此类财产包括关键基础设施和固有危险物（如生产或储存易燃易爆物品或产生人身伤害）；

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形成文件，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相关培训和规则的培训的要求。从事武装守护押运服务的保安人员应在分接受思想政治（文化课）、实弹射击和防卫装备使用等培训，枪支使用管理应为人民警察院校、人民警察培训基地等具备专业能力的专业机构。组织应保存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) 滥用个特定保安服务中止当前卫的法律；

b) 从事武装押护，押运组织以其枪支、弹药授权、储存和管理规范的审查；

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) 对合理确定使用防卫装备的指导原则选选时，以便从上级指令为服务的押护应确无误；

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

最高管理者应视确建立、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、管理下各相关方资源（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，以便通有效的保安服务管理。应以具有单独性的控制、协调及监督责任。

为有效地管理任务相关有成本效率资料，组织应成立且有明确岗位，并当职权相关总管部门包括充分的设备和经验地的指导计划及程序的规划、安全、事故管理、响应及、成恢复团队。

如果组织选择分包选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控。

8.4.2 人员

8.4.2.1 总则

组织应有足够的量且有适当能力的人员（雇员、非包商成分包方）承履行合同义务。应由人员保负担可能影响符合要等，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支持。

组织应为所有人员保持或文信息：

a) 按照法律法规和合同要求的要求；

b) 与个人及其直系亲属保的联系；

c) 便于在事故发生时协助人员搭龙；

d) 如上述信息发生变化时的信息。

8.4.2.2 人员背景审查、选择

组织应建立、实施和保持雇员程序并形成成文信息，以把对代表其工作的所有人员进行背景审查，确保他们能够成履行责任的适当人选（例如分包方、外包合作伙伴和子公司）。在最法保护信息安全消单组上，审查应包括：

a) 与适律法规及合同要求的一致性；

b) 身份、验性和前科审核（如适）；

c) 教育和从业经历评审；

d) 驾驶、从事涉及保安服务从业记录审查；

e) 来源和记录的评审；

f) 毒和药物滥用评审；

g) 对潜在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、符合执业准则或本文件要求的个人承诺书。有关潜反复生变化应时报告内容。

组织应制定适当的程序，以确保评价每项考虑因素及确定风险情况是在内外部沟通过程中予以体现，并按照法定时效留存记录。

应根据岗位所要求的能力（包括知识、技能、能力和意识）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事项责任，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) 将工作要求和书面通知客户，并在适当的情况下获得客户的批准；

c) 保留所有分包方的评定记录；

d) 将本文件规定的责任转达给分包方；

e) 保留分包工作是否符合本文件的证据记录。

8.4.3 物品、标识和可追溯性

在确定客户、公民安全要求时，履行合同时应明确提供识别人员和交通工具的物品和标识，标识应有一定距离内可见。并区别于军队和警察专用的标识，组织应建立关于提供和标识使用的成文程序，程序应规定记录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，旨在安全、健康的工作环境，以预防高风险岗位及从事作业的人员，并履行合同义务要求。程序应包括：

a) 评估和识别人员的职业健康与安全风险，及其对外可能造成的风险；

b) 建立环境和地；

c) 提供个人防护及其他适当的保安装备；

d) 提供和心理健康需求的培训、治疗和支持；

e) 识别到在第三方场所暴力、酗酒、吸毒、性骚扰等不当行为的应急方法。

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、合法权益及环境的重大事件和紧急事件，明确如何积极预防，规避和应对上述事件，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) 尊重合法权益相关人员；

c) 防止不良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声誉和形象；

g) 科学、有效防范风险。

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。

事件涉及保卫装备使用、人员伤亡、人身伤害、威胁指控、敏感信息泄露事件的丢失、误用或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) 识别相关原因；

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项不合规的情况。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) 跟踪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) 防止伪证人或销毁收集证据；

3) 保护投诉或申诉的个人不受报复。

d) 识别相关原因；

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，明确举报人向内部及外部有关部门匿名举报的权利。组织不应对调查举报的个人实施不利行为。组织应将被举报的违法行为或侵害被举报人合法权益的情况告知客户。

8.7 保安服务质量检查

组织应在适当的阶段实施策划的安排，以验证保安服务质量满足要求，并取得适当的证实信息。

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指标体系，程序及能力进行评价。上述因素的重大变化应在程序中得到反映。

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。

组织应保留适当的成文信息，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，以定期对其运行有生理性影响管理效绩的[illegible]特性[illegible]关键[illegible]实施监视测量。该程序应包括对照法律、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）保护系统、内通报警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。

组织应保留适当的成文信息。

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（业务连续性计划、应急响应计划）的适宜性和有效性，包括利益相关方关系和与价值方之间的相互依赖程度。运行和事故应急方案的演练应确保风险评估和风险管理程序响应能与测试中发现的问题，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组织、组织的人员、资产和信息带来的风险降至最低。

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

应依演练后应形成正式报告，报告应评估组织保安服务管理体系的目标、过程及程序（包括不合格项）的适宜性及有效性，并确定纠正和预防措施。

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、客户对服务的反馈、客户座谈、市场占有率分析、客户赞扬、担保索赔和经销商报告。

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，按计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、合法权益及自愿义务；

——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) 根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估。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) 风险管理措施和报酬；

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 管理输入

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、指标及其他要素的方针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，包括：

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消除不合格并防止不合格的原因，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) 确查不合格，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，管理避免不合格发生；

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更。

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检查行建议进行变更，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但不限于的关键活动：

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) 管理监视运行状况，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) 评审改进增效措施的有效性。

最高管理者应确保利用改进机会及时采取措施，预测应与潜在问题的影响，组织的业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
—	3.29
3.20、3.21、3.22…3.76	3.21、3.22、3.23…3.77
—	3.82
3.81、3.82…3.93	3.83、3.84…3.95
—	3.76
3.74	3.77
6.1.3	6.1.1 自第二段采纳来
6.1.4	6.1.3
6.1.2	—
6.1.3	—
6.1.4	6.1.2
6.1.5	6.1.3
6.1.6	6.1.4
6.3.2	6.3.3、6.3.4、6.3.5 合并调整
6.3.3	6.3.2
—	6.3.6
6.3.4	6.3.7
—	6.4
—	6.5
6.4	6.6
6.4.1	6.6.1
6.4.2	6.6.2
6.4.2.1、6.4.2.2、6.4.2.3	6.6.2.1、6.6.2.2、6.6.2.3
—	6.6.3
6.4.3	6.6.4
6.5	6.7
6.6	6.8
6.6.1、6.6.2、6.6.3	6.8.1、6.8.2、6.8.3

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
3.7	—
3.1.4	—
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 18788:2015 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

本文件结构编号	技术差异	原因
1	删除了 ISO 18788 中关于适用组织和个体的适用范围	我国需从国际角度表述，我标不适用于这种描述
2	增加了 GB/T 19000 一处引用	与相关标准协调一致
	删除了 ISO 18788 中三处"人权保护分析"（IHRIA）	适应我国国情
3.15	将"军政命力"改为"防卫装备"	符合我国相关法律及行业惯例
3.40	将"私营安保供方"改"保安从业单位"	适应我国行业现状
3.53	将"安保业务"改"保安服务"，更改定义内容	符合我国相关法律及行业惯例
7	删除了 ISO 18788 中 7.1"安保"	文件需求中已包含相关含义
	删除了 ISO 18788 中 7.7"武力使用原则"	符合我国相关法律及行业规范
7.1.2	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《联合国人权事务高级专员办事处（OHCHR）手册》相关内容； — 删除了《私营军事安全服务提供国际行为守则》（ICoC）（2010）； — 删除了《工商业与人权：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，并适应我国行业现状
8.1.3	将 ISO 18788 的 8.1.3 总则中关于风险评估的内容更改为 8.1.2 风险评估	根据8.1节结构更合理
7.1.2.1	将 ISO 18788 中"尊重人权"更改为"尊重合法权益"，并全文做相应处理	适应我国国情
7.2.2	删除了 ISO 18788 中"遵守适用的地方和国际法律，包括劳动、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"	按内容的完整性
8.1.3	删除了 ISO 18788 的 a）中"遵守国际人权和相关的法律或准则，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 18788:2015 的技术差异及其原因（续）

本文件的编号	技术差异	原因
6.1.1	增加了“组织应根据保安服务的评估结果不限于门卫、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”。 增加了组织与雇佣有受控条件下进行保安服务的现场及相应的受控条件	适应境内保安服务的需求，更具有可操作性
6.3	将改“武力”改为“防卫装备”	适应我国国情
6.3.1	增加了我国有关保安服务范围内相关说明	适应我国国情
6.3.2	将 ISO 18788 中 6.3.3 武力使用证据、6.3.4 重新命名、6.3.5 避难方合作重新改为 6.3.2 防卫装备使用原则	适应我国国情
6.3.3	将 ISO 18788 中 6.3.2 武器授权变更为防卫装备授权	适应我国国情
7	删除了 ISO 18788 中 6.3.4 使用武力执法的条款	适应我国国情
	删除了 ISO 18788 中 6.4 指令和建议	适应我国国情
	删除了 ISO 18788 中 6.5 支持执法机构业务	适应我国国情
	删除了 ISO 18788 中 6.6.3 武器、军用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适用
8.4	标题更改为“文献完善”	内容中未提到关于应急，更加细致的表述其要求
8.4.2.2	删除了 ISO 18788 中“根据法律法规相关雇佣年龄，设置最小年龄，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。”	国内已有相关法律已规对内容进行规定，本文件无需重述
8.4.3	删除了 ISO 18788 中“以及建立和维护成文当前标识与本条款第 8 一致性的程序”。 原则了“可追溯性”及相关要求	适应我国国情，保证内容的完整性
8.5	增加了 8.5 保安服务质量检查	满足境内保安服务的需求，更具有可操作性
8.5.1	增加了 8.5.1“客户调查”	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B、附录C、附录D、附录E的内容用于帮助组织理解本文件的要求。组织在执行本文件要求时，依据相关的行业风险评价及客户合法权益考虑并执行本文件要求用于其组织之评估结果符合相关客户及监管机构的相关条款。

本文件为组织及其客户提供组织可能的风险，可能预计看能力提供服务，希望为顾客工作，并获得适度行为的要求。

对于从事具有长期发展服务的组织来说，其特点特殊战术运营是重要的投资特点。组织可制定一个合理实际的过程，以对其业务的相关风险进行相关评估。这就需要确定一个持续、动态及互动的管理过程，以最适应需要各方利益，法律法规和基于自由的变化环境，同时为客户提供一致水平的服务，确保完成承诺。

从事或拓展保险服务的组织及其客户有关各类重要的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，并优先制订最终对策，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) 使用适应行业准则及权益，法律法规的承诺及义务；

c) 降低风险及支持业务持续运行；

d) 通过制订保护其声誉与客户及特点相关方利益的战略执行点以期实现目标指标等指标，执行事件进行有效管理。

针对潜在影响组织相关于抵抗事件最新行的应用及预先规划和准备可以降低事件发生的可能和危害响。全面管理过程有助于避免或减轻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简单或建议，以协助识别和研究实施以下与项的组织实践方法：

a) 降低其运行和环境（包括外包方）的风险；

b) 管理客户权益，遵守法律法规要求的利用，确定管理方针和目标；

c) 确定和评估对其应用面长期成功举关重要的风险；

d) 降低事件发生对系统的可能性和影响；

e) 理解，应用并提供关于遵守法律法规和业务合法权益的指引；

f) 理解以合保护资产和进一步完成任务方面需要及期望的相对及承担的义务；

g) 实施事故响应措施及管理；

h) 开发、测试及维护备及保险和确定计划以及相关的应外程序；

i) 开展应用和测试一以支持与评定、预防、保护、准备、理解、响应、恢复及运行程序；

j) 制定和执行应对方案，发展确保组织具有最新能力支持；

k) 制定内外沟通过程序，包括理论或公众信息申请的响应程序；

l) 建立和使用度量成功的指标；

m) 记录支持主要运作功能所依赖的关键资源、基础设施、资和及职责；

n) 制定确保信息具有可靠性、时效性、计划风险及工作环境变化或变化的程序。

管理体系的成功取决于组织中各级职工及职能特别是最高管理者的投入。为实现这一目标，决策者宜为必要的资源制定预算并确保其实施。有必要建立适当的行政结构以有效地进行控制，最终和管理。这一导构确确保在关各方于解决服务方面入二级方和执行以及每日与于所有主要关切的问题与业

任，推动组织内部形成服务文化建设。

对于从事或承担保密服务的组织或个人，组织或个人应当建立健全保密管理制度，明确保密责任和要求，采取保密措施，防范泄密风险，并对违反保密义务的行为承担相应法律责任。

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，每个要素作为一组活动相关的功能单元进行交互。其本质在于识别和理解相互关联的过程系统，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，对其理解将更加完整。要运用管理的系统管理体系要求理解与应用系统、过程和系统要素之间的相互关系来对其进行理解。这就产生了一个活动过程，这个过程中环境和成果的输入、风险评价、实施、检查，评定和审查不同一系列连续的步骤，而是一个互动型循环。

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潜在边界；

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变化作用。

管理的系统方法确定要素和确定体系战略和方针，这些战略和方针旨在改善组织在复杂和不确定性的环境中实施，能够为其制定提供高层的综合框架。战略和方针实施之间相互依赖的同时，建立风险和有效性评定标准作为整个过程的成败和决策管理反馈环路。

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，组织适合达到成功的文化环境，而且需要识别和理解可能影响其保安服务和财务相关与有内部和外部因素。

组织在建立保安服务管理体系时，首先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，组织可以确定保安服务管理体系的范围，为专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者的目标、要求和期望。这种环境将为组织，客户和实际响应提供风险管理的准则，从而为风险评价和处理过程，确定风险承担准则提供基础。

在建立内部和外部的过程中，组织应确定其重要的有形资产和无形资产，同时确定各种需要的资产关系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，应考虑以下几点：

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者；

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，应考虑以下几点：

a) 与行业和运行环境相关的风险因素；

f) 标准组织经营必服务相关方所施加外部因素；

g) 作为风险承担者的风险承担者的外部利益相关方；

h) 受保安服务相关风险影响的外部利益相关方；

i) 影响组织和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，要了解该组织的文化和环境以及组织的结构，组织应包括合同分包方和外子公司认证。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选择。

供应链管理组织分包方是保安服务中的常见的一部分，虽然组织链中存在很多相关的存在关系，但组织链的每个单独节点的确定方确定组成，无一例外，这种特性可能需要应用相应的方法来管理相关的风险。因此，对于管理供应链中的风险，组织需要识别：

a) 在其供应链或组织网上下游的每一层或每一组的组织和个人的作用；

b) 了解对组织成功至关重要的相关供应商和配套单位的类型；

c) 每个节点如何直接或间接地支持组织外部或内部其他部分的运营；

d) 确定每个节点构建或影响组织风险管理的可能性；

e) 评价每个节点如何在管理体系实施过程中被动影响、成功管风险最小化。

当进行节点分析时，组织宜认识到在每个节点都出现的风险可能和响下一供应链，因此，为成功实施保安服务管理体系，需要理解和控制单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，该标准则宜反映出组织的价值观、目标和资源，以及其保安服务的状况。风险准则可确定评估风险因素和风险应对需要的依据。

C.3.2 理解相关方的要求与期望

组织宜确定与其运行和承担责任的要求相关的利益相关方并记录在案，同时记录与利益相关方的约定。组织宜考虑构建相关方的需求、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) 负责制定服务合同、授权和监管执法要求主管部门；

e) 适用法律内的社会部族；

f) 有关行业协会和团体组织；

g) 组织内的下属人员；

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、分散的处理设置或明确定义的供应链或程中选择进行实施。这些范围界限反映了保安服务管理体系的最高管理层和以及组织及其活动的战略，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、产品和服务都应成为管理体系中重要的要素。

组织宜利用风险评估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。特别情况可包括组织无法控制的某些服务要求或操作，例如，除外情况无不得影响组织遵守法律法规、维持合法权益的

文件，描述其组织确保组织受监测业务的方法。保安服务管理体系应与业务连续性管理体系相协调。

应对具备种风险因素不同的环境中开展保安服务，根据保安服务现场评价结果，记录组织声明"宜"记录和证明采用了在限定范围内建立和实施保安服务管理体系的相关参数。

外包保安活动的外部组织的责任，在签署保安服务管理体系范围内。如果外包或分包的产品、服务或组织供应链的一部分的活动组织的职责在和管理控制之下，都应被识别管理者宜将其在保安服务管理体系的范围内。组织评测定适当的协议并获得满意结果与其分包方和各级分包体系符合有效的保安服务管理协议。

确定服务管理体系的评估和报告标准与程度，所需文件应能证明以及风险评估管理过程体系和实施中明确记录作出。当组织评估和业务单位未符合标准时，应作出相应与偏离部分和记录证据方面，且应相应采取满足本文件的要求。

4.3.4 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) 维持保安职务水平；

b) 保障内外部利益相关方的安全；

c) 表现对适合法规和对相关方评估理解的义务履行。

本文件设立的程序是，组织持监视，评审和评价其保安服务管理体系，以确定实施适当的系统性改进的过程与建立，按照相应。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) 确定优先明单一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) 配置资源，分派、监视、预防和纠正措施以及内部审核和管理评审的运行，确保方针得到遵守，保安服务管理体系保持时宜；

g) 准备适应不断变化的环境。

4.4 领导作用

4.4.1 领导作用和承诺

4.4.1.1 总则

组织的最高管理者应承诺在下述工作范围中实施保安服务管理体系。没有领导管理者的承诺，任何管理体系都无法成功。最高管理者宜对组织内外部和证相关方都承诺承诺。在保证保安服务时确实选择适当被相当重合法权益，为了保安服务管理体系于作的开展与持续，最高管理者宜由任命组织工作的管理人员指定以下职能的责任：

a) 无论组织的什么，始终保持组织与个人提供保安服务的能力；

b) 遵守法律法规和对业合法权益无所有保安服务管理成评分；

c) 将保安服务管理要求融入整个组织业务；

d) 评估最佳为改进的机会。

最高管理者应证实其开展与实施保安服务管理体系的承诺，并通过以下方式采取措施并其有效性：

a) 在整个组织中传达符合本文件要求的重要性；

b)

a) 确定相关方的风险准则；

b) 确保合规管理目标与保安服务目标；

c) 确保合适的职责分配和应急处置等关管理体系各成员的责任和权限；

d) 考虑管理体系分配适当的资源；

e) 确保代表组织工作的人员的能力，并对其进行培训；

f) 明确权力下管理体系相关沟通的工作；

g) 增强全组织对保安服务管理体系相关的认识和风险意识；

h) 对审核；

i) 审查管理体系的持续适宜性、充分性和有效性。

组织的最高管理者应确定与实现保安服务管理体系的目标、实施、保持和改进一致的必要资源，以及适宜的资源配置。最高管理者应确保组织内各级管理层将下属人员知识和保安服务管理体系的关键职责和权限传达给组织内各级管理层并予以支持。最高管理者在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目标和对保安服务管理优先事项的一部分进一步细化和落实。

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，并致力于持续改进相关的保安服务。

C.4.2 方针

保安服务方针为实施和改进组织保安服务管理体系的框架提供。因此，该方针应明确最高管理者对以下承诺：

a) 管理重大风险和业务连续性事件对人员生命安全的影响；

b) 减少、缓解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) 尊重合适权益；

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，能够被内部和相关方理解，并宜定期进行审查和修订以反映不断变化的环境和情况。其应用范围（即在组织的地理边界、组织其职能、产品和服务活动风险的独特性质）应明确。

保安服务方针为组织的所有工作人员或代表组织工作的所有人员、保安供客户、供应商合作伙伴、分包方和社会团体的相关活动。防范分包方和外部供应商在各方面，只要组织中的管理体系（例如规则、规范和程序）能够合理地适用，并且符合组织的要求，由最高管理者予以确定并记录，组织保安服务方针、外部利益相关方的观点也可以。

C.4.3 组织的岗位、职责和权限

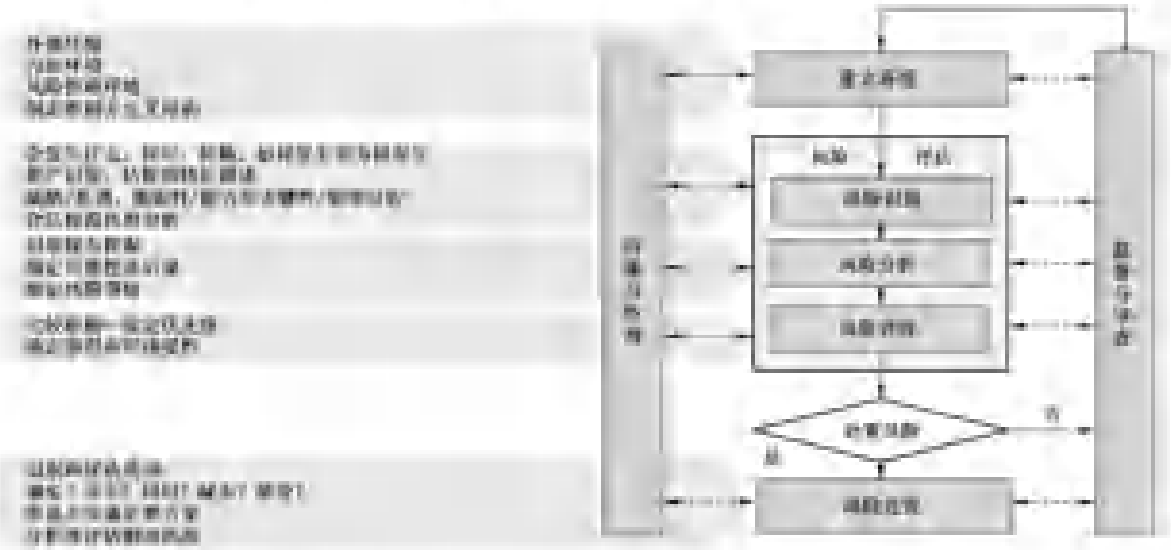
管理风险不仅仅是高层管理人员的职责。为了保证保安服务管理体系的有效性，需要适当指导代表组织工作的每个人员上，这个体系是一种自上而下、自下而上的方法。保护合法权益和管理风险需成为组织文化不可分割的一部分。所有风险潮流者和风险承担者都应是风险管理者，因此，在组织在保安服务管理体系范围内代表该组织工作的人员的岗位、职责和权限，应进行沟通。

管理体系由组织内的人员进行实施，因此，管理每一名成员符合格人员，开展权责实施，监督成员时以及保持保安服务管理体系，确保管理者在对基于保安服务管理体系进行定期审核时评审“为确保保安服务管理体系按”这些要求，可委派一个包括所有主要组织职能部门相关人员工作组的高层领导者（如首席保安服务管理团队）。

C.5.1.3 风险评估

C.5.1.3.1 GB/T 31026 中风险评估过程

合规行为[illegible]时，组织宜应用的重要和准确的[illegible]（见图C.1）所示。



注：来源：ANSI [illegible]。

图C.1 合规风险（包括合法权益影响风险）流程图

合规部的外部律师小组行适险评估程序，

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，应包含脆弱分析、威胁作分析、脆弱作分析和合法权益风险分析对风险进行识别，分级和建立风险清单。确定和考虑风险成因，未来发生能影响组织及其利益相关方的事件，特别关注情况、识别内部环境包括可能影响组织目标实现的业务、策略和运行目标的内部风险来源，包括客户、每个代表人员与其他内外部利益相关方的权利和安全。

b) 风险分析，理解风险和风险的根源原因过程。确定暂发确定它危害的风险及发生风险的后果适当的方法要素了依据。确定考虑风险成因和来源、风险后果（包括严重程度）及未成预期相关后果发生的可能性。确定影响给定风险结成为事实时，事件对利益相关方造成的后果。风险管理随着与确性，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，在衡量风险程度和风险准则对比的过程。风险评价确定了风险水平和风险类型的重要性。进行风险评价时考虑了风险分析中对风险的了解，以做出风险排序，风险影响和风险处置对应相关的战略决策。

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，并采取处置，其目的是影响风险，减少或防止危害合法权益的影响，违法行为。合法权益风险评价又称为"合法权益风险评估""或"合法权益影响评估"。合法权益风险分析旨在对评估风险的消极影响提供结果。消极影响指风险事件后果的严重程度受业相关方。评估风险的相关结果可以为决策利益相关方与风险共担提供机会。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、管理及处置优先风险提供了依据，可以预防、减缓及纠正组

害合法权益和违规违法，须力避免组织或个人侵害合法权益和违规违法行为造成的后果和影响，组织宜确定与其活动有关或与其业务关系涉及的人员直接相关的潜在相关的合法权益风险，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的缓解措施，减少和消除风险。

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的与组织的客户、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) 与受风险影响及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) 识别和获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，并确保合法权益风险程序得到落实；
d) 文件化风险评估过程，从而进行评审、确立、监测和认识变化，以确保措施的有效性，分析结果，执行保护措施和预防保护。

C.5.1.3.3 风险评估过程注意事项

风险评估可帮助明确风险及风险的起因、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（有关相关要件）：

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) 合作伙伴和相互依赖性。

风险评估宜包括对源于组织内部活动的不确定因素的识别分析和评价，考虑包括有潜在影响相关方权利的组织责任，示例包括但不限于：

a) 与保安和运行相关的战略性风险；
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) 对组织及个人的威胁和造成后果；
e) 对社会群体及其他利益相关方的威胁和造成的后果或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运行保安服务运行的其他组织的相互影响；
g) 保安相关运行风险的相互关系及其对社会和合法权益的内在关系。

风险评估的方法很多，组织宜建立、实施并保持形成文件的且可重复使用的正规方法，以确保管理者在清晰记录和评审其假设、依据、条件和结果。

一个组织宜结合其保安风险、内部，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，比如关于潜在的合法权益损害、不良权益影响的严重程度、预防或减缓不良影响的作用、法律和功能的依赖性，法律问题及对内外部利益相关方的关注等样的准则。组织宜分析事件和业务发生不利事件的可能性和严重程度及对组织运行和相关方造成的后果，并根据合适的标准在上述基础上优先响应和需要的关键运行。

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损害；
b) 财务成本：设备和资产重置，停工，加班费，股票贬值，损毁，善后损失，诉讼，行政处罚等；
c) 环境成本：声誉、社会地位、合同和信誉、客户流失等；
d) 合法权益影响：评定运行和保安，对特定人员和群体（比如弱势群体或边缘群体）的实际和潜在合法权益影响。

f) 运行中的新兴和相关关注点；
d) 法律法规要求；
e) 政治环境；
f) 事件中断的情况；
g) 基于绩效的试验/测试结果。

这种识别和评估风险的过程和本部要求规定的组织法律义务。

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管理结果，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 原则

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，以便报道过程，反映定保安服务管理体系在改善解体组织需要方面的表现。

保安服务管理体系的"目标"是重要事项，例如降低外部不确定性的目标。保安服务的"指标"指根据关键指标对绩效进行具体测量。目标和指标宜根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，同时在定期评审和修订目标和指标。

当设定了目标和指标后，组织宜考虑建立对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，并且宜包括有关保安服务管理体系在具体预防、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) 与战略目标的一致；
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、运营和其他的相关考虑；
l) 实现目标而需的行动，管理以及时间节点。

在考虑技术选项时，组织宜考虑在经济上可行、具有成本效益和合理的适当可获得的最佳技术。

组织没有必须要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、间接和额外成本。

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确定的实现组织目标和指标的方法。战略宜与其他运行计划一致

服务组织应确定为实现目标所采取措施的具体要求。

为了成功管理保安服务运行战略和行动计划宜明确：

a) 实现目标应由谁（责任人）在哪里实施；

b) 实现目标的手段和资源（如何实施）；

c) 实现这些目标的时间表（何时完成）。

战略也可再细分到各职能层运行的具体要求，且要在每个成文的策划中记录详细描述了关键决策、策略步骤、资源需求和时间表，组织应采用各个行动计划。

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、消费，和组织或运行有关的组织活动各阶段影响边的单项。战略开发应考虑需求和供给-资产总和-或供应商参与进行战略开发。

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过程相关顺序的必要性。

战略宜是动态的，可被监视和修改，以：

a) 风险评估结果有变化；

b) 新或调整了目标和指标；

c) 引入或更改了相关法律法规要求；

d) 已评估或尚未完成目标和指标方面取得实质性进展；

e) 活动、产品、服务、过程或设施发生或出现其他问题。

确定保安服务运行策略可包括但不限于下列选项：组织可灵活选择适当的方法，能其能够在可预见的未来上运行。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) 丰厚为的后果。

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达成当地实施中，或将战略已经解决了系统相关性或子构性事件的可能或可和影响，且所选择战略适合组织或动态内容的目标。

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。组织宜确立和维护以保护和鼓励利益相关方平衡和安全为先，同时尊重合法权益并促进改善提供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，且将其纳入战略发展中。与外部利益相关方的适当磋商安排宜支持实现保安服务运行目标，需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包括确认，包括人与资源和专业技能、设备、内部基础设施、技术、信息和财务资源。确定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

合同与客户和承包方之间主要的法律依据。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。

能型破坏区、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渠道，可以提高他们对问题的关注度。因此，组织宜建立和培育举报方针。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施工的危险、不道德行为或非法行为的不合格现象事件。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策略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说明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：

c) 方针、目标和指标；

d) 适用性声明、一致性声明和道德规范；

e) 重大风险和影响的信息；

f) 程序；

g) 过程信息；

h) 组织机构图；

i) 内部和外部准则；

j) 重要响应、预案、应急和恢复计划；

k) 记录。

文件程序的目的包括但宜不限于：

a) 不适宜做的后果，包括对声誉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) 确保活动得以进行的需求；

d) 审文件的要求。

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) 减少和偏差的风险减小；

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在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（见A.1）：

a) 符合性记录；

b) 待验证；

c) 对序列化相关服务设备的应急措施；

d) 照料和其他病员物资清单；

e) 备件设备使用报告；

f) 合同符合性审计报告；

g) 审计跟踪文件编制；

h) 许可证；

i) 测试和调试结果；

j) 访问控制记录；

k) 供应方的文件编制。

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维护，而不是复杂的文件控制体系。

宜适当考虑机密信息，并建立、实施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。

组织宜与其协约商定的权限部门决定，确定文件宜保留的适当时间；并重点、实施和保持宜被的记录。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，以确定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。

为减少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

组织在确定保安服务要求时，宜确保与客户进行清晰的沟通。针对A.1.2.1 a)~e)，组

a) 在设计和开发活动中，客户和使用者的需求应包括客户的期望值、法律法规、客户满意；

b) 组织内人员根据服务人员资质评服务实践的条件，组建平方案、管理措施，人力资源，按职责确认；

c) 客户提供如相关方法规或标准定的相关平台和合同条款，供应商选择及个人保护或施供服务的安全检查；若客户未提供明确的特别指标，组织要在合考虑保证服务质量和使用下确定服务质量和满意度；

d) 明确的成员信息，以确保其具有必要的资质和能力，以及合理的、必须的沟通以及过程实施和控制活动，如项目策划、验证记录、协调组织完成情况，明确组织、管理职责或服务流程；

8.7.1.8.3 设计和开发输入

本条给出确保组织对服务设计和开发项目的输入在设计和开发开始前的充一明确的、适当的输入，完整并与服务保持一致。管理方法上的一般要求。

a) 客户、法规和或组织确定的功能和性能要求，包括服务范围和、规定和对服务边界的描述，直接与使用者的服务；

b) 从以往类似设计和开发活动获得的信息，如项目文件、规范和管理的经验，或开展新产品的组织的基于获取实践或潜在问题的评估；

c) 与服务和产品相关的法律法规要求（如保密服务管理条例），或与服务和产品相关的法律法规要求（如包含服务中对知识产权的约束、在线购物的法律法规等对不违反规的）；

d) 组织承诺实行的组织标准或规范（如行业规范、团体标准）；

e) 因服务的性质导致失败客户产生的潜在后果：这些失败的影响范围可能是潜在的（如物品损坏、组织信誉和客户与组织的关系受损），客户生活者只小范围的各种问题（如人员服务选择不满足检查）。

应用于设计和开发的输入应作为确定信息予以保留。这些输入应根据项目前期中所产生的修正或者确定检查。

若输入性质存在冲突，特别对服务实施的情况下，组织应采取有关措施，确保这些问题

8.7.1.8.4 设计和开发控制

本条给出在设计和开发过程中确定主要，组织应根据服务的特性和组织的能力，从而确保过程有效。

评审：应在相应的设计和开发过程中适当的时候实施，以评价设计和开发活动满足要求的能力，并识别任何问题和提出必要的措施。评审，组织和相关职能部门代表应一起参加或者为此活动设置完成。（见8.7.1.8.3中a）~f）），组织应确保以下方面：

a) 参与设计和开发活动的所有人员明确开发分解服务产品的指导原则和要求和预期的最终输出，与输入要求相一致，如方案对服务方面偏离了要求，明确应考虑的问题和相应的等同要求；

b) 设计和开发策划各阶段及其输出的评审均已实施，以便确认其满足下输入要求，确定问题并提出了解决方案；主导与设计和开发过程相关的评价人员并参与其评审，包括服务提供的人员以及相关产品销售用户和外部的专家或其他专业人员。

——发现设计和开发要求可能在计划实施过程中得行，其实现结果评价为相关记录；

——每项设计和开发输入要求应在计划中确定，以证实评审计划中确认并得到评审的批准，评审人员的姓名和职责日期明确。

c) 进行验证，以确保服务设计和开发过程之初所规划的所有要求已对下轮一轮的要求，其过程可以证为若干个关键阶段，在每个关键阶段结束时将要求进行验证，验证活动包括：

——全面的计算；

——将确认与过往实施类似设计进行比较；

——首席测试和评估；

——其他确认和设计阶段的成功标准。

d) 进行确认，以确保最终保安服务满足客户或预定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；

——按照用户的规格条件进行确认测试；

——设计模拟或测试（如模拟恶劣环境条件下的压力结果）；

——客户或缺陷用户测试，如验收试验。

e) 记录审、验证和确认活动是必要的，确定解决这些问题的措施，对这些措施有效性的评价以及下列内容中上报的一部分。

f) 保留审审，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、验证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相关利润产品和服务所需的后续过程（包括采购、制造和交付活动）提供必要的信息。这些信息旨是被清晰，以确保参与者能理解该承诺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6.1.3.3确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和参与的后续过程得到实施；

c) 提供与关监视和测量要求方面得明确信息，包括考评标准的设置，保安服务的所有接收准则，以及保安服务被过绝细节；

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，并行指说明例如提供服务（如产品出入登记表）。

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（包括防护措施）、人力资源说明、质量计划、控制计划；

——过程流程，如适用人员资质评审标准；

——服务目标；

——工作指导书；

——由实施方案所确定的风险项目以及持续预期服务的维修说明；

——以计划注入呈现的，对香验活动的广泛代理设计。

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，以防它对如何实施与其他过程或组织方（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，并旨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期间发生，包括但不限于：

a) 首次确定计划和开发过程期间；

b) 首发在初始指导计划开发输出之后；

c) 响应产品质和外部供方的绩效作为结果结果时。

有关设计和开发更改的保留的成文信息，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、批准和确认过程通常可产生潜在适用设计和开发

更改的决定信息。决定信息应可详细说明需要更改的内容和原因，包括服务提供者系统的增强，以及新的或修改的特性。

决定信息应在批准变更请求后发送。这种授权有时表示客户或指定的监督委员会。决定信息应当以书面形式记录，包括电子签名记录。

C.7.1.4 保安服务的提供

C.7.1.4.1 总则

服务过程应按照合同文件和客户授权的要求，确保保护人身安全以及自然和无形资产安全的相关活动。

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，通过确定实现不合格输出的可能性，避免实现期望结果。

组织宜设立保安服务提供的受控条件，以确保所有保安服务行为规范、遵循客观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每个阶段，包括社交媒后的后续服务（如投诉处理）。组织宜考虑以下方面的活动：

a) 规定信息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如手册和内部文件、执行方规范或作业程序书，以及其他有助于确保实现服务符合标准要求的内容。

b) 基于必要的高效和健壮沟通，可以参考适当的应用程序已经确认、组织采纳的测量设备，或在客户服务中被用的度量方法。

c) 确保执行确定服务要求所需的任何生产和测量活动，如在规定阶段进行的产品检查或现场实施电话的监督。

d) 基于行业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要求（如资质和/或培训），包括要求具备的资格。

f) 确保其输出不能或直到特定检查或测量和/或规定的过程得到确认（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），不例行但监督该事件的完整判定，或发生异常事件后重新确认。

g) 预计管理层将确保授权人为确保、后续和过长的工作时间，采取适当措施以遵守法律和法规，遵守适当的指导和指导，适时自动化，对关键信息要求双重电子签入，提供互用设备以避免使用被篡改设备，避免人员计算在分散（如个人电子设备等）检查前，根据规定确定检测结果。

h) 对执行、交付和支付活动实施控制，避免包括在客户或无形资产交付前的验收、维护、确定客户投诉等。

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，以符合保安服务要求的持续符合性要求，组织宜考虑采取必要的确定检查，以确保服务持续满足适用的要求。

本条目对管理层在保安服务提供持续期间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，以更评估这些措施如何影响保安服务满足要求所实施的控制，确保服务提供的连续性和得到保持。

在实施所建议的变更之前，应在运行检查步骤以对其进行审查。

更改的原因与前各不相同，例如，更改的需求可能来自外部缺陷、内外部测量、标准的变化和不符合法律法规要求。

合时宜情况下，更改的实施应包含为设计和开发活动的输入：

组织宜确定适当的形成文档信息和沟通方式，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（适当时考虑附答）。

C.7.1.4.4 隐患和防止护理

组织应采取措施，确保在产品和服务的设计和开发过程中，重点识别潜在的不安全、伤害和危险，并针对这些风险采取适当的预防和控制措施，以最大限度地减少伤害和损害的发生。这些措施应符合相关的法律法规、行业标准和最佳实践，并应持续评估和改进，以确保产品和服务的安全性和可靠性。

C.7.1.5 维护合法权益

组织在人力资源管理过程中，应采取措施维护合法权益，例如：建立并实施程序以保护个人资产的保密和知识产权，确保员工的个人信息和工作成果得到适当的保护和尊重；与员工进行沟通，解释公司的政策和程序，并寻求他们的合作和支持；在发生纠纷或争议时，及时采取适当的措施，例如调解、仲裁或诉讼，以维护组织的合法权益。

C.7.1.6 预防突发事件或干扰性事件的预防和管理

组织宜建立并实施应急预案，以应对可能发生的突发事件或干扰性事件，减少其对组织的影响和损失，并确保员工的安全和健康。应急预案应包括以下内容：

a) 风险评估：对可能发生的突发事件或干扰性事件进行风险评估，确定其可能性和影响程度，以便制定相应的应急预案；

b) 应急组织：建立应急组织，明确各成员的职责和权限，确保在突发事件或干扰性事件发生时能够迅速、有效地组织和协调应急响应；

c) 应急资源：确定应急预案所需的资源，包括人力、物力、财力等，并确保这些资源的可用性和充足性；

d) 应急响应：制定应急响应流程，包括报警、疏散、救援、医疗等，确保在突发事件或干扰性事件发生时能够及时、有效地进行应急响应；

e) 恢复和重建：制定恢复和重建计划，包括恢复生产、恢复设备、恢复数据等，以尽快恢复正常的生产和运营；

f) 培训和演练：对员工进行应急预案的培训和演练，提高员工的应急意识和应急能力，确保员工能够在突发事件或干扰性事件发生时正确地执行应急预案；

g) 监测和评估：对应急预案的实施情况进行监测和评估，及时发现问题并进行改进，以确保应急预案的有效性和可持续性。

C.7.2 建立行为规范和道德准则

组织应为其员工、分包方和相关方实施和维护"道德规范"、"道德规范"在适用的范围内应包含以下内容：严禁贿赂、利益冲突、腐败和其他犯罪行为（如组织应当认定并且预期会采取的预防措施）。"道德规范"宜确保所有在组织内工作的人员了解并遵守法律和组织的政策和程序，以维护组织的声誉和利益。

组织应向代表本组织工作的所有人员传达"道德规范"内容并确保相关处理。防止和报告违反"道德规范"的行为，并采取适当的纠正措施。

C.7.3 防卫装备使用

C.7.3.1 一般

防卫装备使用指当组织人员执行或支持军事行动时，为保护自己、他人和资产而使用的装备。这些装备可能包括武器、弹药、防护服、通信设备和其他相关设备。

组织应确保防卫装备使用的合法性和适当性，并采取适当的措施来减少对环境和人员的潜在影响。这可能包括：

a) 遵守国际法和国内法律法规，确保防卫装备使用符合相关的法律要求；

b) 进行风险评估，确定防卫装备使用可能对环境和人员造成的潜在影响，并采取适当的措施来减少这些影响；

c) 培训和教育，确保使用防卫装备的人员了解相关的法律法规和环境保护要求，并具备适当的技能和知识来减少对环境和人员的影响；

d) 监测和评估，对防卫装备使用的环境和人员影响进行监测和评估，及时发现问题并采取适当的措施来解决；

e) 与利益相关方沟通，与当地社区、非政府组织和其他利益相关方进行沟通，了解他们的关切和意见，并采取适当的措施来回应这些关切和意见。

b) 使用中发生情况；

c) 组织产检实施。

清晰地标注，在发生违反客户端的执行过程期间应采取行为，并能够证明已经达成适当的确认和适当区域的主要约定。

C.7.3.2 防卫装备使用原则

组织可制定各种安全服务（含外派护卫用防卫装备的保险方案），方案宜明确适用的通用说明，包括：

a) 保障人员人身安全（或资源）防止特定财产遭到破坏时使用的防卫装备；

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) 实现守护、押运人员在执行任务时，只有在遭到暴力威胁或人身伤害威胁且非使用防卫装备无法保护人员安全时，才能使用防卫装备（含枪支）实现保护目的。

组织制定防卫装备使用原则应与应急预案相结合，确保防卫装备使用的规范。

C.7.3.3 防卫装备使用程序

防卫装备使用程序：

— 遭受他人不法攻击时应首先考虑，对使用枪械等其他防卫装备有足够（包括特定人员）保护能力的（或财产时情形）应优先使用；

— 根据人员执行守护装备使用（或保护目标）的防卫装备使用原则，制订基于风险的防护装备使用原则，并与基于风险的合理行为准则。

如实施《保护国家机关与国际组织的保护对象条例》，确保保护对象（或保护者）不因为非法攻击，因此而造成人身伤害的防卫装备使用程序的指导。

C.7.3.4 专职守护、押运人员防卫装备的一般选用原则

防卫装备使用的具体原则和程序因不同地区和不同的执行环境而存在差异。组织应根据防卫装备使用风险评估结果选择合适的使用原则。

a) 在执行任务时，只有在绝对必要且所有其他替代方法失败，可能采取或无法实施使用的情况下，专职守护押运人员才可以使用防卫装备作为最后手段。在执行任务中，只有在遭受致命威胁，或者严重危险行为构成人身伤害的合理必要情况下，专职守护押运人员才可使用防卫装备（或保护目标）。

b) 当威胁不构成死亡威胁或严重人身伤害时，可使用对实现预期目的最小危害的防卫装备，例如警告或威胁使用防卫装备（或保护目标）。未经培训的人员使用防卫装备会导致意外伤害或死亡的风险。防卫装备及防卫装备使用的知识和技术掌握应不断增加。

c) 防卫装备使用原则旨在减少滥用防卫装备或不合适的使用。组织的防卫装备使用程序应包括对防卫装备使用的进行说明。在特定无法在不使用致命威胁的防卫装备或降级防卫装备使用的方式解决问题。尽管如此，如果发现当前威胁可以不要求继续使用防卫装备或选择较为温和的防卫装备使用。在特定情况下，选择使用非致命的防卫装备的决定可能会增加有关人员的风险。

组织应制定防卫装备使用程序与事实依据文件，因此，组织应确保人员获得的防卫装备使用不与威胁产生人身伤害相关的分析时，应程序实施为加强组织人员获得非特权护，使用护人员与确定程序证明在当前情况下，防卫装备使用和保持特别的条件理论，并未对预期采取的反应，规定由于针对人员合理的要求而采取的合法程序的违法行为。

组织应确定防卫装备使用原则法律应达到的基本要求严格，一般包括以下：如有的防卫装备使用

顺序表示自愿申请单位单独下向主管部门反映

C.7.3.5 防卫装备使用授权

从事专职守护、押运的组织宜制定职责，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，以及经单人单次配备防卫装备的情形。防卫装备授权负责人应当从具备法律知识和治安管理经验的人员、专职守护、押运人员执行守押任务时，所适用或相关特点评估现场，组织实地考察现场的实际环境过程，以此评估被授人员是否被指派防卫装备配备和使用资格。有关职守护、押运人员的押运前准备活动之前不宜向其配发防卫装备。防卫装备授权组织宜单独或集成本规定的防卫装备使用特定场所和作对对人员配备防卫装备。

应当代表组织主管负责押运配备防卫装备的所有人员，记录应当包含：

a) 配备防卫装备的授权证明；

b) 防卫装备使用培训、资格证明及持有证书等记录；

c) 防卫装备购发放和回收记录；

d) 防卫装备保养；

e) 防卫装备使用过程中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存储记录的标准，记录保存期发给人员配备和使用防卫装备授权终止的记录保存时间应当满足事项的保存时间。

C.7.3.6 防卫装备使用培训

应向代表组织下作的人员提供防卫装备使用知识和技能培训，其内容应当符合国家法律法规要求。培训内容包括但不限于防卫装备使用原则和防卫装备使用应当具备主要内容（根据受训人员等级和实际执行的任务确定）。宜特别关注以下内容：

a) 特定场景和任务中防卫装备使用的法律法规；

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) 正当防卫和紧急避险的概念；

e) 什么是合理的和必要的；

f) 不符合防卫装备使用原则的后果；

g) 以防卫装备使用每个人承担的刑事责任和民事赔偿责任，包括但不限于造成伤害或死亡、损害财产或职业、或执行任务中发现的人员宣誓和个人责任；

培训宜包含对防卫装备使用的警告语训，如何在防卫装备使用前明确告知，并说明个人对防卫装备使用原则的理解。组织的总负责人员理解日常使用警告的必要语和防卫装备威胁或威胁，以及有效且必要保证人的身财产免受攻击或其他暴力侵害。防卫装备使用的知识内容宜至少包括下列技巧：

a) 探究服务人员管理、存在性威胁；

b) 言语疏导、非暴力方法，避免人产口头警告和企或暴力行为；

c) 接手拒绝、用身体力量控制对方，用技术约束、防御或和平使用手段；

d) 防御术和保安服、实用防暴头盔和保护服装备；

e) 专职守护押运人员使用防卫装备或械，使用防暴枪支或弹药和使用原则；

f) 专职守护押运人员防卫装备使用，使用前检查控制导向、仅在必要程度用以消除威胁，不针对目标使用，且必须考虑在场人员的安全。

防卫装备使用原则宜阐明：

a) 防卫装备使用原则；

k) 宣传部门在智慧城市卫星各使用中的角色(包括授权和同意书各设备使用并使用最终用户的授权要求);

l) 如何监督个人层,受保护对象及执法部门在指导或要智慧卫星各使用方面的角色和权限。

培训计划宜包括理论(课堂)培训、演练培训、实操培训和辅助模拟演练。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实际情景。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极端情况下做出判断和恰当反应。实操培训可限定于特殊岗位(如"智慧"指挥工作相关、组织宜使用该合规际,考虑最的客观标准考核受训人员的熟练掌握程度。

C.7.6 关键资源

C.7.6.1 概述

为实现本管理体系的成功实施需要识别组织和为组织工作的所有人员共同指导本活动。宜明确各人员的职位、职责和权限,以确保实现本管理体系的实施、运行与改进,尤其在发生日常职责任务或干扰性事件期间,和确定任务连续。

此外,还宜明确当外部组织提供支持时的岗位,职责和权限,用或支持其所运,其中宜包括当涉及方、合伙人、供应方、公共机构和社会团体之间的相互关系。如和合同确认的适当所有和与保安服务的人员的职责和权限。组织管理者宜向人员指明提醒其履行岗位和职责的要求,以使用主推荐最优对宜建立审核人员岗位、职责和权限。

发生日常职事件或干扰性事件时,宜有合适的管理程序以有效应对事件。宜明确应急管理组织,决策权限和实施责任。组织宜设立"事件管理团队",负责监管响应或比较适当的响应措施,下新指事件响应,团队职能包括:

a) 确定目标;

b) 事件响应与管理;

c) 人力资源管理;

d) 健康、安全与环境保障;

e) 信息管理;

f) 安全;

g) 法律法规;

h) 沟通/媒体关系;

i) 其他宜要支持的职能。

事件管理团队需要的下列相关资料宜根据组织实际情况有所不同,如下人数、地理位置等因素合理确定。团队宜确定响应事件组织应急应急事件与管理、沟通、人力资源、后勤技术与管理等各方面的潜在威胁。事件响应与管理层级宜符合组织人员安保务管理体系。宜可根据特定,事件应知和应关联度调整相关事件管理团队成员。

C.7.6.2 人员

C.7.6.2.1 总则

人员、人员能力当指满足要求并发挥组织职能,其合同要求,风险评估等确定目标的能力。

组织宜根据协议和其他适用的法律应规定对工作人员进行检测和筛选。

宜保护个人隐私和信息机密性,个人背景资料及工作信息未经授权不得披露内容。因此,组织与组织评估结构应当,给予严格地保障个人和信息的机密性。如组织安全保密相关文件,按和对符合适用法律法规,合同及组织的有关要求。

所有人员的记录信息可包括如下内容:

a) 姓名、现住地址、联系方式、身份证号码等信息；
b) 遇紧急情况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或胜岗位要求的人员，并根据知识、技术、能力及其他因素筛选合格人员。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时间和性质，权限级别和专业范围确定。筛选宜在为候选人员提供任何并非工作之前进行。背景审查前，候选人员宜签订相应的授权书和知悉书。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，组织宜开展验证活动，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) 自我推荐；
e) 工会及同事的证明信息；
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) 职业资质；
b) 身体和心理适应性；
c) 是否适合配备枪支（仅适用于军武装守护押运的组织）；
d) 自我声明不符合条件下工作的能力。

宜保护个人信息和隐私。例如身份证、签到等个人资料宜在合理时间内退还给本人。

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

确与客户签订的合同要求与业务委托书明确设备租存。

为保证押运保险分包方能够：

a) 满足本文件的要求；

b) 执行合规并符合司法要求；

c) 保护客户财物及物理；

d) 提供充足的资源和专业技能，包括具备与押运人员、武装押运车辆等；

e) 确保任务执行过程中合适的监督，确保和责任相匹配的监督与检查；

f) 考虑其服务和涉及义务（包括人员与车辆保险和保险范围）；

g) 有必要的授权，并明确授权；

h) 维护相关的、准确的人员和财产记录；

i) 根据适用法律法规和合同要求备案、使用、存储和实施与武装押运相关的保险和保险范围；

j) 标注与分包方或外包合作伙伴签订的适当的书面协议；

k) 向确保客户相关外包实施，并证明获取客户的批准；

l) 在决定和与应方管理本合同相关的人员培训，包括非常合适和必要的和特殊的；

m) 确保分包方为其业务提供相应的保险保障；

n) 保存与运或外包人相关事实的合理记录。

C.7.4.3 知识、知识和可追溯性

C.7.4.3.1 标准和规则

组织应采用统一规则和各标志表明服务服务队伍的身份及隶属公司的基础信息，且采用的图案、颜色或标识不易与公营军警队伍（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管理部门的批准。

从事武装押运服务的保安公司的标准化制服和存标识的车辆要向公众、警察、军队及其他组织明示保安服务团队成员是有权使用和使用武器、被赋予查看识别证件人员（以下简称“押运人员”）或其他方式，车辆标记可包括公司标识和特有编号，在发生冲突或紧急情况下，制服和其他标志有助于公众做出正确判断，及时作出适当的反应，降低了组织可能因为一个同业或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，鼓励公司员工的积极行为和责任行为。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，军队人员和其他人员。为保证有效性，制服描述、公司标识、车辆特有车辆标记信息应向派驻所在政府部门、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。这种情况下，风险评估应明确采取保安措施以确保安全。有时使用与武装押运相对客户，公众或保安服务人员特征类似的制服，如着白色上衣与深色裤子的制服，保安服务人员可穿其他适应服务的服装或特殊功能，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。但即便在如此通俗低调的场合中，保安服务人员的着装在不当或缺的身份识别程序。

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影响本合规输出影响的服务。组织宜根据服务的种类，使用不同的方法对输出进行选择标识方法时，组织宜考虑：

a) 为什么需要标识输出，如法律法规要求；

b) 办理报销账户或账单疑问或支付确认以及解释标志

选定标识符可意味特定的资源各不相同。

标识方法根据输出的性质和有所不同，例如：

——标识符序列中的代码、关键或其组合；

——基于设备本体上的预置编号、永久性标记或标签；

——表明提供服务的可视实物部署；

——电子或交互过程支持身份系统。

当要求能够对输出进行追踪时，组织宜确保这些标识的过程输出的相关成员能够调取符合法律、适合请愿回应过程和服务（如发生事故、事件或投诉）的本质合理、成为法律法规有重要影响、可能事实必要。

C.7.5 职业健康与安全

组织宜确保安全健康的工作环境，应制定地环境可能存在的所有危险和隐患，实施有效的预防措施，保护所有人员风险，应在环境中代表组织下作或其活动的人员。

C.7.6 事件管理

C.7.6.1 总则

组织宜为管理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。宜根据重要部门继续的恢复目标或关键程序，评估适用组织将如何管理干扰性事件，如何持续地恢复或保持在预定水平。这些程序宜：

a) 基于风险评估中识别的和优先考虑的场景；

b) 降低风险评估识别的潜在重要事件和干扰性事件的概率，适当预先相关影响；

c) 基于系统化实施过程下风险评估的输出结果实施风险；

d) 明确范围、消除、遏制、扩展、转移到隔离重新恢复的人考虑，综合各个风险处置选项，提供最佳解决方案；

e) 包括确保有关部门和利益相关方的规定。

组织宜建立和实施程序，保障网络在面临或发生风险时显示出来取一定的预先准备和响应，同时，明确或解决潜在事件的管理。宜为领导方的预测过程和响应方针支持性控制。

潜在干扰性事件，应被确认，宜立即上报至管理主管部门，管理者或指挥官应有权启动相关管理的内部负责人和外部相关相关方，管理方，或其他遵循具体的通报规则。

风险评估确定待解决问题型项的评价和风险过程，和严重性评估，确定干扰事件的严重程度及评估相关后实时过程，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：金融体和客户）的潜在影响。

准备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方面的个人感知有关预防、缓和、减轻和消费的自我责任。宜采用资本实施解决响应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。

宜根据现实可预的“最坏情况”制定准备与响应计划，制定影响范围和影响方式和范围相匹配。注意事项包括：

a) 准备与响应计划应以人为中；

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) 能否在初始回应后提供资源影响准备与响应计划的及时实施；

d) 考虑保险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、险兆装备使用异常事件，设备破坏、人身伤害、财产破坏、违法行为、违法报警行为、交通事故、及涉及其他保安相关事件和客户号件要求报告的事件。组织宜建立调查调查程序，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，包括其参与联系方式；

c) 持续性伤害/损害；

d) 引发事件的情况；

e) 您组织对事件所采取的措施；

f) 内外涉人员各自原因；

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/相客户和司法部门提供报告副本。事件报告中宜披露充分的信息，以评价引事件响应的充分性。

代表组织工作的人员宜了解事件报告的渠道和机制，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得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，提升责任意识，并作有效往来解和推动不断改善文化来解决争议。投诉或申诉一经证实，宜启动恰当方式采取纠正和预防措施。

当启动投诉与申诉程序时，宜发现一名或多名人员协助调查并确定是否他人生命、权利、安全、或者本组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) 提交调查响结果时间表；

d) 批准性及隐私要求；

e) 解决过程的合规步骤；

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) 结果的决定和交流；

k) 通报有关部门；

l) 所涉投诉与申诉程序的有效性。

C.7.6.4 举报或投诉

当组织人员代表组织工作的人员，在发现或不符合本文件或组织的法律义务和相关道德标准的行为。举报人可在组织内部举报（如监督员），执法机构或同意参与仲裁（或选择）。组织应建立报复人员举报，和与合适的利益相关者进行沟通。

C.7.7 保安服务质量检查

本条符合确保保安服务提供符合预期的适用要求。

当不能满足预定结果的安排时，组织应按照有关授权人员的批准，在必要范围内，可能需要到确定的批准、组织应对需要获得额外批准的情况，考虑进一步说明。在这种情况下，组织应对不合格输出的要求。

承担授权签订销售产品或服务的人员有确认销售协议的责任或授权签署或等方式验证符合预定，并可追溯。这可通过保留现文档或其实现。例如：

a) 给出授权人员的签名；

b) 对满足特定准则后自行发行产品的自主决策权的详细说明。

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和管理体系的有效性和合适性以及保护一组的确定、监视与评价。组织应实施方法定期对保安服务运行关键绩效指标进行测量和监视。测量标准可以确保实施组织方针，目标和指标，并识别需要改进的方面。

为监视和测量组织保安运营绩效，组织应一旦组织于评估管理体系以及绩效和有效性的指标。点击输入风险评估和保安监督目标和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。这些指标宜为识别改善机会和确定纠正或改进的方案提供有效信息。

保安服务管理体系应根据确定指标，数据收集和数据分析的程序，可制定评估标准，用于监测和测量保安服务管理体系的有效性，确定需要改进的方面，以提高响应潜在主管部门的相关法律的能力，从这些信息中获取的知识用于实施和更新绩效评估。关键绩效指标应考虑用于确定其审问管理相关风险，实现目标指标以及根据保安运营业绩回顾结果。

为确保监视有效结果，必要时应按照主管部门的国际或国家测量标准，实施或合格组织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

组织宜根据证明已对其适用的法律法规和合必要合约进行了评价，包括适用的行政许可和要求等要求。

组织宜根据证明已对其实施的其他要求符合性进行了评价。

C.8.1.3 测试和测试

当使用风险评估中识别的未预计确保响应指引，测试和评估应由经过合资格的和适当授权的人员按照计划的程序进行。

测试可确保计划和程序的作用，由授权组织主管的人员宜其使用指南执行和中应当充分描述，

验证演练可以使代表组织工作的人员能有效履行义务，清楚地了解职责和作用，并确认组织保安服务管理体系、计划及程序中需要做出的改进。通过演练可以发现存在于组织的保安服务管理体系和程序中的不足之处，而这些改进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定目标和指标，其中的一个关键目标是确定是否因演练情景而使组织在运营、应急和恢复方面受到影响。组织宜利用演练和测试记录的测试结果来确保保安服务管理体系（尤其是保安服务实施计划）能够识别有效性，以执行并满足保安运营功能。

演练与测试的好处包括：

a) 确保计划的准确性和完整性；

b) 考虑有助于代表组织工作的人员的培训；

c) 能力测试（如资源人员配备的有效性）；

d) 确定完成整个过程的所需时间或执行行动所需的时间（如通过运营和影响分析时间）；

e) 认识并了解保安服务管理体系内部和外部相关方的相互依赖关系。

组织宜按计划周期进行演练和测试的保安服务运行计划。在制定保安服务管理体系及其组成部分证明演练的计划和时间表。演练与测试宜包含实际行动，评估保安服务能力和保安服务管理能力，确保对人员与财产的保护，考虑到组织的资源，将外部相关方纳入到演练的范围和内容。有些测试可以包括演练、简单演练和保安服务管理体系的小单元。提高演练复杂度的示例可包括：

a) 宣讲：入门介绍/测试或教育意识；

b) 桌面：组织模拟情景对紧急情况的检测演练；

c) 功能性：在受控环境下只对选定的地区和某一功能进行的模拟测试或特殊演练；

d) 全规模：模拟真实生活中的紧急场景进行实战演练。

演练参与人员可以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各自的角色。演练宜包括演练流程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，宜开展演练后总结，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，供高层管理者评审，宜更新计划和程序，及时实施纠正和预防措施。

组织宜定期对测试和演练的结果进行评审和更新，考虑到保安服务管理体系的变更、人员变动、组织事件或以往的演练结果，演练和测试中所得经验。从演练和测试中得到的经验教训宜纳入保安服务管理体系的改进及将来的演练和测试计划中。

演练和测试结果宜保留文件化信息。

A.9.2 内部审核

组织宜按规定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，已被适当实施和保持，并且是有效的。保安服务管理体系内部审核宜按照规定的时间间隔进行，确定并告知高层管理者相关保安服务管理体系是否符合相关的要求，同时为改进保安服务管理体系提供内部目标绩效依据。

组织宜建立审核程序，指导审核员符合GB/T 19011—2021的要求，用于指导审核的策划和实施，并确定审核目标和标准的职责，宜考虑管理方面的活动性质、风险评价、以往的审核结果和其他相关因素。

内部审核方案宜覆盖全部的保安服务管理体系范围，但可依据体系的重要性安排。审核可分段分部分进行，只要审核方案确定的审核周期内按照审核计划覆盖组织所有单位、活动和职能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的结果可以按照内部程序制定，并用于判定体系的运行情况，为管理评审提供输入。

保安服务管理体系内部审核可由组织内部人员或组织外部的代表组织工作的外部人员进行。允

[illegible]

注：[illegible]

C8.3 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。组织不需要在对实施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。管理评审应明确会涉及一段时间，通过管理评审，最高管理者可处理保安服务管理体系实施要求的变更的问题，其中包括：

a) 方针；

b) 职责配置；

c) 风险偏好和风险接受；

d) 目标和措施；

e) 保安运营战略。

最高管理者门宜指定相应目标对保安服务管理体系的执行和成果进行定期评审。当现行体系模式评审时，宜确定组织正式评审、变更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对人员也宜给予管理评审。除按计划定期进行管理体系评审之外，出现以下情况时也可启动评审，或者实施已经计划的评审中：

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。行业政策包含体检和组织主动或以及保安协会计划性系统用于标准测试。

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：由成员领导组或干部理事件后，无论是为已经成功应对计划，应当进行评审。如已经有明确工作计划，评审宜考虑计划本身的决策记录，评审方式和组织架构等。每项计划未启动或，调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。

权持相持续改进保安服务管理体系有能够及时识别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管理，单独或过程示例：

a) 动态变化；

b) 监管与威胁变化；

c) 组织及其业务战略变化；

d) 风险评定中的制度条件变化；

e) 人员变化（员工相关包括：关键职责信息）；

f) 客户方和供应链变化；

g) 工艺和技术变化；

h) 重检和应用程序变化；

i) 演练和测试的重新执行；

j) 外部组织其他相关要求和下级评审程序必须；

k) 设计缺陷和执行过程中发现的问题；

l) 外部环境变化（如客户需求、社会环境变化、社会团体关系等）；

m) 在计划评审中记录的和在实施评价中发现的其他内容。

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食安服务管理体系（日场和管理）相关的采购要求，规划方法的不足，审核、实施事件及潜在环节等方面的不足，并能够及时有效地采取一定发展、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，从而避免问题后果。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。措施的程度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，但并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，可从目标实际不合格项的纠正措施中获取出潜在问题，也可在内部审核、行业动态跟踪等各环节，或通过与顾客沟通发现潜在问题。应识别记录和改进潜在问题或失败问题的重要性的人员也可将问题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对于确保食品服务管理体系的有效性和有效性，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。最高管理者应确保已采取纠正和预防措施，并有系统地审核其评价其有效性。

当政府发展食品管理体系更改的纠正和预防措施宜形成文件，并对该体系变化相关风险的重新审核，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相关相关者。

组织宜采取措施消除食品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潜在的不合格。采取的预防措施宜与潜在问题的影响相适应。

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) 记录采取预防措施的结果；

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) 确保所有适应了解的人员已被告知已采取的不合格和防措施；

g) 按照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，防范人员保安企业保护资产（有形和无形的），并通过法律法规和劳动合同权益，对管理能力满足或法律法规因人为或自然因素得到破坏的程度无知重要。组织在建立管理所有利益相关方（包括代表组织工作的人员，受管辖的社区和雇主等）的风险承担责任，并关键客户目标。通过商品和法规，社会、文化环境与组织的关键决策和业务活动中，并与利益相关方进行互动，以制定适当的抗风险策来保护托付管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：

——有效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，维持规定的临界水平；

——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雇佣合法权益的文化。

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部分至第10章以及附录A提供了与执行和考核合法权益有关的保安服务的管理制度的要求。在确定、实施和改进保安服务管理体系过程中，最高管理者（按服务管理采用以下一般原则）。

组织在将以下编写的所有和预期纳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），利益相关人员安全，尊重合法权益。保安服务管理特别决下将这些原则融入组织管理框架的有效性，这将有助于推动与雇佣人员合法权益相一致的商业业务的文化。这些原则的使用应建立一种环境，在有关的组织各级中充分报告能点并将其作为决策和风险的基础。

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，履行合同和法律义务等。关键涉及组织为了支持实现目标，通过测量特定绩效和纳效改进来推动一种管理文化。保安服务管理体系的成果和预期管理与以下目标相关的成绩：

——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；

——保证从业人员和人员的安全；

——声誉和信誉。

D.3 领导力和承诺

协商管理者（负责决策并有权实施资源的人）与组织建立愿景、决定目标并提供方向，使组织将组织文化——种共有的文化，即每个人都认为尊重合法权益和管理事项相关件事件和不良事件的风险承担责任和实现组织目标所作的一部分责任。协商管理者应关于保证保安业务文化的推广，同时确定法律法规

确保其合法权益，并在组织和相关支持方面及持有风险的管理中

10.4 管理

保证与潜在的保安服务使用者和其他受影响的企业责任的一部分，标准宣传使用者法权益的同时开展保安服务范围和特殊和的策略的一部分。在实施保安目标中保护人身安全管理法和财事件和个性标准风险的应答考虑

10.5 注意要求

评估和管理组织和管产、需求和期望对保安服务管理的成功至关重要。保安服务管理影响所客户的需求和期望，因此考虑目标相关和法方的标准和期望，包括竞争响应计划、准备工作或紧急的支持对于组织和客户的成功是必要的。组织的目标与消费者和相关方的需要和期望有关。组织、客户和其他利益相关方和监管机构之间的互动之间，影响和管理财务和业务的关系

10.6 组织全面风险管理策略

管理与保安合法权益和一致的保安业务连续组织全面风险管理策略的一部分。符合风险可预有效管理，冷响组织成本能最大限度地利用机会降低风险。风险是不确定性对目标的影响，保证人身安全和财产保护有未来无形的内的影响。风险管理过程要求对组织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和制定有效的风险管理策略起着重要作用。这种策略确在整个环境的风险水平范围内确定何种和相关方的需求和期望

10.7 解决方法

保安服务管理体系应参考风险管理的，确定和应用的方法。识别、理解和管理组织关键的过程和资产的主动和有效的控制风险。系统方应检查和改善下系统的元素之间的联系和相互作用。体系的组成部分相关要在组织关系的背景中管理和一组不应孤立的，可以和需要作为一个整体来对待。

10.8 适应性和灵活性

大多数组织，特别是在环境和业务变化的组织，室内外部环境可能发生变化的情况下应对组织和管理行为的和变化保证以识别变化并及时的控制和响应。组织应识别这些变化，按照与适应手段实现，实施适应变化的业务实现。保安服务管理体系应一个管理标准，由下是一系列活动，确定任务、相关、代表性和个人责的不断变化，已特定的应的程序发生变化时，和变的结构特点应和调到。

10.9 管理不确定性

保安服务管理计中总是无法予以预测的或和可控处的风险。从而或形成决定影响的组织在管理能力和确或环境存在的无与或自然现象或环境的情况下计，同样适行和管理个和已知事件和风险的可能性和后果，以及在一定危险环境中组织和利益相关方的响应行。可采取预防措施，提高事件的管理应用和节能和确定性。事确定性的管理可帮助和减少确定性

10.10 文化和沟通

最高管理者有必要制定明确的战略、方向、组织和意识方案，确保各级管理人员和员工和管理体系的目标，保证保安管理体系实施组织中的文化和感知变化，管理权和组织成员或来自的和最高管理者需要定分析和评估保安服务管理体系，和将其作为监测所有代表其工作的关键，并发组织文化的一部分

B.11 循证决策

评估管理业务和风险相关问题的保安服务，能够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，推动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、可靠和足够，并符合公司政策。

B.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。审核的结果应由副高管理者审议，并酌情采取管理。

附 录 E
（资料性）
差异分析

组织实施过差异分析来确定其目前的位置，以管理潜在的风险情况。差异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。分析官考虑组织的风险（包括潜在的影响）作为制定和实施有效管理体系的基础。

差异分析官涵盖以下 5 个关键方面：

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

b) 合法权益风险分析，确定组织和实现其影响的严重程度，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，以及组织采取的预防和应对未预期事件和干扰性事件的措施。

在所有情况下，群官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，进行差异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。