ISO 28000-2022

国际标准

ISO/TS
28000

第2版
2022-03-15

安全与韧性 安全管理体系 要求

Security and resilience —
Security management systems — Requirements

目次

前言

国际标准化组织（ISO）是由各国标准化团体（ISO成员团体）组成的世界性的联合会。制定国际标准工作通常由ISO的技术委员会完成。各成员团体若对某技术委员会确定的项目感兴趣，均有权参加该委员会的工作。与ISO保持联系的各国际组织（官方的或非官方的）也可参加有关工作。ISO与国际电工委员会（IEC）在电工技术标准化方面保持密切合作的关系。

制定本标准及其后续标准维护的程序在ISO/IEC指引 第1部分均有描述。应特别注意用于各不同类别ISO文件批准准则。本标准根据ISO/IEC导则第2部分的规则起草（见www.iso.org/directives）。

本标准中的某些内容有可能涉及一些专利权问题，对此应引起注意。ISO不负责识别任何这样的专利权问题。在标准制定期间识别的专利权细节将出现在引言/或收到的ISO专利权声明清单中（www.iso.org/patents）。

ISO与合格评定相关的特定术语和表述含义的解释以及ISO遵循的世界贸易组织（WTO）贸易技术壁垒（TBT）原则相关信息访问以下URLL：www.iso.org/iso/foreword.html.

本标准由ISO/TC 292安全与韧性分委员会制定。

第二版取消并取代了第一版（ISO 28000:2007），第一版在技术上进行了修订，但保留了现有的要求，为使用前一版的组织提供连续性。主要变化如下：

——在第 4 章中加入了关于原则的建议，以便与 ISO31000 更好地协调；

——在第 8 章中增加了建议，以便与 ISO22301 更好地保持一致，促进整合，包括：

- 安全策略、程序、过程和应对；
- 安全计划。

有关本标准的任何反馈应直接向用户所在国家标准机构提出，这些机构的完整名单可以www.iso.org/members.html中找到。

引言

大多数组织正经历着安全环境中越来越多的不确定性和波动性。因此，他们面临着影响其目标的安全问题，他们希望在其管理体系内系统地解决这些问题。正式的安全管理方法可以直接增进组织的业务能力和可信度。

本标准规定了安全管理体系要求，包括对供应链安全保证至关重要的方面。它要求组织：

——评估其运营的安全环境，包括其供应链(包括依赖关系和相互依存关系)；

——确定是否有足够的安全措施来有效管理与安全相关的风险；

——管理组织对法律法规和自愿义务的遵守情况；

——协调安全过程和控制，包括供应链的相关上游和下游过程和控制，以满足组织的目标。

安全管理与业务管理的许多方面相关联。它们包括组织控制或影响的所有活动(包括但不限于对供应链产生影响的活动)。应考虑对组织安全管理有影响的所有活动、职能和业务，包括(但不限于)其供应链。

关于供应链，必须考虑到供应链本质上是动态的。因此，一些管理多个供应链的组织可能希望其供方满足相关的安全标准，作为纳入该供应链的条件，以满足安全管理的要求。

本标准将策划-实施-检查-处置(PDCA)模式应用于组织策划、建立、实施、运行、监视、评审、保持和持续改进安全管理体系的有效性，见表1和图1。

表1：PDCA模型的解释

策划(建立)	建立与改进安全相关的安全方针、目标、指标、控制措施、过程和程序，以提供符合组织总方针和目标的结果。
实施(执行和运行)	执行和运行安全方针、控制措施、过程和程序。
检查(监视和评审)	根据安全方针和目标监视和评审绩效，向管理层报告结果以供评审，并确定和授权补救和改进措施。
处置(保持和改进)	根据管理评审的结果，通过采取纠正措施，保持和改进安全管理体系，并重新评价安全管理体系的范围和安全方针和目标。

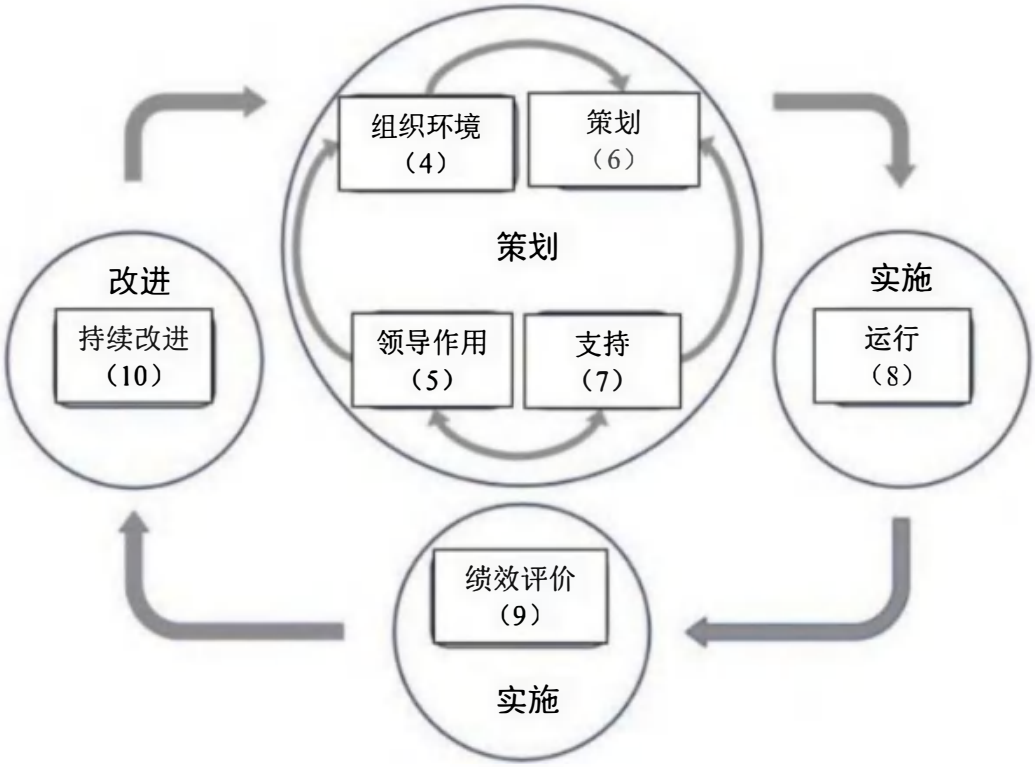

图1：应用于安全管理体系的PDCA模式

这确保了与其他管理体系标准的一致性，如ISO 9001、ISO 14001、ISO 22301、ISO/IEC 27001、ISO 45001等，从而支持与相关管理体系的一致和整合实施和运行。

对于有此愿望的组织，可以通过外部或内部审核程序来验证安全管理体系与本标准的一致性。

安全与韧性—安全管理体系—要求

1 范围

本标准规定了安全管理体系要求，包括与供应链相关的方面。

本标准适用于所有类型和规模的组织（如商业企业、政府或其他公共机构和非营利组织），旨在建立、实施、保持和改进安全管理体系。它提供了一个整体的、共同的方法，并不针对具体行业或部门。

本标准可以在组织整个生命周期中使用，并可应用于任何层级的内部或外部活动。

2 规范性引用文件

下列文件对于本标准的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本标准。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本标准。

ISO 22300 安全与韧性——术语

3 术语和定义

ISO 22300 界定的以及下列术语和定义适用于本标准。

ISO 和 IEC 在以下地址维护用于标准化的术语数据库：

ISO 在线浏览平台：https://www.iso.org/obr

IEC 在线电工术语库：http://www.electropedia.org/

3.1

组织 organization

为实现目标，由职责、权限和相互关系构成自身功能的一个人或一组人。

注：组织包括但不限于企事业单位、政府机构、社团、个体工商户，或者上述组织的某部分或其组合，无论其是否为法人组织、公有或私有。

3.2

相关方（利益相关方） interested party; stakeholder

可影响或者受到决策或活动所影响，或者自认为受决策或活动影响的个人或组织。

示例：相关方可包括顾客、游客、居民、社区、供方、监管部门、非政府组织、投资方和工作人员。

3.3

最高管理者 top management

在最高层指挥和控制组织的一个人或一组人。

注1 :在保留对安全管理体系)承担最终责任的前提下，最高管理者有权在组织内授权和提供资源。

注 2 :若管理体系的范围仅覆盖组织的一部分，则最高管理者是指那些指挥和控制该部分的人员。

3.4

管理体系 management system

组织用于建立方针和目标以及实现这些目标的过程的一组相互关联或相互作用的要素。

注1 : 一个管理体系可针对单个或多个领域。

注 2 : 体系要素包括组织的结构、岗位和职责、策划、运行、绩效评价和改进。

注 3 : 管理体系的范围可包括：整个组织，组织中具体且可识别的职能或部门，或者跨组织的一个或多个职能。

3.5

安全管理体系 safety management system

用于建立和实现安全方针和目标的管理体系或管理体系的一部分。

3.6

方针 policy

由组织最高管理者正式表述的组织的意图和方向。

3.7

目标 objective

要实现的结果。

注1 :目标可以是战略性的、战术性的或运行层面的。

注 2 : 目标可涉及不同领域(如财务的、健康安全的和环境的目标),并可应用于不同层面(如战略层面、组织整体层面、项目层面、产品和过程层面)。

注 3 :目标可按其他方式来表述，例如：按预期结果、意图、追求、目的、运行准则来表述目标。

注 4 : 安全目标，是由组织设定的，与安全方针一致的，与安全相关的目标。

3.8

风险 risk

不确定因素对目标的影响。

注1:影响是指对预期的偏离——正面的或负面的。

注 2 : 不确定性是指对事件及其后果或可能性缺乏甚至部分缺乏相关信息、理解或知识的状态。

注 3 : 通常，风险以潜在事件和后果，或两者的组合来描述其特性。

注 4 : 通常，风险以某事件 (包括情况的变化)的后果及其发生的可能性的组合来表述。

注 5 :本标准中风险指安全风险。

3.9

过程 process

利用输入实现预期结果的相互关联或相互作用的一组活动。

注：过程的“预期结果”称为输出，还是称为产品)或服务，随相关语境而定。

3.10

能力 competence

应用知识和技能实现预期结果的本领。

3.11

成文信息 documented information

组织需要控制并保持的信息及其载体。

注1：成文信息可以任何格式和载体存在，并可来自任何来源。

注2：成文信息可涉及：

——管理体系，包括相关过程；

——为组织运行而产生的信息(一组文件)；

——实现结果的证据(记录)。

3.12

绩效 performance

可测量的结果。

可量化的结果。

注1：绩效可能涉及定量或定性的发现。结果可由定量或定性的方法来确定或评价。

注2：绩效可能涉及活动、过程、产品、服务、体系或组织(3.1)的管理。

3.13

持续改进 continual improvement

提高绩效的循环活动。

注1：提高绩效涉及使用安全管理体系以实现与安全方针(3.11)和安全目标)相一致的整体安全绩 效的改进。

注2：持续并不意味着不间断，因此活动不必同时在所有领域发生。

3.14

有效性 effectiveness

完成策划的活动并得到策划的结果的程度。

3.15

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”是指组织和相关方的惯例或一般做法，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(3.8.6)中阐明。

3.16

符合 conformity

满足要求。

3.17

不符合 nonconformity

未满足要求 。

3.18

纠正措施 corrective action

为消除不合格的原因并防止再发生所采取的措施。

3.19

审核 audit

为获得审核证据并对其进行客观评价，以确定满足审核准则的程度所进行的系统的、独立的和文件化的过程。

注1：审核可以是内部(第一方)审核或外部(第二方或第三方)审核，也可以是一种结合(结合两个或多个领域)的审核。

注2：内部审核由组织自行实施或由外部方代表其实施。

注3：“审核证据”和“审核准则”的定义见GB/T 19011。

3.20

测量 measurement

确定数值的过程。

3.21

监视 monitoring

确定体系、过程或活动的手段和过程。

注：为了确定状态，可能需要检查、监督或批判地观察。

4 组织环境

4.1 理解组织及其环境

组织应确定与其宗旨相关并影响其实现安全管理体系预期结果的内部和外部因素，包括其供应链的要求。

4.2 理解相关方的需求和期望

4.2.1 总则

组织应确定：

——与安全管理体系有关的相关方；

——这些有关的相关方的要求；

——这些需求中哪些将通过安全管理体系来解决。

4.2.2 法律法规和其他要求

组织应：

a) 实施和保持一个程序，以确定、获取和评估与其安全有关的适用法律、法规和其他要求；

b) 确保在实施和保持其安全管理体系时考虑到这些适用的法律法规和其他要求；

c) 将这些信息形成文件并保持更新；

d) 适当时将此信息传达给相关方。

4.2.3 原则

4.2.3.1 总则

组织中安全管理的目的是创造价值，特别是保护价值。

组织应采用图2中给出的原则，并在4.2.3.2至4.2.3.9条款中描述。

图2：原则

4.2.3.2 领导作用

各级领导应建立统一的目标和方向。他们应创造条件，使组织的战略、方针、过程和资源协调一致，以实现其目标。

4.2.3.3 基于现有最佳信息的结构化和全面性的程序方法

包括供应链在内的结构化和全面性的安全管理方法应有助于取得一致和可比较的结果，只有将活动作为相互关联的连贯系统进行运行的过程来管理时，才能更加有效和高效地得到结果。

4.2.3.4 定制化

安全管理体系应是定制的，并与组织的外部和内部环境和需求要适应。安全管理体系应与其目标有关。

4.2.3.5 包容的人员积极参与

组织应适当地、及时地让相关方参与进来。它应适当考虑他们的知识、观点和看法，以提高对安全管理的认识并促进知情的安全管理。组织应确保所有层级的人都得到尊重和参与。

4.2.3.6 整合方法

安全管理是所有组织活动的有机组成部分。它应与组织的所有其他管理系统相整合。

组织的风险管理（无论是正式的、非正式的还是直观的）都应被整合至安全管理体系中。

4.2.3.7 动态和持续改进

组织应持续关注通过学习和经验进行改进，以保持绩效水平，对变化做出反应，并随着组织的外部和内部环境的变化创造新的机会。

4.2.3.8 考虑人和文化因素

人的行为和文化对安全管理各方面都有很大影响，应在每个层次和阶段都考虑到。决策应基于对数据和信息的分析和评价，以确保决策更加客观，对决策有信心，更有可能产生预期的结果。应考虑每个人的看法。

4.2.3.9 关系管理

为了持续的成功，组织应管理好与所有相关方的关系，因为他们可能会影响组织的绩效。

4.3 确定安全管理体系的范围

组织应确定安全管理体系的边界和适用性，以确定其范围。

在确定范围时，组织应考虑：

——4.1 中提及的各种外部和内部因素；

——4.2 中提及的要求。

组织应将范围形成成文信息。

如果组织选择外部提供任何影响其安全管理体系符合性的过程时，组织应确保这些过程受控。此类外部提供过程的必要控制和责任应在安全管理体系中加以确定。

4.4 安全管理体系

组织应按照本标准的要求建立、实施、保持和持续改进安全管理体系，包括所需的过程及其相互作用。

5 领导作用

5.1 领导作用和承诺

最高管理者应通过以下方式证实其在安全管理体系方面的领导作用并承诺：

——确保制定安全方针和安全目标，并与组织战略方向相一致；

——确保识别和监视组织相关方的需求和期望，并及时采取适当措施来管理这些期望，以确保确保安全管理体系要求融入组织的业务过程；

——确保将安全管理体系要求求融入组织的业务流程；

——确保安全管理体系所需的资源是可获得的；

——沟通有效的安全管理和符合安全管理体系要求的重要性；

——确保安全管理体系实现其预期结果；

——确保安全管理目标、指标和方案的可行性；

——确保组织的其他部分产生的任何安全方案都能补充安全管理体系；

——指导和支持人员为安全管理体系的有效性作出贡献；

——推动组织安全管理体系的持续改进；

——支持其他相关管理者在其职责范围内发挥领导作用。

注：本标准使用的“业务”一词可广义地理解为涉及组织存在目的的核心活动。

5.2 安全方针

5.2.1 建立安全方针

最高管理者应制定安全方针，以便：

a）与组织的宗旨相适应；

b）为建立安全目标提供框架；

c）包括对满足适用要求的承诺；

d）包括对持续改进安全管理体系的承诺；

e）考虑安全方针、目标、指标、方案等可能对组织的其他方面产生的不利影响。

5.2.2 安全方针要求

安全方针应：

——与其他组织方针相一致；

——与组织整体安全风险评估相一致；

——规定在收购或与其他组织合并或在其他情况下，对其进行评审。

——组织业务范围发生变化，可能影响安全管理体系的连续性或相关性；

——描述并分配主要的责任和成果责任；

——作为成文信息而可被获取；

——在组织内予以沟通；

——适宜时，可为有关相关方所获取。

注：组织可以选择有一个详细的安全管理方针供内部使用，其中包括将提供足够的信息和指导，以推动安全管理体系（部分内容可以保密），并有一个包含广泛目标的摘要（非保密）版本，以便向其相关方传播。

5.3 岗位、职责和权限

最高管理者应确保相关岗位的职责和权限在组织内得到分配和沟通。

最高管理者应指定以下职责和权限：

a）确保安全管理体系符合本标准的要求；

b）向最高管理者报告安全管理体系的绩效。

6 策划

6.1 应对风险和机遇的措施

6.1.1 总则

在策划安全管理体系时，，组织应考虑到4.1所提及的因素和4.2所提及的要求，并确定需要应对的风险和机遇，以：

——确保安全管理体系能够实现其预期结果；

——预防或减少不利影响；

——实现持续改进。

组织应策划：

a）应对这些风险和机遇的措施；

b）如何：

——在安全管理体系过程中整合并实施这些措施；

——评价这些措施的有效性。

管理风险的目的是创造和保护价值。管理风险应融入安全管理体系。与本组织及其相关方的安全有关的风险在8.3中述及。

6.1.2 确定与安全有关的风险并确定机遇

确定与安全有关的风险以及识别和利用机遇，需要进行主动的风险评估，其中应包括考虑但不限于以下方面：

a）物理或功能故障以及恶意或犯罪行为；

b）环境、人、文化以及其他内部或外部因素，包括组织控制之外的但能影响组织安全的因素；

c）安全设备的设计、安装、维护和更换；

d）组织的信息、数据、知识和通信管理；

e）与安全威胁和漏洞有关的信息；

f）供方之间的相互依存关系。

6.1.3 应对与安全有关的风险和利用机遇

对已确定的安全相关风险的评价应提供以下投入（但不限于此）：

a）组织的整体风险管理；

b）风险应对；

c）安全管理目标；

d）安全管理过程；

e）安全管理体系的设计、规范和实施；

f）确定足够的资源，包括人员配置；

g）确定培训需求和所需的能力水平。

6.2 安全目标及其实现的策划

6.2.1 建立安全目标

组织应在相关的职能和层次上建立安全目标。

安全目标应：

a）与安全方针保持一致；

b）是可测量的（如可行）；

c）考虑到适用的要求；

d）予以监视；

e）予以沟通；

f）适时更新；

g）作为成文信息提供。

6.2.2 确定安全目标

在计划如何实现其安全目标时，组织应确定：

—— 要做什么；

—— 需要什么资源；

—— 由谁负责；

—— 何时完成；

—— 如何评价结果。

在建立和评审其安全目标时，组织应考虑到：

a）技术、人力、管理和其他选择；

b）相关方的意见和影响。

安全目标应与组织对持续改进的承诺相一致。

6.3 变更的策划

当组织确定需要对质量管理体系进行变更时，包括第10章中所确定的变更，变更应按所策划的方式实施。

组织应考虑：

a）变更目的及其潜在后果；

b）安全管理体系的完整性；

c）资源的可获得性；

d）职责和权限的分配或再分配。

7 支持

7.1 资源

组织应确定并提供所需的资源，以建立、实施、保持和持续改进质量管理体系。

7.2 能力

组织应：

——确定在其控制下从事影响其安全绩效的工作的人员所需具备的能力；

——确保这些人员基于适当的教育、培训或经验是能胜任的，必要时获得适当的安全许可；

——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。

7.3 意识

在组织控制下从事工作的人应知晓：

——安全方针；

——他们对安全管理体系的有效性的贡献，包括改进安全绩效的益处；

——不符合安全管理体系要求的后果；

他们在实现遵守安全管理方针和程序以及安全管理体系要求方面的作用和职责，包括应急准备和响应要求。

7.4 沟通

组织应确定与安全管理体系相关的内部和外部沟通，包括：

——沟通什么；

——何时沟通；

——与谁沟通；

——如何沟通：

——在沟通之前，对信息的敏感性进行评估。

7.5 成文信息

7.5.1 总则

组织的安全管理体系应包括：

a) 本标准所要求的成文信息；

b) 组织所确定的、为确保安全管理体系有效性所需的成文信息。

成文信息应说明实现安全管理目标和指标的职责和权限，包括实现这些目标和指标的手段和时限。

注：安全管理体系的成文信息的范围可能因人而异。

注：对于不同组织，质量管理体系成文信息的多少与详略程度可以不同，取决于：

——组织的规模，以及活动、过程、产品和服务的类型；

——过程及其相互作用的复杂程度；

——人员的能力。

组织应确定信息的价值，并确定所需的完整性水平和安全控制，以防止未经授权的访问。

7.5.2 创建和更新

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，以保持适宜性和充分性。

7.5.3 成文信息的控制

应控制安全管理体系和本标准所要求的成文信息，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）；

c）定期评审，必要时进行修订，并由授权人员批准其适当性；

d）过时的文件、数据和信息被迅速从所有发放点和使用点删除，或以其他方式保证不被非预期使用；

e）为法律或知识保存目的或两者而保留的档案文件、数据和信息得到适当的识别。

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。

对于组织所确定的策划和运行安全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：对于成文信息的“访问”可能意味着仅允许查阅或者意味着允许查阅和并授权修改。

8 运行

8.1 运行的策划和控制

组织应策划、实施和控制满足要求所需的过程，并实施第6章确定的措施，具体方法是：

——建立过程准则；

——按照准则实施过程控制。

组织应保留必要的成文信息，确保过程已按策划得到实施。

8.2 确定过程和活动

组织应确定那些为实现以下目标所必需的过程和活动：

a）遵守其安全方针；

b）遵守法律法规和监管的安全要求；

c）其安全管理目标；

d）其安全管理体系的交付；

e）供应链所需的安全水平。

8.3 风险评估和应对

组织应实施并保持风险评估和应对程序。

注：风险评估和应对的过程在ISO 31000中涉及。

组织应：

a）确定其与安全有关的风险，根据其安全管理所需的资源对这些风险进行优先排序；

b）分析和评估已确定的风险；

c）确定哪些风险需要应对；

d）选择并实施应对这些风险的方案；

e）准备和实施风险应对计划。

注：本条款的风险涉及到组织及其相关方的安全。风险和与管理体系有效性有关的机遇将在6.1中讨论。

8.4 控制

8.2中所列过程应包括对人力资源管理的控制，以及适当时对与安全有关的设备、仪器和信息技术项目的设计、安装、运行、整修和调整。如果对现有的安排进行了改变，或引入了可能对安全管理产生影响的新安排，组织应在实施之前考虑相关的安全相关风险。要考虑的新的或改变的安排应包括：

a）修订组织结构、岗位或责任；

b）培训、意识和人力资源管理；

c）修订安全管理方针、目标、指标或方案；

d）修订过程和程序；

e）引入新的基础设施、安全设备或技术，其中可能包括硬件和/或软件；

f）适当时引进新的承包商、供方或人员；

g）对外部供方的安全保证要求。

组织应控制策划的变更，评审非预期变更的后果，必要时，采取措施减轻不利影响。

组织应确保与安全管理体系相关的外部提供的过程、产品或服务得到控制。

8.5 安全策略、程序、过程和应对方法

8.5.1 确定和选择战略和应对方法

组织应实施并保持系统的程序，以分析与安全有关的脆弱性和威胁。基于这种脆弱性和威胁分析以及随之而来的风险评估，组织应确定并选择一种安全策略，其中包括一个或多个程序、过程和应对方法。

识别的依据应是策略、程序、过程和应对的程度：

a）保持组织的安全；

b）减少安全漏洞的可能性；

c）减少威胁实现的可能性；

d）缩短任何安全处理缺陷的期限并限制其影响；

e）提供充足的资源。

选择应基于战略、过程和应对的程度：

——满足保护组织安全的要求；

——考虑组织可能或不可能承担的风险的数量和类型；

——考虑相关的成本和效益。

8.5.2 资源要求

组织应确定实施所选安全程序、过程和应对方法的资源要求。

8.5.3 应对的实施

组织应实施和保持选定的安全处理。

8.6 安全计划

8.6.1 总则

组织应根据选定的战略和应对方法，制定并将安全计划和程序形成文件。组织应实施并保持一个响应结构，以便能够及时有效地警告并向有关方面通报与安全有关的漏洞和迫在眉睫的安全威胁或正在发生的安全违规行为。响应结构应提供计划和程序，以便在迫在眉睫的安全威胁或正在发生的安全违规行为期间管理本组织。

8.6.2 响应结构

组织应实施并保持一种结构，确定一个指定的人或一个或多个小组负责应对与安全有关的脆弱性和威胁。指定人员或每个小组的作用和责任以及该人员或小组之间的关系。

应明确确定、沟通和记录团队。

总体而言，各小组应能做到：

a) 评估安全威胁的性质和程度及其潜在影响；

b) 根据预先确定的阈值评估影响，以证明启动正式回应的合理性；

c) 启动适当的安全响应；

d) 策划需要采取的措施；

e) 以生命安全为第一优先，确定优先次序；

f) 监视与安全有关的漏洞的任何变化、威胁者的意图和能力的变化或安全违规行为的影响以及组织的反应；

g) 启动安全应对；

h) 与相关方、当局和媒体沟通；

i) 与沟通管理部门一起为沟通计划做出贡献。对于每个指定的人或团队，应有：

——确定的工作人员，包括具有履行其指定职责的必要职责、权限和能力的候补人员；

——指导其措施的成文程序，包括应对措施的启动、运行、协调和沟通的程序。

8.6.3 警告和沟通

组织应将以下程序形成文件并加以保持：

a) 向相关方进行内部和外部沟通，包括沟通的内容、时间、对象和方式；

注：组织可以记录和维护如何以及在何种情况下的程序、组织与员工和他们的紧急联系人进行沟通。

组织应将如何以及在何种情况下与员工及其紧急联系人进行沟通的程序形成文件并加以保持。

b) 接收、记录和回应相关方的沟通，包括任何国家或区域风险咨询系统或同等机构；

c) 确保在违反安全规定、出现漏洞或威胁时沟通方式的可用性；

d) 促进与安全威胁和/或违法行为应对者的结构化沟通；

e) 提供组织在发生安全违规事件后对媒体反应的细节，包括沟通策略；

f）记录违反安全规定的细节、采取的措施和作出的决定。在适用的情况下，还应考虑和实施以下内容：

——提醒可能受到实际或即将发生的安全违规行为影响的相关方；

——确保多个应对组织之间的适当协调和沟通。警告和通信程序应作为组织测试和培训计划的一部分进行演练。

8.6.4 安全计划的内容

组织应安全计划形成文件并加以保持。这些计划应提供指导和信息，以协助团队应对安全漏洞、威胁和/或违规行为，并协助组织进行应对和恢复其安全。

总的来说，安全计划应包含：

a）各小组将采取的措施的细节，以：

1）继续或恢复商定的安全状态；

2）监视实际或即将发生的安全威胁、漏洞或违规行为的影响以及组织对其的反应；

b）参照预设的阈值和启动反应的过程；

c）恢复组织安全的程序；

d）管理安全漏洞和威胁或实际或即将发生的安全侵犯行为的直接后果的细节，并适当考虑到：

1）个人的福利；

2）可能受到损害的资产、信息和人员的价值；

3）防止核心活动的（进一步）损失或不可用。

每个计划都应包括：

——其目的、范围和目标；

——实施该计划的团队的作用和责任；

——实施解决方案的措施；

——启动(包括启动标准)、运行、协调、和沟通团队行动所需的信息；

——内部和外部的相互依存关系；

——其资源需求；

——其报告要求；

——退出过程。

每个计划都应是可用的，并在需要的时间和地点提供。

8.6.5 恢复

组织应具有文件化的过程，以从安全违规之前、期间和之后采取的任何临时措施中恢复组织的安全。

9 绩效评价

9.1 监视、测量、分析和评价

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（如适用），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。

组织应评价安全管理体系的绩效和有效性。

9.2 内部审核

9.2.1 总则

组织应按照策划的时间间隔进行内部审核，以提供有关安全管理体系的下列信息：

a）是否符合：

1）组织自身的安全管理体系要求；

2）本标准的要求。

b）是否得到有效的实施和保持。

9.2.2 内部审核方案

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、实施和保持审核方案，审核方案包括频次、方法、职责、策划要求和报告。

组织应：

a）规定每次审核的审核目标、准则和范围；

b）选择审核员实施审核，以确保审核过程客观公正；

c）确保将审核结果报告给相关管理者。

d）验证安全设备和人员是否得到适当的部署；

e）确保采取任何必要的纠正措施，不做无谓的拖延，以消除发现的不符合及其原因；

f）确保后续审核措施包括验证所采取的措施和报告验证结果。

保留成文信息，作为实施审核方案以及审核结果的证据。

审核程序（包括任何时间表），应基于对组织活动的风险评估结果和以往审核的结果。审核程序应涵盖范围、频率、方法和能力，以及进行审核和报告结果的职责和要求。

9.3 管理评审

9.3.1 总则

最高管理者应按照策划的时间间隔对组织的安全管理体系进行评审，以确保其持续的适宜性、充分性和有效性。

组织应考虑分析和评价的结果以及管理评审的结果，以确定是否存在与业务或安全管理体系有关的需求或机会，并作为持续改进的一部分加以解决。

注：组织可以使用安全管理体系过程，如领导作用、策划和绩效评价，以实现改进。

9.3.2 管理评审输入

管理评审应包括：

a）以往管理评审所采取措施的状况；

b）与安全管理体系相关的内外部因素的变化；

c）与安全管理体系有关的相关方的需求和期望的变化；

d）下列有关安全绩效的信息，，包括其趋势：

1）不符合和纠正措施；

2）监视和测量结果；

3）审核结果；

e）持续改进机会；

f）对遵守法律要求和本组织同意的其他要求的审核和评估结果；

g）来自外部相关方的沟通，包括投诉；

h）组织的安全绩效；

i）目标和指标的实现程度；

j）纠正措施的状况；

k）以往管理评审的后续措施；

I）不断变化的环境，包括与安全方面有关的法律、法规和其他要求（见4.2.2）的发展；

m）改进的建议。

9.3.3 管理评审输出

管理评审的结果应包括与持续改进机会有关的决定和对安全管理体系的任何变更需求。

组织应保留成文信息，作为管理评审结果的证据。

10 改进

10.1 持续改进

组织应持续改进安全管理体系的适宜性、充分性和有效性。组织应积极寻求改进的机会，即使不是因为与安全有关的漏洞和迫在眉睫的安全威胁或正在发生的安全违规行为而促使相关的有关方面改进。

10.2 不符合和纠正措施

当发生不符合时，组织应：

a）对不符合做出应对，并在适用时：

1）采取措施以控制和纠正不合格；

2）处置后果；

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

1）评审不符合；

2）确定不符合的原因；

3）确定是否存在或可能发生类似的不符合；

c）实施所需的措施；

d）评评审所采取的纠正措施的有效性；

e）需要时，变更安全管理体系。

纠正措施应与不符合所产生的影响相适应。

应保留成文信息，作为下列事项的证据：

——不符合的性质以及随后所采取的措施；

——任何纠正措施的结果；

——对安全方面的调查：

- 失败，包括近乎失误和错误警报；
- 事故和紧急情况；
- 不符合；

采取措施，减轻此类故障、事故或不符合所产生的任何后果。

程序应要求在实施之前，通过安全相关风险的评估过程对所有拟议的纠正措施进行评审，除非立即实施可以防止即将发生的生命或公共安全风险。

为消除实际和潜在不符合的原因而采取的任何纠正措施，应与问题的严重程度相适应，并与可能遇到的安全管理相关风险相适应。

参考文献

[1] ISO 9001 质量管理体系-要求

[2] ISO 14001 环境管理体系-要求与使用指南

[3] ISO 19011 管理体系审核指南

[4] ISO 22301 安全与韧性-业务连续性管理体系-要求

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

[6] ISO 28001 供应链安全管理体系 实施供应链安全、评估和计划的最佳实践 要求和指南

[7] ISO 28002 供应链安全管理体系 供应链韧性的开发--要求及使用指南

[8] ISO 28003 供应链安全管理体系 对供应链安全管理体系审核认证机构的要求

[9] ISO 28004-1 供应链安全管理体系 ISO 28000 实施指南

[10] ISO 28004-3 供应链安全管理体系 ISO28000 实施指南第 3 部分：中小业务采用 ISO28000 的附加特定指南(海港除外)

[11] ISO 28004-4 供应链安全管理体系 ISO28000 实施指南第 4 部分：若以符合 ISO28001 为管理目标实施 ISO28000 的附加特定指南

[12] ISO 31000 风险管理指南

[13] ISO 45001 职业健康和安全管理体系—要求与使用指南

[14] ISO 导则 73，风险管理 - 术语

BS ISO 28000:2022

BSI Standards Publication

Security and resilience — Security management systems — Requirements

bsi.

National foreword

This British Standard is the UK implementation of ISO 28000:2022. It supersedes BS ISO 28000:2007, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee GW/3, Private Security Management & Services.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

Published by BSI Standards Limited 2022

ISBN 978 0 539 12989 2

ICS 03.100.01; 03.100.70

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 April 2022.

Amendments/corrigenda issued since publication

Date	Text affected

BS ISO 28000:2022

INTERNATIONAL STANDARD

ISO 28000

Second edition
2022-03-15

Security and resilience — Security management systems — Requirements

Reference number
ISO 28000:2022(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 292, *Security and resilience.*

This second edition cancels and replaces the first edition (ISO 28000:2007), which has been technically revised, but maintains existing requirements to provide continuity for organizations using the previous edition. The main changes are as follows:

— recommendations on principles have been added in Clause 4 to give better coordination with ISO 31000;

— recommendations have been added in Clause 8 for better consistency with ISO 22301, facilitating integration including:

  — security strategies, procedures, processes and treatments;

  — security plans.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

Most organizations are experiencing an increasing uncertainty and volatility in the security environment. As a consequence, they face security issues that impact on their objectives, which they want to address systematically within their management system. A formal approach to security management can contribute directly to the business capability and credibility of the organization.

This document specifies requirements for a security management system, including those aspects critical to the security assurance of the supply chain. It requires the organization to:

— assess the security environment in which it operates including its supply chain (including dependencies and interdependencies);

— determine if adequate security measures are in place to effectively manage security-related risks;

— manage compliance with statutory, regulatory and voluntary obligations to which the organization subscribes;

— align security processes and controls, including the relevant upstream and downstream processes and controls of the supply chain to meet the organization's objectives.

Security management is linked to many aspects of business management. They include all activities controlled or influenced by organizations, including but not limited to those that impact on the supply chain. All activities, functions and operations should be considered that have an impact on the security management of the organization including (but not limited to) its supply chain.

With regard to the supply chain, it has to be considered that supply chains are dynamic in nature. Therefore, some organizations managing multiple supply chains may look to their providers to meet related security standards as a condition of being included in that supply chain in order to meet requirements for security management.

This document applies the Plan-Do-Check-Act (PDCA) model to planning, establishing, implementing, operating, monitoring, reviewing, maintaining and continually improving the effectiveness of an organization's security management system, see Table 1 and Figure 1.

Table 1 — Explanation of the PDCA model

Plan (Establish)	Establish security policy, objectives, targets, controls, processes and procedures relevant to improving security in order to deliver results that align with the organization's overall policies and objectives.
Do (Implement and operate)	Implement and operate the security policy, controls, processes and procedures.
Check (Monitor and review)	Monitor and review performance against security policy and objectives, report the results to management for review, and determine and authorize actions for remediation and improvement.
Act (Maintain and improve)	Maintain and improve the security management system by taking corrective action, based on the results of management review and reappraising the scope of the security management system and security policy and objectives.

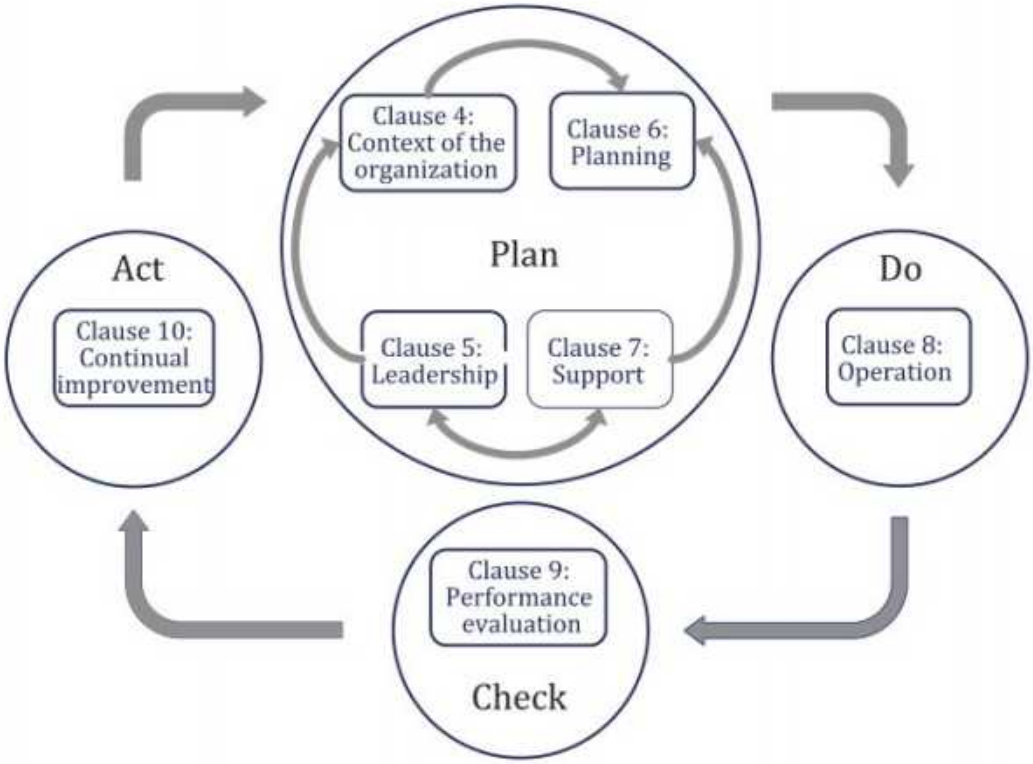

Figure 1 — PDCA model applied to the security management system

This ensures a degree of consistency with other management system standards, such as ISO 9001, ISO 14001, ISO 22301, ISO/IEC 27001, ISO 45001, etc., thereby supporting consistent and integrated implementation and operation with related management systems.

For organizations that so wish, conformity of the security management system to this document may be verified by an external or internal auditing process.

This page deliberately left blank

INTERNATIONAL STANDARD ISO 28000:2022

Security and resilience — Security management systems — Requirements

1 Scope

This document specifies requirements for a security management system, including aspects relevant to the supply chain.

This document is applicable to all types and sizes of organizations (e.g. commercial enterprises, government or other public agencies and non-profit organizations) which intend to establish, implement, maintain and improve a security management system. It provides a holistic and common approach and is not industry or sector specific.

This document can be used throughout the life of the organization and can be applied to any activity, internal or external, at all levels.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 22300, *Security and resilience — Vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 22300 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
organization
person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its *objectives* (3.7)

Note 1 to entry: The concept of organization includes, but is not limited to, sole-trader, company, corporation, firm, enterprise, authority, partnership, charity or institution, or part or combination thereof, whether incorporated or not, public or private.

Note 2 to entry: If the organization is part of a larger entity, the term "organization" refers only to the part of the larger entity that is within the scope of the *security management system* (3.5).

3.2
interested party (preferred term)
stakeholder **(admitted term)**
person or *organization* (3.1) that can affect, be affected by, or perceive itself to be affected by a decision or activity

3.10
competence
ability to apply knowledge and skills to achieve intended results

3.11
documented information
information required to be controlled and maintained by an *organization* (3.1) and the medium on which it is contained

Note 1 to entry: Documented information can be in any format and media, and from any source.

Note 2 to entry: Documented information can refer to:

— the *management system* (3.4), including related *processes* (3.9);

— information created in order for the organization to operate (documentation);

— evidence of results achieved (records).

3.12
performance
measurable result

Note 1 to entry: Performance can relate either to quantitative or qualitative findings.

Note 2 to entry: Performance can relate to managing activities, *processes* (3.9), products, services, systems or *organizations* (3.1).

3.13
continual improvement
recurring activity to enhance *performance* (3.12)

3.14
effectiveness
extent to which planned activities are realized and planned results are achieved

3.15
requirement
need or expectation that is stated, generally implied or obligatory

Note 1 to entry: "Generally implied" means that it is custom or common practice for the *organization* (3.1) and *interested parties* (3.2) that the need or expectation under consideration is implied.

Note 2 to entry: A specified requirement is one that is stated, e.g. in *documented information* (3.11).

3.16
conformity
fulfilment of a *requirement* (3.15)

3.17
nonconformity
non-fulfilment of a *requirement* (3.15)

3.18
corrective action
action to eliminate the cause(s) of a *nonconformity* (3.17) and to prevent recurrence

3.19
audit
systematic and independent *process* (3.9) for obtaining evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled

Note 1 to entry: An audit can be an internal audit (first party) or an external audit (second party or third party), and it can be a combined audit (combining two or more disciplines).

Note 2 to entry: An internal audit is conducted by the *organization* (3.1) itself, or by an external party on its behalf.

Note 3 to entry: "Audit evidence" and "audit criteria" are defined in ISO 19011.

3.20
measurement
process (3.9) to determine a value

3.21
monitoring
determining the status of a system, a *process* (3.9) or an activity

Note 1 to entry: To determine the status, there can be a need to check, supervise or critically observe.

4 Context of the organization

4.1 Understanding the organization and its context

The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended result(s) of its security management system including the requirements of its supply chain.

4.2 Understanding the needs and expectations of interested parties

4.2.1 General

The organization shall determine:

— the interested parties that are relevant to the security management system;

— the relevant requirements of these interested parties;

— which of these requirements will be addressed through the security management system.

4.2.2 Legal, regulatory and other requirements

The organization shall:

a) implement and maintain a process to identify, have access to and assess the applicable legal, regulatory and other requirements related to its security;

b) ensure that these applicable legal, regulatory and other requirements are taken into account in implementing and maintaining its security management system;

c) document this information and keep it up to date;

d) communicate this information to relevant interested parties as appropriate.

4.2.3 Principles

4.2.3.1 General

The purpose of security management within the organization is the creation and, in particular, the protection of value.

The organization should apply the principles given in Figure 2 and described in 4.2.3.2 to 4.2.3.9.

Figure 2 — Principles

4.2.3.2 Leadership

Leaders at all levels should establish unity of purpose and direction. They should create conditions to align the organization's strategies, policies processes and resources to achieve its objectives. Clause 5 explains the requirements with regard to this principle.

4.2.3.3 Structured and comprehensive process approach based on best available information

A structured and comprehensive approach to security management including the supply chain should contribute to consistent and comparable results, which are achieved more effectively and efficiently when activities are understood and managed as interrelated processes functioning as a coherent system.

4.2.3.4 Customized

The security management system should be customized and proportionate to the organization's external and internal context and needs. It should be related to its objectives.

4.2.3.5 Inclusive engagement of people

The organization should involve interested parties appropriately and in a timely manner. It should consider their knowledge, views and perceptions appropriately to improve awareness of and facilitate

informed security management. The organization should ensure that everybody at all levels is respected and involved.

4.2.3.6 Integrated approach

Security management is an integral part of all organizational activities. It should be integrated with all other management systems of the organization.

The organization's risk management – whether formal, informal or intuitive – should be integrated into the security management system.

4.2.3.7 Dynamic and continually improved

The organization should have an ongoing focus on improvement through learning and experience to maintain the level of performance, to react to changes and to create new opportunities as the external and internal context of the organization changes.

4.2.3.8 Considering human and cultural factors

Human behaviour and culture significantly influence all aspects of security management and should be considered at each level and stage. Decisions should be based on the analysis and evaluation of data and information to ensure they result in greater objectivity, confidence in decision-making and are more likely to produce desired results. Individual perceptions should be considered.

4.2.3.9 Relationship management

For sustained success, the organization should manage its relationships with all relevant interested parties as they might influence the performance of the organization.

4.3 Determining the scope of the security management system

The organization shall determine the boundaries and applicability of the security management system to establish its scope.

When determining this scope, the organization shall consider:

— the external and internal issues referred to in 4.1;

— the requirements referred to in 4.2.

The scope shall be available as documented information.

Where an organization chooses to have any process that affects conformity with its security management system externally provided, the organization shall ensure that such processes are controlled. The necessary controls for and responsibilities of such externally provided processes shall be identified within the security management system.

4.4 Security management system

The organization shall establish, implement, maintain and continually improve a security management system, including the processes needed and their interactions, in accordance with the requirements of this document.

5 Leadership

5.1 Leadership and commitment

Top management shall demonstrate leadership and commitment with respect to the security management system by:

— ensuring that the security policy and security objectives are established and are compatible with the strategic direction of the organization;

— ensuring that the requirements and expectations of the organization's interested parties are identified and monitored, and appropriate timely action is taken to manage these expectations to ensure the integration of the security management system requirements into the organization's business processes;

— ensuring the integration of the security management system requirements into the organization's business processes;

— ensuring that the resources needed for the security management system are available;

— communicating the importance of effective security management and of conforming to the security management system requirements;

— ensuring that the security management system achieves its intended result(s);

— ensuring the viability of the security management objectives, targets and programmes;

— ensuring any security programmes generated from other parts of the organization complement the security management system;

— directing and supporting persons to contribute to the effectiveness of the security management system;

— promoting continual improvement of the organization's security management system;

— supporting other relevant roles to demonstrate their leadership as it applies to their areas of responsibility.

NOTE Reference to "business" in this document can be interpreted broadly to mean those activities that are core to the purposes of the organization's existence.

5.2 Security policy

5.2.1 Establishing the security policy

Top management shall establish a security policy that:

a) is appropriate to the purpose of the organization;

b) provides a framework for setting security objectives;

c) includes a commitment to meet applicable requirements;

d) includes a commitment to continual improvement of the security management system;

e) considers the adverse impact that the security policy, objectives, targets, programmes, etc. can have on other aspects of the organization.

5.2.2 Security policy requirements

The security policy shall:

— be consistent with other organizational policies;

— be consistent with the organization's overall security risk assessment;

— provide for its review in case of the acquisition of, or a merger with, other organizations, or other changes to the business scope of the organization which could affect the continuity or relevance of the security management system;

— describe and allocate primary accountability and responsibility for outcomes;

— be available as documented information;

— be communicated within the organization;

— be available to interested parties, as appropriate.

NOTE Organizations can choose to have a detailed security management policy for internal use which would provide sufficient information and direction to drive the security management system (parts of which can be confidential) and have a summarized (non-confidential) version containing the broad objectives for dissemination to their interested parties.

5.3 Roles, responsibilities and authorities

Top management shall ensure that the responsibilities and authorities for relevant roles are assigned and communicated within the organization.

Top management shall assign the responsibility and authority for:

a) ensuring that the security management system conforms to the requirements of this document;

b) reporting on the performance of the security management system to top management.

6 Planning

6.1 Actions to address risks and opportunities

6.1.1 General

When planning for the security management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to:

— give assurance that the security management system can achieve its intended result(s);

— prevent, or reduce, undesired effects;

— achieve continual improvement.

The organization shall plan:

a) actions to address these risks and opportunities;

b) how to:

— integrate and implement the actions into its security management system processes;

— evaluate the effectiveness of these actions.

The purpose of managing risks is the creation and protection of value. Managing risk shall be integrated into the security management system. Risks related to the security of the organization and its interested parties are addressed in 8.3.

6.1.2 Determining security-related risks and identifying opportunities

Determining security-related risks and identifying and exploiting opportunities requires a proactive risk assessment which shall include consideration of, but not be limited to:

a) physical or functional failures and malicious or criminal acts;

b) environmental, human and cultural factors and other internal or external contexts, including factors outside the organization's control affecting the organization's security;

c) the design, installation, maintenance and replacement of security equipment;

d) the organization's information, data, knowledge and communication management;

e) information related to security threats and vulnerabilities;

f) the interdependencies between suppliers.

6.1.3 Addressing security-related risks and exploiting opportunities

The evaluation of the identified security-related risk shall provide input to (but not be limited to):

a) the organization's overall risk management;

b) risk treatment;

c) security management objectives;

d) security management processes;

e) the design, specification and implementation of the security management system;

f) the identification of adequate resources including staffing;

g) the identification of training needs and the required level of competence.

6.2 Security objectives and planning to achieve them

6.2.1 Establishing security objectives

The organization shall establish security objectives at relevant functions and levels.

The security objectives shall:

a) be consistent with the security policy;

b) be measurable (if practicable);

c) take into account applicable requirements;

d) be monitored;

e) be communicated;

f) be updated as appropriate;

g) be available as documented information.

6.2.2 Determining security objectives

When planning how to achieve its security objectives, the organization shall determine:

— what will be done;

— what resources will be required;

— who will be responsible;

— when it will be completed;

— how the results will be evaluated.

When establishing and reviewing its security objectives, an organization shall take into account:

a) technological, human, administrative and other options;

b) views of and impacts on appropriate interested parties.

The security objectives shall be consistent with the organization's commitment to continual improvement.

6.3 Planning of changes

When the organization determines the need for changes to the security management system, including those identified in Clause 10, the changes shall be carried out in a planned manner.

The organization shall consider:

a) the purpose of the changes and their potential consequences;

b) the integrity of the security management system;

c) the availability of resources;

d) the allocation or reallocation of responsibilities and authorities.

7 Support

7.1 Resources

The organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the security management system.

7.2 Competence

The organization shall:

— determine the necessary competence of person(s) doing work under its control that affects its security performance;

— ensure that these persons are competent on the basis of appropriate education, training, or experience and are appropriately security cleared;

— where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken;

Appropriate documented information shall be available as evidence of competence.

NOTE Applicable actions can include, for example: the provision of training to, the mentoring of, or the reassignment of currently employed persons; or the hiring or contracting of competent persons.

7.3 Awareness

Persons doing work under the organization's control shall be aware of:

— the security policy;

— their contribution to the effectiveness of the security management system, including the benefits of improved security performance;

— the implications of not conforming with the security management system requirements;

— their roles and responsibilities in achieving compliance with the security management policy and procedures and with the requirements of the security management system, including emergency preparedness and response requirements.

7.4 Communication

The organization shall determine the internal and external communications relevant to the security management system, including:

— on what it will communicate;

— when to communicate;

— with whom to communicate;

— how to communicate;

— the sensitivity of information prior to dissemination.

7.5 Documented information

7.5.1 General

The organization's security management system shall include:

a) documented information required by this document;

b) documented information determined by the organization as being necessary for the effectiveness of the security management system.

The documented information shall describe the responsibilities and authorities for achieving security management objectives and targets, including the means and timelines to achieve those objectives and targets.

NOTE The extent of documented information for a security management system can differ from one organization to another due to:

— the size of organization and its type of activities, processes, products and services;

— the complexity of processes and their interactions;

— the competence of persons.

The organization shall determine the value of information, and establish the level of integrity required and the security controls to prevent unauthorized access.

7.5.2 Creating and updating documented information

When creating and updating documented information, the organization shall ensure appropriate:

— identification and description (e.g. a title, date, author, or reference number);

— format (e.g. language, software version, graphics) and media (e.g. paper, electronic);

— review and approval for suitability and adequacy.

7.5.3 Control of documented information

Documented information required by the security management system and by this document shall be controlled to ensure:

a) it is available and suitable for use, where and when it is needed;

b) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity);

c) it is periodically reviewed and revised as necessary, and approved for adequacy by authorized personnel;

d) obsolete documents, data and information are promptly removed from all points of issue and points of use, or otherwise assured against unintended use;

e) archival documents, data and information retained for legal or knowledge preservation purposes or both are suitably identified.

For the control of documented information, the organization shall address the following activities, as applicable:

— distribution, access, retrieval and use;

— storage and preservation, including preservation of legibility;

— control of changes (e.g. version control);

— retention and disposition.

Documented information of external origin determined by the organization to be necessary for the planning and operation of the security management system shall be identified, as appropriate, and controlled.

NOTE Access can imply a decision regarding the permission to view the documented information only, or the permission and authority to view and change the documented information.

8 Operation

8.1 Operational planning and control

The organization shall plan, implement and control the processes needed to meet requirements, and to implement the actions determined in Clause 6, by:

— establishing criteria for the processes;

— implementing control of the processes in accordance with the criteria.

Documented information shall be available to the extent necessary to have confidence that the processes have been carried out as planned.

8.2 Identification of processes and activities

The organization shall identify those processes and activities that are necessary for achieving:

a) compliance with its security policy;

b) compliance with legal, statutory and regulatory security requirements;

c) its security management objectives;

d) the delivery of its security management system;

e) the required level of security of the supply chain.

8.3 Risk assessment and treatment

The organization shall implement and maintain a risk assessment and treatment process.

NOTE The process for risk assessment and treatment is addressed in ISO 31000.

The organization should:

a) identify its security-related risks, prioritizing them to the resources required for its security management;

b) analyse and evaluate the identified risks;

c) determine which risks require treatment;

d) select and implement options to address those risks;

e) prepare and implement risk treatment plans.

NOTE Risks in this subclause relate to the security of the organization and its interested parties. Risks and opportunities related to the effectiveness of the management system are addressed in 6.1.

8.4 Controls

The processes listed in 8.2 shall include controls for human resource management, as well as the design, installation, operation, refurbishment and modification of security-related items of equipment, instrumentation and information technology, as appropriate. Where existing arrangements are revised or new arrangements introduced that could have impact on security management, the organization shall consider the associated security-related risks before their implementation. The new or revised arrangements to be considered shall include:

a) revised organizational structure, roles or responsibilities;

b) training, awareness and human resource management;

c) revised security management policy, objectives, targets or programmes;

d) revised processes and procedures;

e) the introduction of new infrastructure, security equipment or technology, which may include hardware and/or software;

f) the introduction of new contractors, suppliers or personnel, as appropriate;

g) the requirements for security assurance of external suppliers.

The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.

The organization shall ensure that externally provided processes, products or services that are relevant to the security management system are controlled.

8.5 Security strategies, procedures, processes and treatments

8.5.1 Identification and selection of strategies and treatments

The organization should implement and maintain systematic processes for analysing vulnerabilities and threats related to security. Based on this vulnerability and threat analysis and consequent risk assessment, the organization should identify and select a security strategy which comprises one or more procedures, processes and treatments.

Identification should be based on the extent to which strategies, procedures, processes and treatments:

a) maintain the organization's security;

b) reduce the likelihood of security vulnerability;

c) reduce the likelihood of a threat being actualised;

d) shorten the period of any security treatment deficiencies and limit their impact;

e) provide for the availability of adequate resources.

Selection should be based on the extent to which strategies, processes and treatments:

— meet the requirements to protect the organization's security;

— consider the amount and type of risk the organization may or may not take;

— consider the associated costs and benefits.

8.5.2 Resource requirements

The organization shall determine the resource requirements to implement the selected security procedures, processes and treatments.

8.5.3 Implementation of treatments

The organization shall implement and maintain selected security treatments.

8.6 Security plans

8.6.1 General

The organization shall establish and document security plans and procedures based on the selected strategies and treatments. The organization shall implement and maintain a response structure that will enable timely and effective warning and communication of vulnerabilities related to security and imminent security threats or ongoing security violations to relevant interested parties. The response structure shall provide plans and procedures to manage the organization during an imminent security threat or an ongoing security violation.

8.6.2 Response structure

The organization shall implement and maintain a structure, identifying a designated person or one or more teams responsible for responding to vulnerabilities and threats related to security. The roles and responsibilities for the designated person or each team and the relationship between the person or teams shall be clearly identified, communicated and documented.

Collectively, the teams should be competent to:

a) assess the nature and extent of a security threat and its potential impact;

b) assess the impact against pre-defined thresholds that justify initiation of a formal response;

c) activate an appropriate security response;

d) plan actions that need to be undertaken;

e) establish priorities using life safety as the first priority;

f) monitor the effects of any variation in vulnerabilities related to security, changes to the intent and capability of threat actors or security violations and the organization's response;

g) activate the security treatments;

h) communicate with relevant interested parties, authorities and the media;

i) contribute to a communication plan with communication management.

For each designated person or team there should be:

— identified staff, including alternates with the necessary responsibility, authority and competence to perform their designated role;

— documented procedures to guide their actions including those for the activation, operation, coordination and communication of the response.

8.6.3 Warning and communication

The organization should document and maintain procedures for:

a) communicating internally and externally to relevant interested parties, including what, when, with whom and how to communicate;

NOTE The organization can document and maintain procedures for how, and under what circumstances, the organization communicates with employees and their emergency contacts.

b) receiving, documenting and responding to communications from interested parties, including any national or regional risk advisory system or equivalent;

c) ensuring the availability of the means of communication during a security violation, vulnerability or threat;

d) facilitating structured communication with responders to security threats and/or violations;

e) providing details of the organization's media response following a security violation, including a communications strategy;

f) recording the details of the security violation, the actions taken and the decisions made.

Where applicable, the following should also be considered and implemented:

— alerting interested parties potentially impacted by an actual or impending security violation;

— ensuring appropriate coordination and communication between multiple responding organizations.

The warning and communication procedures shall be exercised as part of the organization's testing and training programme.

8.6.4 Content of the security plans

The organization shall document and maintain security plans. Those plans should provide guidance and information to assist teams to respond to a security vulnerability, threat and/or violation and to assist the organization with the response and restoring its security.

Collectively, security plans should contain:

a) details of the actions that the teams will take to:

   1) continue or restore the agreed security status;

   2) monitor the impact of the actual or impending security threats, vulnerabilities or violation and the organization's response to it;

b) reference to the pre-defined threshold(s) and process for activating the response;

c) procedures to restore the security of the organization;

d) details to manage the immediate consequences of a security vulnerability and threat or actual or impending security violation giving due regard to:

   1) the welfare of individuals;

   2) the value of the assets, information and personnel potentially compromised;

   3) the prevention of (further) loss or unavailability of core activities.

Each plan should include:

— its purpose, scope and objectives;

— the roles and responsibilities of the team that will implement the plan;

— the actions to implement the solutions;

— the information needed to activate (including activation criteria), operate, coordinate and communicate the team's actions;

— internal and external interdependencies;

— its resource requirements;

— its reporting requirements;

— a process for standing down.

Each plan should be usable and available at the time and place at which it is required.

8.6.5 Recovery

The organization shall have documented processes to restore the organization's security from any temporary measures adopted before, during and after a security violation.

9 Performance evaluation

9.1 Monitoring, measurement, analysis and evaluation

The organization shall determine:

— what needs to be monitored and measured;

— the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results;

— when the monitoring and measuring shall be performed;

— when the results from monitoring and measurement shall be analysed and evaluated.

Documented information shall be available as evidence of the results.

The organization shall evaluate the performance and the effectiveness of the security management system.

9.2 Internal audit

9.2.1 General

The organization shall conduct internal audits at planned intervals to provide information on whether the security management system:

a) conforms to:

   1) the organization's own requirements for its security management system;

   2) the requirements of this document;

b) is effectively implemented and maintained.

9.2.2 Internal audit programme

The organization shall plan, establish, implement and maintain (an) audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting.

When establishing the internal audit programme(s), the organization shall consider the importance of the processes concerned and the results of previous audits.

The organization shall:

a) define the audit objectives, criteria and scope for each audit;

b) select auditors and conduct audits to ensure objectivity and the impartiality of the audit process;

c) ensure that the results of the audits are reported to relevant managers.

d) verify that the security equipment and personnel are appropriately deployed;

e) ensure that any necessary corrective actions are taken without undue delay to eliminate detected nonconformities and their causes;

f) ensure that follow-up audit actions include the verification of the actions taken and the reporting of verification results.

Documented information shall be available as evidence of the implementation of the audit programme(s) and the audit results.

The audit programme, including any schedule, shall be based on the results of risk assessments of the organization's activities and the results of previous audits. The audit procedures shall cover the scope, frequency, methodologies and competencies, as well as the responsibilities and requirements for conducting audits and reporting results.

9.3 Management review

9.3.1 General

Top management shall review the organization's security management system, at planned intervals, to ensure its continuing suitability, adequacy and effectiveness.

The organization shall consider the results of analysis and evaluation, and the outputs from management review, to determine if there are needs or opportunities relating to the business or to the security management system that shall be addressed as part of continual improvement.

NOTE The organization can use the processes of the security management system, such as leadership, planning and performance evaluation, to achieve improvement.

9.3.2 Management review inputs

The management review shall include:

a) the status of actions from previous management reviews;

b) changes in external and internal issues that are relevant to the security management system;

c) changes in needs and expectations of interested parties that are relevant to the security management system;

d) information on the security performance, including trends in:

   1) nonconformities and corrective actions;

   2) monitoring and measurement results;

   3) audit results;

e) opportunities for continual improvement;

f) results of audits and evaluations of compliance with legal requirements and other requirements to which the organization subscribes;

g) communication(s) from external interested parties, including complaints;

h) the security performance of the organization;

i) the extent to which objectives and targets have been met;

j) status of corrective actions;

k) follow-up actions from previous management reviews;

l) changing circumstances, including developments to legal, regulatory and other requirements (see 4.2.2) related to security aspects;

m) recommendations for improvement.

9.3.3 Management review results

The results of the management review shall include decisions related to continual improvement opportunities and any need for changes to the security management system.

Documented information shall be available as evidence of the results of management reviews.

10 Improvement

10.1 Continual improvement

The organization shall continually improve the suitability, adequacy and effectiveness of the security management system. The organization should actively seek opportunities for improvement, even if not prompted by vulnerabilities related to security and imminent security threats or ongoing security violations to relevant interested parties.

10.2 Nonconformity and corrective action

When a nonconformity occurs, the organization shall:

a) react to the nonconformity, and as applicable:

   1) take action to control and correct it;

   2) deal with the consequences;

b) evaluate the need for action to eliminate the cause(s) of the nonconformity, in order that it does not recur or occur elsewhere, by:

   1) reviewing the nonconformity;

   2) determining the causes of the nonconformity;

   3) determining if similar nonconformities exist, or can potentially occur;

c) implement any action needed;

d) review the effectiveness of any corrective action taken;

e) make changes to the security management system, if necessary.

Corrective actions shall be appropriate to the effects of the nonconformities encountered.

Documented information shall be available as evidence of:

— the nature of the nonconformities and any subsequent actions taken;

— the results of any corrective action;

— the investigation of security-related:

   — failures, including near misses and false alarms;

   — incidents and emergency situations;

   — nonconformities;

— taking action to mitigate any consequences arising from such failures, incidents or nonconformities.

Procedures shall require that all proposed corrective actions are reviewed through the assessment process of security-related risk prior to implementation unless immediate implementation forestalls imminent exposures to life or public safety.

Any corrective action taken to eliminate the causes of actual and potential nonconformities shall be appropriate to the magnitude of the problems and commensurate with the security-management-related risks likely to be encountered.

Bibliography

[1] ISO 9001, *Quality management systems — Requirements*

[2] ISO 14001, *Environmental management systems — Requirements with guidance for use*

[3] ISO 19011, *Guidelines for auditing management systems*

[4] ISO 22301, *Security and resilience — Business continuity management systems — Requirements*

[5] ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*

[6] ISO 28001, *Security management systems for the supply chain — Best practices for implementing supply chain security, assessments and plans — Requirements and guidance*

[7] ISO 28002, *Security management systems for the supply chain — Development of resilience in the supply chain — Requirements with guidance for use*

[8] ISO 28003, *Security management systems for the supply chain — Requirements for bodies providing audit and certification of supply chain security management systems*

[9] ISO 28004-1, *Security management systems for the supply chain — Guidelines for the implementation of ISO 28000 — Part 1: General principles*

[10] ISO 28004-3, *Security management systems for the supply chain — Guidelines for the implementation of ISO 28000 — Part 3: Additional specific guidance for adopting ISO 28000 for use by medium and small businesses (other than marine ports)*

[11] ISO 28004-4, *Security management systems for the supply chain — Guidelines for the implementation of ISO 28000 — Part 4: Additional specific guidance on implementing ISO 28000 if compliance with ISO 28001 is a management objective*

[12] ISO 31000, *Risk management — Guidelines*

[13] ISO 45001, *Occupational health and safety management systems — Requirements with guidance for use*

[14] ISO Guide 73, *Risk management — Vocabulary*

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Copyright in BSI publications

All the content in BSI publications, including British Standards, is the property of and copyrighted by BSI or some person or entity that owns copyright in the information used (such as the international standardization bodies) and has formally licensed such information to BSI for commercial publication and use.

Save for the provisions below, you may not transfer, share or disseminate any portion of the standard to any other person. You may not adapt, distribute, commercially exploit or publicly display the standard or any portion thereof in any manner whatsoever without BSI's prior written consent.

Storing and using standards

Standards purchased in soft copy format:

- A British Standard purchased in soft copy format is licensed to a sole named user for personal or internal company use only.
- The standard may be stored on more than one device provided that it is accessible by the sole named user only and that only one copy is accessed at any one time.
- A single paper copy may be printed for personal or internal company use only.

Standards purchased in hard copy format:

- A British Standard purchased in hard copy format is for personal or internal company use only.
- It may not be further reproduced – in any format – to create an additional copy. This includes scanning of the document.

If you need more than one copy of the document, or if you wish to share the document on an internal network, you can save money by choosing a subscription product (see 'Subscriptions').

Reproducing extracts

For permission to reproduce content from BSI publications contact the BSI Copyright and Licensing team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member.**

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email cservices@bsigroup.com.

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Useful Contacts

Customer Services
Tel: +44 345 086 9001
Email: cservices@bsigroup.com

Subscriptions
Tel: +44 345 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

bsi.