认　证　规　则

供应链安全管理体系认证规则

编　　号：ZXB-SCSMS-01-2025

受控 状态：受 控

版本	编修	审核	批准	编写/修订日期	发布日期
A/0	崔海军	张京梅	郑宇兵	20250728	20250729
A/0	崔海军	张京梅	郑宇兵	20250827	20250827
A/0	崔海军	张京梅	郑宇兵	20251203	20251203

管理体系手册编制/修订履历

版本	修订内容	编写日期/修订日期	发布日期
A/0	新编	20250728	20250729
A/0	认证证书及认证标志的要求	20250827	20250827
A/0	认证证书及认证标志的要求	20251203	20251203

目录

一、概述

1.1 为规范供应链安全管理体系认证活动，确保认证的公正性、客观性和有效性，依据《中华人民共和国认证认可条例》等相关法律法规及认证行业通用准则，制定本规则。

1.2 本规则规定了供应链安全管理体系认证的程序、要求和管理规范，适用于认证机构开展供应链安全管理体系认证活动，以及申请认证的各类组织。

1.3 供应链安全管理体系认证旨在帮助组织建立、实施、保持和改进供应链安全管理体系，识别和控制供应链各环节的安全风险（如信息泄露、物流中断、供应商合规问题等），保障供应链的连续性、稳定性和安全性，提升组织供应链管理水平和市场竞争力。

二、适用范围及技术规范

2.1 适用范围

本规则适用于所有涉及供应链活动的组织，包括但不限于制造业、零售业、物流运输业、信息技术服务业、医药行业、食品行业等，无论其规模、类型和供应链复杂程度如何。申请认证的组织应具有明确的供应链范围（如采购、生产、仓储、运输、销售、回收等环节），且供应链活动符合相关法律法规要求。

2.2 技术规范

组织实施供应链安全管理体系应符合以下标准及规范：

ISO 28000:2022《安全和复原力－安全管理系统－要求》；

国家及地方关于供应链安全、数据安全、物流安全、产品质量安全等相关法律法规（如《中华人民共和国数据安全法》《中华人民共和国安全生产法》《中华人民共和国物流行业安全管理办法》等）；

行业特定的供应链安全管理要求（如医药行业的冷链物流安全规范、汽车行业的零部件供应链追溯要求等）。

三、基本要求

3.1 ZXB 应获得国家认监委批准或备案后方可开展供应链安全管理体系认证。

3.2 申请认证的组织应具备合法经营资质，提供有效的营业执照、相关行业许可证书（如涉及特殊行业）等证明文件。

3.3 组织应建立符合本规则及相关技术规范要求的供应链安全管理体系，体系文件应包括但不限于：供应链安全方针和目标、管理手册、程序文件、作业指导书、记录表单等，且文件应具有适宜性、充分性和可操作性。

3.4 供应链安全管理体系应已正式运行至少 3 个月，且组织能提供体系运行的相关证据（如运行记录、风险评估报告、内部审核报告、管理评审报告等）。

3.5 组织应承诺遵守认证相关规定，配合认证机构的审核活动，提供真实、完整的信息和资料。

四、对认证人员的要求

4.1 应具备 CCAA 任一管理体系审核员资格，经 ZXB 技术部评价后可获得供应链安全管理体系审核员资格。

4.2 审核员应具备以下专业能力：

熟悉供应链管理相关知识，包括供应链规划、采购管理、物流运作、库存控制、供应商管理等环节；

掌握供应链安全风险识别、评估和控制的方法（如风险矩阵、故障模式与影响分析 FMEA 等）；

了解相关法律法规、技术规范及行业特点，能结合组织实际识别供应链安全合规风险；

具备良好的沟通能力、分析判断能力和现场审核经验，能独立完成审核任务并出具客观的审核报告。

4.3 审核人员应遵守职业道德规范，保持公正性、客观性和保密性，不得与申请认证的组织存在可能影响审核公正性的利益关系。

五、受理程序

5.1 受理认证申请

5.1.1 ZXB 需通过网站或文件向申请认证的组织（以下简称“申请组织”）至少公开以下信息：

（1）可开展认证业务的范围，以及获得认可的情况；

（2）ZXB 授予、保持、扩大、更新、缩小、暂停或撤销认证及其证书等环节的制度规定；

（3）认证证书样式；

（4）对认证决定的申诉程序；

（5）分支机构和办事机构的名称、业务范围、地址等。

5.1.2 组织向认证机构提交书面认证申请，申请材料应包括：

（1）《管理体系认证申请书》（需明确认证范围、组织基本信息等）；

（2）有效的营业执照、行业许可证书、资质证书等的复印件；

（3）供应链安全管理体系文件（管理手册、程序文件清单等）；

（4）组织架构图、供应链流程图（明确供应链各环节及涉及的外部方）；

（5）体系运行证明材料（如风险评估报告、内部审核报告、管理评审报告等）；

（6）其他必要的补充材料（如多场所组织的场所清单、外包过程说明等）。

5.1.2 认证机构在收到申请材料后，应在 5 个工作日内确认材料是否齐全，对材料不齐全的，应通知组织补充，补充材料时间不计入受理时限。

5.2 申请评审

5.2.1 认证机构对申请材料进行评审，评审内容包括：

1）组织经营资质的有效性；

2）认证范围的适宜性（是否与组织实际供应链活动一致）；

3）体系文件是否符合相关技术规范要求；

4）体系运行时间及证据的充分性；

5）组织是否存在影响认证的重大问题（如违法违规记录、重大供应链安全事故未处理等）。

5.2.2 评审通过的，进入下一环节；评审未通过的，认证机构应书面通知组织，说明未通过原因，组织可在整改后重新申请。

5.3 签订认证合同

5.3.1 申请评审通过后，认证机构与组织签订《管理体系认证合同》，明确双方权利和义务、认证范围、审核安排、认证费用、证书有效期、保密条款、争议解决方式等内容。

5.3.2 合同签订后，组织应按合同约定支付认证费用。

5.4 审核时间

5.4.1 认证机构根据组织的规模、供应链复杂程度、认证范围等因素，参照本规则附录 A《供应链安全管理体系认证审核时间表》确定审核人日数。

5.4.2 初次认证审核分为第一阶段和第二阶段，两阶段审核间隔时间一般不超过 3 个月（特殊情况经双方协商可适当延长，但最长不超过 6 个月）。

5.4.3 审核时间应在审核计划中明确，如需调整，认证机构与组织应提前沟通并达成一致。

5.4.4 在特殊情况下，可以减少审核时间，但减少的时间不得超过附录 A 所规定的审核时间的 30%。整个审核时间中，现场审核时间不应少于 80%。

5.5 受理转换认证证书

5.5.1 组织从其他认证机构转换至本机构申请供应链安全管理体系认证的，应提交以下材料：

转换认证申请书；

原认证证书复印件及最近一次审核报告；

原认证机构的注销证明或不存在未了事宜的声明；

本规则 5.1.1 中要求的其他材料（如体系文件、运行证据等）。

5.5.2 认证机构对转换申请进行评审，必要时可进行现场审核（重点关注体系的连续性和有效性），符合要求的，按本规则规定授予认证证书，原证书有效期可连续计算。

5.5.2.3 被暂停的证书不能转证。

六、审核准备

6.1 方案策划

认证机构根据组织的规模、供应链结构（如单一场所 / 多场所、简单 / 复杂供应链）、风险等级等制定审核方案，明确审核目的、范围、准则、方法、阶段划分及审核人日数，确保审核的充分性和有效性。审核方案应经认证机构相关负责人批准。

审核方案应包括两个阶段初次审核，第一年和第二年的监督审核和第三年再认证到期前进行的再认证审核。三年的认证周期从初次认证/再认证决定算起。审核方案的确定和任何后续调整应考虑受审核组织的规模、供应链安全管理体系的范围、

体系的复杂程度和风险级别、供应链安全管理体系文件的变化情况、以及经过证实的管理体系有效性水平和以往审核的结果等。

6.2 审核组

6.2.1 认证机构根据审核方案组建审核组，审核组成员应具备与组织行业特点、供应链类型相关的专业能力，必要时可聘请技术专家提供支持（技术专家不参与审核结论表决，技术专家主要负责提供认证审核的技术支持，不作为审核员实施审核，不计入审核时间，其在审核过程中的活动由审核组中的审核员承担责任。）。

6.2.2 审核组组长由认证机构指定，负责审核组的管理、审核计划的实施及审核报告的编制。

6.2.3 认证机构应将审核组组成情况书面通知组织，组织如对审核组成员有异议且有合理理由的，可在收到通知后 3 个工作日内提出，认证机构应予以协调解决。

6.3 审核计划

6.3.1 审核组组长在审核前编制审核计划，内容包括：

1）审核目的、范围、准则；

2）审核时间、地点及日程安排（明确各阶段审核的具体时间、审核部门 / 环节、审核员分工）；

3）审核组成员及职责；

4）需组织配合的事项（如提供资料、安排陪同人员、确定访谈对象等）；

5）审核报告的提交时间。

6.3.2 审核计划应在审核前 5 个工作日提交组织确认，组织无异议的，按计划实施；有异议的，双方协商调整。

七、实施审核

7.1 初次认证第一阶段

7.1.1 第一阶段审核目的：确认组织的供应链安全管理体系文件与相关标准的符合性，评估体系运行的基本情况，识别重大供应链安全风险及潜在问题，为第二阶段审核提供依据。

7.1.2 审核内容包括：

1）供应链安全方针、目标的适宜性和合理性；

2）体系文件的完整性、系统性（如是否覆盖供应链各环节的安全管理要求）；

3）风险评估过程的充分性（如风险识别是否全面、评估方法是否科学）；

4）内部审核和管理评审的实施情况；

5）组织对第二阶段审核的准备情况。

7.1.3 第一阶段审核可采用文件审核与现场抽查相结合的方式，审核结束后，审核组出具第一阶段审核报告，明确是否具备第二阶段审核条件。如存在影响第二阶段审核的问题，组织应完成整改后再进行第二阶段审核。

7.2 初次认证第二阶段

7.2.1 第二阶段审核目的：全面评估供应链安全管理体系运行的有效性，验证体系是否达到认证要求，能否实现组织的供应链安全方针和目标。

7.2.2 审核内容包括：

1）供应链各环节（采购、生产、物流、仓储、销售等）安全管理措施的实施情况及有效性；

2）风险控制措施的落实情况（如供应商准入审核、物流运输监控、信息安全防护等）；

3）员工对供应链安全知识的掌握程度及职责履行情况；

4）不符合项的纠正情况（如第一阶段审核发现问题的整改效果）；

5）供应链安全绩效指标的达成情况（如安全事故发生率、供应链中断时长等）。

7.2.3 第二阶段审核以现场审核为主，通过查阅记录、现场观察、员工访谈、数据分析等方式收集审核证据，形成审核发现。

7.3 不符合项的纠正和纠正措施及其结果的验证

7.3.1 审核组根据审核证据，对不符合相关标准或体系文件要求的事项，开具不符合项报告，明确不符合项的性质（轻微或严重）、事实描述及整改要求。

7.3.2 组织应在收到不符合项报告后，在规定期限内（轻微不符合项一般不超过 1 个月，严重不符合项一般不超过 3 个月）制定纠正措施计划，实施纠正和纠正措施，并提交整改报告及相关证据。

7.3.3 审核组对组织的整改情况进行验证，可采用文件验证或现场验证的方式。验证通过的，不符合项关闭；未通过的，组织需重新整改，直至验证通过。严重不符合项未在规定期限内完成整改的，本次审核不予通过。

7.4 审核报告

7.4.1 审核组在审核结束后（且不符合项验证通过后）编制审核报告，报告内容包

括：

（1）申请组织的名称和地址；

（2）审核的申请组织活动范围、产品和员工人数；

（3）审核组组长、审核组成员及其任何所使用的技术专家(适用时)及其个人注册信息；

（4）审核活动的实施日期和天数；

（5）接受审核的过程和每个受审核过程的绩效完成情况；

（6）识别出的不符合项。不符合项的表述，应基于客观证据和审核依据，用写实的方法准确、具体、清晰描述，易于被申请组织理解。不得用概念化的、不确定的、含糊的语言表述不符合项；

（7）审核组对是否通过认证的意见建议。

7.4.2 审核报告可随附必要的用于证明相关事实的证据或记录，包括文字或照片等音像资料。

7.4.3 ZXB 需将最终审核报告提交申请组织，并保留签收或提交的证据。

7.4.4 对终止审核的项目，审核组应将已开展的工作情况形成报告，ZXB 将此报告及终止审核的原因提交给申请组织，并保留签收或提交的证据。

7.4.5 在出现严重不符合项时，要求在 3 个月内进行现场跟进审核，直到达到标准后再提交完整报告。

八、认证决定

8.1 认证机构在收到审核报告及相关材料后，由认证决定人员对审核结论、体系运行情况、整改效果等进行综合评价，做出认证决定。

8.2 审核组成员不得参与对审核项目的认证决定。

8.3 认证决定分为 “通过认证”“不通过认证” 两种：

审核结论为推荐通过，且无影响认证的重大问题的，做出 “通过认证” 决定，授予认证证书；

存在以下情况之一的，做出 “不通过认证” 决定：审核结论为不推荐通过；严重不符合项未有效整改；提供虚假材料或隐瞒重要信息；存在重大违法违规行为等。

8.4 认证机构应将认证决定书面通知组织，不通过认证的，应说明原因，并告知组织可在整改后重新申请认证。

九、监督审核程序

9.1 监督审核目的：验证组织供应链安全管理体系的持续有效性，确保其符合认证要求，及时发现并纠正体系运行中的问题。

9.2 监督审核频次：认证证书有效期内，每年至少进行 1 次监督审核。对于高风险行业或体系运行存在问题的组织，认证机构可增加监督频次。

9.3 监督审核时间：首次监督审核应在认证证书颁发后 12 个月内进行，后续监督审核间隔不超过 12 个月。监督审核人日数参照附录 A 执行，人日为初次审核人日数的 1/3，可适当调整。但整个认证周期内监督审核总时间不得低于按 5.4 条计算初次审核人日数的 2/3。

9.4 监督审核内容：

1）体系方针、目标的实现情况及适应性；

2）关键供应链安全风险的控制效果；

3）内部审核和管理评审的实施情况；

4）以往不符合项的持续改进情况；

5）体系变更（如供应链结构调整、重大工艺变化等）的符合性和有效性；

6）顾客反馈及供应链安全事故的处理情况。

9.5 监督审核流程：参照本规则 6.3（审核计划）、7.2（第二阶段审核方式）、7.3（不符合项整改）、7.4（审核报告）执行。

9.6 监督审核结论：监督审核通过的，保持认证资格；不通过的，按本规则 11.5（暂停认证证书）处理。

十、再认证程序

10.1 认证证书有效期为 3 年，组织应在证书到期前 3 - 6 个月向认证机构提出再认证申请，申请材料参照 5.1.1 执行。

10.2 再认证审核目的：全面评估供应链安全管理体系在证书有效期内的持续有效性、适宜性和充分性，以及组织对体系的改进情况，确认是否符合换发新证书的要求。

10.3 再认证审核范围与初次认证一致，必要时可根据组织实际情况调整。审核内容包括体系的持续运行有效性、管理评审的充分性、重大变更的控制情况、监督审核中发现问题的改进情况等。

10.4 再认证审核可采用 “完整体系审核” 或 “基于监督审核的简化审核” 方式：

完整体系审核：流程参照初次认证的第一阶段和第二阶段审核，但可适当简化第一阶段审核；

简化审核：获证组织的内部和外部环境无重大变更时，再认证审核可省略第一阶段审核。

10.5 再认证审核人日数一般为初次认证审核人日数的 2/3（具体参照附录 A）。

10.6 认证机构根据再认证审核结论做出再认证决定：通过的，换发新证书，证书有效期重新计算；不通过的，证书到期后自动失效，组织可在整改后重新申请认证。

十一、认证的批准、拒绝、保持、扩大、缩小、暂停、恢复或撤销认证证书

11.1 认证批准

组织通过初次认证或再认证审核，且符合认证要求的，认证机构批准认证，颁发认证证书。

11.2 认证拒绝

存在以下情况之一的，认证机构拒绝认证申请：

1）申请材料虚假或不完整，经补充后仍不符合要求；

2）供应链安全管理体系不符合相关标准及本规则要求，且无法在规定期限内有效整改；

3）拒绝配合认证机构的审核活动或干扰审核公正性；

4）存在重大违法违规行为或严重供应链安全事故未处理完毕。

11.3 认证保持

组织通过监督审核，且体系持续符合认证要求的，保持其认证资格和证书有效性。

11.4 认证范围扩大或缩小

11.4.1 扩大认证范围：组织因业务扩展需增加供应链环节或覆盖场所的，应向认证机构提出书面申请，提交新增范围的体系文件、运行证据等材料。认证机构对申请进行评审，必要时进行现场审核（审核人日数根据新增范围大小确定），审核通过的，变更认证证书范围。

11.4.2 缩小认证范围：组织因业务调整需减少供应链环节或覆盖场所的，应向认证

机构提出书面申请，说明原因。认证机构核实后，变更认证证书范围，原范围对应的认证资格终止。

11.5 认证证书暂停

组织存在以下情况之一的，认证机构暂停其认证证书，暂停期限一般不超过 6 个月：

1）监督审核发现体系运行存在严重问题，未在规定期限内整改；

2）未按规定接受监督审核或再认证；

3）供应链安全管理体系发生重大变更未及时通知认证机构；

4）存在轻微违法违规行为，但未造成严重后果；

5）其他可能影响体系有效性的情况。

认证机构暂停证书时，应书面通知组织，说明暂停原因、暂停期限及整改要求。暂停期间，组织不得使用认证证书及认证标志。

11.6 认证证书恢复

组织在暂停期限内完成整改，经认证机构验证符合要求的，恢复其认证证书有效性，并书面通知组织。

11.7 认证证书撤销

1）组织存在以下情况之一的，认证机构撤销其认证证书：

2）暂停期限内未完成整改或整改后仍不符合要求；

3）提供虚假材料或隐瞒重大信息，骗取认证证书；

4）发生重大供应链安全事故，且与体系失效直接相关；

5）存在严重违法违规行为，被相关部门处罚；

6）主动申请撤销认证证书；

7）其他严重违反认证规则或合同约定的行为。

认证机构撤销证书时，应书面通知组织，说明撤销原因，并收回原证书（无法收回的，公告作废）。自撤销之日起，组织不得使用认证证书及认证标志。

十二、认证证书及认证标志的要求

12.1 认证证书应包括以下信息：

（1）获证组织名称、地址和组织机构代码；

（2）供应链安全管理体系覆盖的生产经营或服务的地址和业务范围。若认证供应链安全管理覆盖多场所，表述覆盖的相关场所的名称和地址信息，该信息应与相

应的法律地位证明文件和/或列于产品标签的相关生产商的信息一致；

（3）供应链安全管理体系符合 ISO 28000：2022 标准的表述；

（4）证书编号；

（5）认证机构名称与标识；

（6）证书签发日期及有效期的起止年月日。对初次认证以来未中断过的再认证证书，可表述该获证组织初次获得认证证书的年月日；

（7）相关的认可标识及认可注册号（适用时）；

（8）证书信息按要求上报认证监管部门；此外，还可通过电话查询或书面向 ZXB 认证查询。

12.2 证书格式

认证证书格式由认证机构统一制定，应符合国家认证认可监管部门的要求，具有唯一性和防伪性。

12.3 证书有效期

认证证书有效期为 3 年，自发证之日起计算。

12.4 证书变更

组织名称、地址、法定代表人等信息发生变更的，应在变更后 30 日内书面通知认证机构，提交变更证明文件。认证机构核实后，换发变更后的证书，原证书有效期不变。

12.5 证书补发

证书遗失或损坏的，组织可向认证机构申请补发，提交补发申请书，认证机构核实后补发证书，补发证书与原证书内容一致，注明 “补发” 字样。

12.5 认证标志要求

a)获证客户在传播媒介(如互联网、宣传册或广告)或其他文件中引用认证状态时，应符合 ZXB 的要求。

b）使用 ZXB 的认证标志，需向 ZXB 提出申请。在使用时，其图案必须按照 ZXB 提供的 图案的比例放大或缩小，并且做到颜色一致。未经 ZXB 许可不得使用认证标志；

c）不得在任何资料中有关于其认证资格的误导性说明； d）不得以误导性方式使用认证文件或其任何部分；

e）不得利用管理体系认证证书和相关文字、符号，暗示或误导公众认为认证证书覆盖 范围外的管理体系、产品或服务、过程、活动和场所获得 ZXB 的认证；

f）宣传认证结果时不得损害 ZXB 的声誉和（或）使认证制度声誉受损，失去公众信任；g）不得擅自更改证书内容；

h）不得伪造、涂改、出借、出租、转让、倒卖、部分出示、部分复印证书；

i）获证客户应妥善保管好认证证书，以免丢失、损坏；

j）获证客户的管理体系若发生重大变化时，应及时报告 ZXB ，接受 ZXB 的调查或监督 检查。对经监督检查不合格者，不得继续使用认证证书；

k）在认证范围被缩小时，应及时修改所有的广告宣传材料；

l）认证证书被暂停期间，相应的认证领域的管理体系认证暂时无效。认证客户应停止 使用认证证书和认证标志，直到造成暂停的问题得到解决。如果客户在规定的时限内未能解 决造成暂停的问题，ZXB 将撤销或缩小相应领域的认证范围；

m）证书被 ZXB 撤销，获证客户应按 ZXB 的要求将证书交还给 ZXB ，并同时使用所有引 用认证资格的广告材料。停止在文件、网站、广告和宣传资料中或广告宣传等商业活动，以 及在工作场所、销售场所展示认证证书；

n）不应允许其标志被获证客户用于实验室检测、校准或检验的报告或证书；

o）标志不应用于产品或产品包装之上，或以任何其它可解释为表示产品符合性的方式 使用；注：产品包装的判别标准是其可从产品上移除且不会导致产品分裂、破裂或损坏。

p）认证证书和认证标志的使用应符合规定；

q）认证标志使用时可以等比例放大或缩小，但不允许变形、变色；

r）证书持有人应对认证证书和认证标志的使用和展示进行有效的控制。

十三、信息通报

13.1 认证机构应及时向国家认证认可监管部门报送认证信息（如认证证书颁发、暂停、撤销等），并按要求公开认证证书信息（可通过官网等渠道）。

13.2 认证机构在做出暂停、恢复、撤销认证证书等决定后，应在 5 个工作日内将相关信息通报组织及相关方（如客户、行业协会等，经组织同意或法律法规要求）。

13.3 组织发生以下情况之一的，应在 15 个工作日内书面通知认证机构：

供应链安全管理体系发生重大变更（如方针目标调整、组织结构重大变动、关键供应商更换等）；

发生重大供应链安全事故或相关投诉；

受到法律法规处罚或行业通报批评；

名称、地址、经营范围等注册信息变更；

其他可能影响体系有效性的重大事项。

十四、受理组织的申诉

14.1 组织对认证机构的认证决定（如拒绝认证、暂停或撤销证书等）有异议的，可在收到决定通知后 30 日内，向认证机构提交书面申诉，说明申诉理由并提供相关证据。

14.2 认证机构收到申诉后，应在 5 个工作日内进行登记，指定与原审核无关的人员组成申诉处理小组，在 60 日内完成调查核实，形成申诉处理报告，做出申诉处理决定（维持原决定、撤销原决定或重新审核），并书面通知组织。

14.3 组织对申诉处理结果仍有异议的，可向国家认证认可监管部门或相关行业协会投诉。

十五、认证记录的管理

15.1 认证机构应建立认证记录管理制度，对认证过程中的各类记录（如申请书、审核计划、审核报告、不符合项报告、认证决定文件、合同、申诉材料等）进行规范管理。

15.2 认证记录应真实、完整、清晰，具有可追溯性，保存方式可采用纸质或电子形式（电子记录需确保安全性和可读性）。

15.3 认证记录的保存期限为认证证书有效期满后至少 3 年；对于撤销或拒绝认证的记录，保存期限为决定做出后至少 3 年。

15.4 认证机构应采取措施防止记录丢失、损坏或泄露，未经组织同意，不得向第三方泄露记录内容（法律法规要求的除外）。

附录 A：供应链安全管理体系认证审核时间表

组织规模（员工人数）	初审审核人日数
1-50	1.5
51- 100	2.5
101 - 150	3.5
151 - 200	4.5
>200	遵循上述递进规律

注：

供应链复杂度划分可根据组织实际情况调整，多场所组织按每个场所增加 20%-30%的人日数；

特殊行业（如医药、航空航天等）可根据风险等级适当增加人日数；

审核人日数包含文件审核、现场审核、不符合项验证及报告编制时间。

国际标准

ISO 28000

第二版
2022-03

安全和复原力 - 安全管理系统 - 要求

参考编号 ISO 28000:2022(E)

内容

前言

ISO（国际标准化组织）是一个由国家标准机构（ISO成员机构）组成的全球联合会。制定国际标准的工作通常是通过ISO技术委员会进行的。每个对某一主题感兴趣的成员机构都有权在该技术委员会中任职。与国际标准化组织联络的国际组织、政府和非政府组织也参与这项工作。国际标准化组织与国际电工委员会（IEC）在所有电工标准化问题上紧密合作。

用于制定本文件的程序和打算进一步维护本文件的程序在ISO/IEC指令第1部分中有描述。特别要注意的是，不同类型的ISO文件需要不同的批准标准。本文件是根据ISO/IEC指令第2部分的编辑规则起草的（见www.iso.org/directives）。

请注意，本文件中的某些内容可能是专利权的对象。ISO不负责识别任何或所有此类专利权。在文件制定过程中发现的任何专利权的细节将在导言中和/或在ISO收到的专利声明列表中（见www.iso.org/patents）。

本文件中使用的任何商品名称是为方便用户而提供的信息，不构成对其的认可。

关于标准的自愿性质的解释，与合格评定有关的ISO特定术语和表达方式的含义，以及关于ISO在技术性贸易壁垒（TBT）中遵守世界贸易组织（WTO）原则的信息，见www.iso.org/iso/foreword.html。

本文件由ISO/TC 292技术委员会（*安全和复原力*）编写。

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条中加入了关于原则的建议，以便与ISO 31000更好地协调。

— 在第8条中增加了建议，以便与ISO 22301更好地保持一致，促进整合，包括。

  — 安全战略、程序、过程和处理。

  — 安全计划。

对本文件的任何反馈或问题应直接向用户的国家标准机构提出。这些机构的完整名单可在www.iso.org/members.html。

简介

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，他们希望在其管理系统中系统地解决这些问题。正式的安全管理方法可以直接促进组织的业务能力和可信度。

本文件规定了对安全管理系统的要求，包括对供应链安全保障至关重要的那些方面。它要求组织做到

— 评估其运作的安全环境，包括其供应链（包括依赖性和相互依赖性）。

— 确定是否有足够的安全措施来有效管理与安全有关的风险。

— 管理对组织所认同的法定、监管和自愿义务的遵守情况。

— 调整安全流程和控制，包括供应链的相关上游和下游流程和控制，以满足组织的目标。

安全管理与企业管理的许多方面相关联。它们包括由组织控制或影响的所有活动，包括但不限于对供应链有影响的活动。应考虑对组织的安全管理有影响的所有活动、功能和操作，包括（但不限于）其供应链。

关于供应链，必须考虑到供应链在本质上是动态的。因此，一些管理多个供应链的组织可能希望其供应商达到相关的安全标准，作为被纳入该供应链的一个条件，以满足安全管理的要求。

本文件将计划-执行-检查-行动（PDCA）模式应用于组织的安全管理系统的规划、建立、实施、运行、监控、审查、维护和持续改进其有效性，见表1和图1。

表1--PDCA模型的解释

计划(建立)	建立与改善安全有关的安全政策、目标、指标、控制、流程和程序，以提供与组织的总体政策和目标相一致的结果。
做 (实施和操作)	实施和操作安全政策、控制、程序和 程序。
检查 (监测和审查)	根据安全政策和目标监测和审查业绩，将结果报告给管理层进行审查， 并确定和授权采取补救和改进行动。
诉讼 (保持和改善)	根据管理审查的结果，采取纠正措施，维护和改进安全管理系统，重 新评估安全管理系统的范围和安全政策及目标。

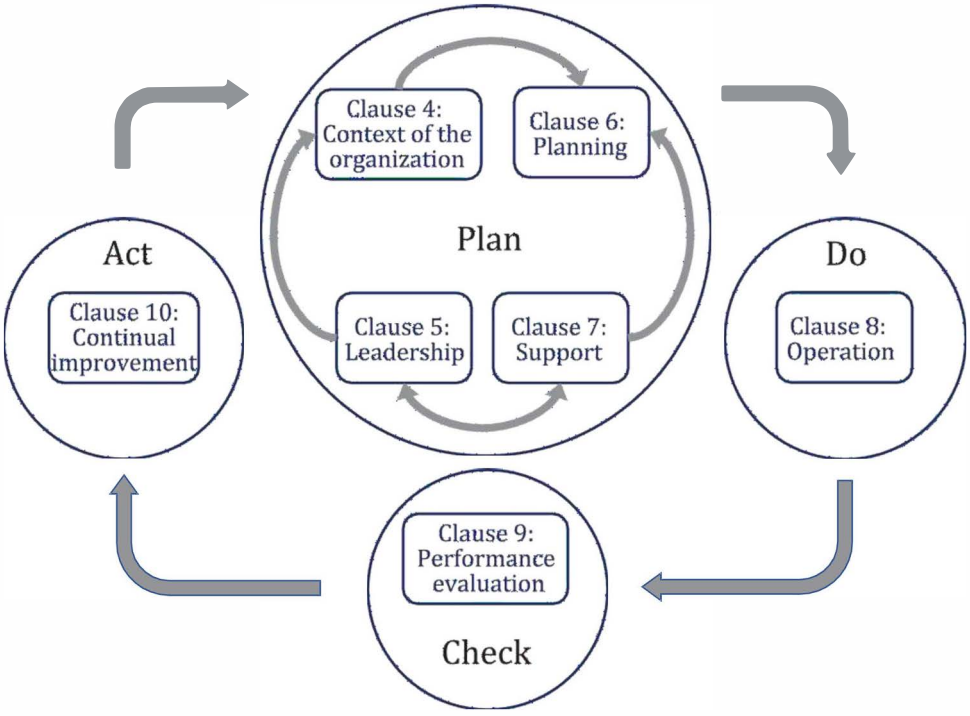

图1 - P DCA模型应用于安全管理系统

这确保了与其他管理体系标准，如ISO 9001、ISO 14001、ISO 22301、ISO/IEC 27001、ISO 45001等的一定程度的一致性，从而支持与相关管理体系的一致和综合实施和运行。

对于有此愿望的组织，可以通过外部或内部审计程序来验证安全管理系统与本文件的一致性。

安全和复原力 - 安全管理系统 - 要求

1 范围

本文件规定了安全管理系统的要求，包括与供应链相关的方面。

本文件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），它们打算建立、实施、维护和改进安全管理系统。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。

这份文件可以在组织的整个生命周期中使用，并且可以适用于任何活动，无论是内部的还是外部的，各级的。

2 规范性参考资料

以下文件在文中被提及，其部分或全部内容构成本文件的要求。对于注明日期的参考文献，仅适用于所引用的版本。对于未注明日期的参考文件，适用于所参考文件的最新版本（包括任何修正案）。

ISO 22300，*安全和复原力- 词汇表*

3 术语和定义

在本文件中，适用ISO 22300和下列术语和定义。国际标准化组织和国际电工委员会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：可在https://www.iso.org/obp

— IEC Electropedia：可在https://www.electropedia.org/

3.1
组织
有自己的职能、责任、权力和关系以实现其*目标的*人或团体（3.7）。

条目注1。组织的概念包括但不限于独资企业、公司、企业、公司、企业、当局、合伙企业、慈善机构或其部分或组合，无论是否成立、公共或私人。

条目注释2。如果该组织是一个较大实体的一部分，"组织 "一词仅指该较大实体中属于*安全管理系统*（3.5）范围的部分。

3.2
利害关系人
利益相关者
能影响、受影响或认为自己受某一决定或活动影响的人或*组织*（3.1）。

3.3
最高管理层
最高层指挥和控制*组织*的人或团体（3.1）。

条目注释1。最高管理层有权在组织内下放权力和提供资源。

条目注释2。如果*管理体系*的范围（3.4）只包括一个组织的一部分，那么最高管理层是指指导和控制该部分组织的人。

3.4
管理系统
一套相互关联或相互作用的*组织*要素（3.1），以建立*政策*（3.6）和*目标*（3.7），以及实现这些目标的*过程*（3.9）。

条目注释1。一个管理系统可以解决单一学科或几个学科的问题。

条目注释2。管理体系要素包括组织的结构、角色和责任、规划和运行。

3.5
安全管理系统
由协调的*政策*（3.6）、*程序*（3.9）和实践组成的系统，一个组织通过它来管理其安全*目标*（3.7）。

3.6
政策
一个*组织的*意图和方向（3.1），由其*最高管理层正式*表达（3.3）。

3.7
目标
要实现的结果

条目注释1。一个目标可以是战略的、战术的、或行动的。

条目注释2。目标可以与不同的学科有关（如财务、健康和安全以及环境）。例如，它们可以是整个组织的，也可以是针对某个项目、产品和*过程*的（3.9）。

条目注3。目标可以用其他方式表达，例如，作为预期的结果，作为目的，作为操作标准，作为安全目标，或通过使用具有类似含义的其他词汇（例如，目的，目标，或目标）。

条目注释4。在*安全管理系统*方面（3.5），安全目标是由*组织*制定的(3.1)，与*安全策略*(3.6)一致，以实现具体的结果。

3.8
风险
不确定性对*目标*的影响 (3.7)

条目注1。效果是对预期的偏离。它可以是积极的、消极的或两者兼而有之，并且可以解决、创造或导致机会和威胁。

条目注释2。目标可以有不同的方面和类别，也可以在不同的层面上应用。

条目注释3。风险通常用风险源、潜在事件、其后果和其可能性来表示。

3.9
过程
一组相互关联或相互作用的活动，使用或改变输入以提供一个结果。

条目注释1。一个过程的结果是否被称为产出、产品或服务，取决于背景。
的参考。

3.10
能力
运用知识和技能来实现预期结果的能力

3.11
记载的信息
一个*组织*需要控制和维护的信息（3.1）以及包含这些信息的媒介

条目注释1。记录的信息可以是任何格式和媒体，以及来自任何来源。条目注释2。记载的信息可以指。

— *管理系统*（3.4），包括相关*过程*（3.9）。

— 为组织运作而创建的信息（文件）。

— 取得成果的证据（记录）。

3.12
业绩
可衡量的结果

条目注释1。业绩可以与定量或定性的调查结果有关。

条目注释2。绩效可以涉及到管理活动、*流程*（3.9）、产品、服务、系统或*组织*（3.1）。

3.13
持续改进
提高*业绩*的经常性活动（3.12）。

3.14
效益
计划活动的实现程度和计划成果的实现程度

3.15
要求
陈述的、一般暗示的或强制性的需要或期望

条目注1。"一般暗示"是指该*组织*的习惯或通常做法(3.1)和*有关各方*（3.2），所考虑的需要或期望是隐含的。

条目注释2。规定的要求是指在*文件资料*中说明的要求（3.11）。

3.16
符合性
满足一项*要求*（3.15）。

3.17
不符合规定
不*符合要求*（3.15）。

3.18
纠正措施
采取行动，消除*不符合要求*的原因（3.17），防止再次发生。

3.19
审计
系统和独立的*程序*（3.9），以获得证据和客观地评价证据，以确定审计标准得到满足的程度。

条目注释1。审计可以是内部审计（第一方）或外部审计（第二方或第三方），也可以是联合审计（结合两个或多个学科）。

条目注释2。内部审计由*组织*（3.1）自己进行，或由外部单位代表组织进行。

条目注释3。"审计证据 "和 "审计标准 "在ISO 19011中定义。

3.20
测量
过程（3.9）来确定一个值

3.21
监测
确定一个系统、一个*过程*（3.9）或一项活动的状态

条目注1。为了确定状况，可能需要检查、监督或严格观察。

4 组织的背景

4.1 了解组织和其背景

组织应确定与其目的相关的、影响其实现安全管理体系预期结果能力的外部和内部问题，包括其供应链的要求。

4.2 了解有关各方的需求和期望

4.2.1 一般

该组织应确定：

— 与安全管理系统有关的有关各方。

— 这些相关方的相关要求。

— 这些要求中的哪些将通过安全管理系统来解决。

4.2.2 法律、监管和其他要求

该组织应：

a) 实施和维护一个程序，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) 确保在实施和维护其安全管理系统时考虑到这些适用的法律、法规和其他要求。

c) 记录这些信息并保持更新。

d) 酌情向有关方面传达这一信息。

4.2.3 原则

4.2.3.1 一般

组织内安全管理的目的是创造，特别是保护价值。

组织应采用图2中给出的、4.2.3.2至4.2.3.9中描述的原则。

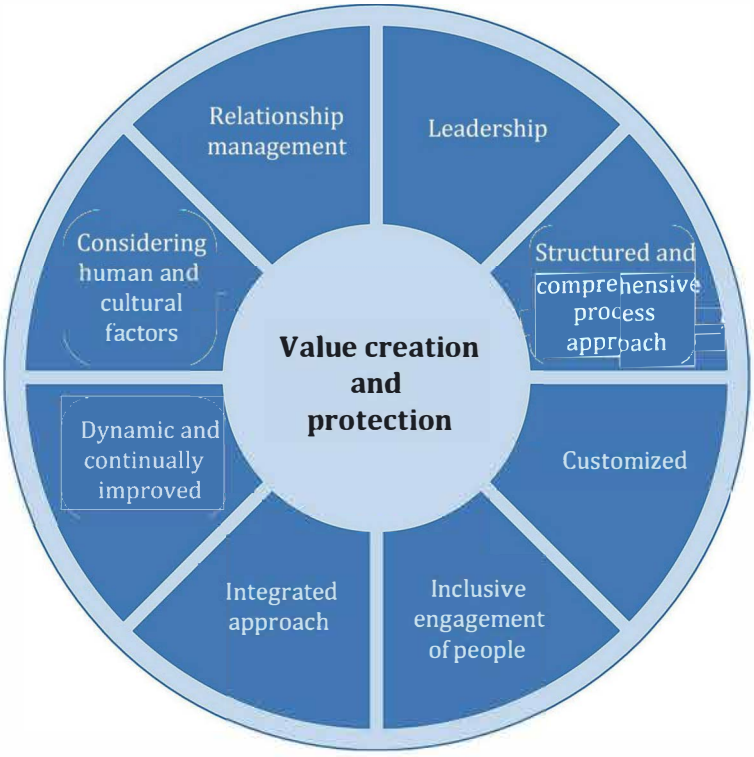

图2 - 原则

4.2.3.2 领导人

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、政策、程序和资源协调一致，以实现其目标。第5条解释了与此原则有关的要求。

4.2.3.3 基于现有最佳信息的结构化和全面的程序方法

包括供应链在内的结构化和全面的安全管理方法应有助于取得一致和可比较的结果，当各项活动被理解为作为一个连贯的系统运作的相互关联的过程并加以管理时，这些结果会更加有效和高效。

4.2.3.4 定制的

安全管理系统应该是定制的，与组织的外部和内部环境和需求相称。它应该与组织的目标相关。

4.2.3.5 人民的包容性参与

组织应适当地、及时地让有关各方参与进来。它应该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。组织应确保所有级别的人都得到尊重和参与。

4.2.3.6 综合方法

安全管理是所有组织活动的一个组成部分。它应该与组织的所有其他管理系统相结合。

组织的风险管理--无论是正式的、非正式的还是直观的--都应该被纳入安全管理系统。

4.2.3.7 充满活力并不断改进

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 考虑到人类和文化因素

人的行为和文化对安全管理的所有方面都有很大的影响，应该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估，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利益方的关系，因为他们可能会影响组织的绩效。

4.3 确定安全管理系统的范围

组织应确定安全管理体系的边界和适用性，以确定其范围。

在确定这一范围时，该组织应考虑： 1:

— 4.1中提到的外部和内部问题。

— 4.2中提到的要求。

该范围应作为文件信息提供。

如果一个组织选择由外部提供影响其安全管理体系符合性的任何流程，该组织应确保此类流程得到控制。应在安全管理体系中确定对这种外部提供的流程的必要控制和责任。

4.4 安全管理制度

组织应根据本文件的要求，建立、实施、维护并持续改进安全管理体系，包括所需的流程及其相互作用。

5 领导人

5.1 领导和承诺

最高管理层应通过以下方式展示对安全管理系统的领导和承诺。

— 确保安全政策和安全目标得到确立，并与组织的战略方向相一致。

— 确保识别和监测组织相关方的要求和期望，并及时采取适当行动管理这些期望，以确保将安全管理系统的要求纳入组织的业务流程。

— 确保将安全管理系统的要求纳入组织的业务流程。

— 确保安全管理系统所需的资源是可用的。

— 传达有效安全管理和符合安全管理系统要求的重要性。

— 确保安全管理系统实现其预期结果。

— 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系统。

— 指导和支持人员为安全管理系统的有效性作出贡献。

— 促进本组织安全管理系统的持续改进。

— 支持其他相关角色，以展示他们的领导力，因为这适用于他们的责任领域。

注本文件中 提到 的 "业务 "可被广义地解释为对组织存在的目的具有核心意义的那些活动。

5.2 安全政策

5.2.1 建立安全政策

最高管理层应制定一项安全政策，以便：

a) 与本组织的宗旨相适应。

b) 提供了一个设定安全目标的框架。

c) 包括承诺满足适用的要求。

d) 包括对持续改进安全管理系统的承诺。

e) 考虑安全政策、目标、指标、方案等对组织的其他方面可能产生的不利影响。

5.2.2 安全政策要求

安全政策应。

— 与其他组织政策相一致。

— 与组织的整体安全风险评估相一致。

— 规定在收购或与其他组织合并的情况下，或在组织的业务范围发生可能影响安全管理系统的连续性或相关性的其他变化时，应对其进行审查。

— 描述并分配主要的问责制和成果责任。

— 可作为文件信息提供。

— 在组织内部进行交流。

— 酌情向有关方面提供。

注意 组织可以选择制定详细的安全管理政策供内部使用，该政策将提供足够的信息和方向来驱动安全管理系统（其中部分内容可以保密），并有一个包含广泛目标的摘要（非保密）版本，以便向其有关各方传播。

5.3 角色、责任和权力

最高管理层应确保相关角色的责任和权限在组织内得到分配和沟通。

最高管理层应指定以下责任和权力：。

a) 确保安全管理系统符合本文件的要求。

b) 向最高管理层报告安全管理系统的绩效。

6 规划

6.1 应对风险和机遇的行动

6.1.1 一般

在规划安全管理体系时，组织应考虑4.1中提到的问题和4.2中提到的要求，并确定需要应对的风险和机会。

— 保证安全管理系统能够实现其预期结果。

— 防止或减少不期望的影响。

— 实现持续的改进。本组织应计

划：

a) 应对这些风险和机遇的行动。

b) 如何。

  — 将这些行动纳入其安全管理系统流程并加以实施。

  — 评估这些行动的有效性。

管理风险的目的是创造和保护价值。管理风险应被纳入安全管理系统。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会

确定与安全有关的风险以及识别和利用机会，需要进行积极主动的风险评估，其中应包括考虑但不限于以下因素。

a) 物理或功能故障以及恶意或犯罪行为。

b) 环境、人类和文化因素以及其他内部或外部环境，包括影响组织安全的组织控制之外的因素。

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) 供应商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会

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) 本组织的整体风险管理。

b) 风险处理。

c) 安全管理目标。

d) 安全管理流程。

e) 安全管理系统的设计、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 安全目标和实现这些目标的规划

6.2.1 确立安全目标

组织应在相关的职能和级别上确立安全目标。这些安全目标应： 1:

a) 与安全政策相一致。

b) 是可衡量的（如果切实可行）。

c) 考虑到适用的要求。

d) 被监测。

e) 被告知。

f) 酌情更新。

g) 可作为文件信息提供。

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。

— 将要做什么。

— 将需要哪些资源。

— 谁将负责。

— 何时完成。

— 如何对结果进行评估。

在建立和审查其安全目标时，一个组织应考虑到：

a) 技术、人力、行政和其他选择。

b) 对有关各方的意见和影响。

安全目标应符合组织对持续发展的承诺。
改进。

6.3 变化的规划

当组织确定需要对安全管理系统进行变更时，包括第10条中所确定的变更，应以有计划的方式进行。

该组织应考虑：

a) 变化的目的及其潜在的后果。

b) 安全管理系统的完整性。

c) 资源的可用性。

d) 职责和权限的分配或重新分配。

7 支持

7.1 资源

组织应确定并提供建立、实施、维护和持续改进安全管理系统所需的资源。

7.2 能力

该组织应：

— 确定在其控制下从事影响其安全性能的工作的人员的必要能力。

— 确保这些人在适当的教育、培训或经验的基础上胜任，并通过适当的安全审查。

— 在适用的情况下，采取行动以获得必要的能力，并评估所采取行动的有效性。

应提供适当的文件资料作为能力的证明。

可适用的行动包括，例如：为目前雇用的人员提供培训、指导或重新分配；或雇用或签约合格人员。

7.3 认识

在组织控制下从事工作的人应了解。

— 安全政策。

— 他们对安全管理系统的有效性的贡献，包括改进安全性能的好处。

— 不符合安全管理系统要求的影响。

— 他们在实现遵守安全管理政策和程序以及安全管理系统的要求方面的作用和责任，包括应急准备和反应要求。

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：1:

— 关于它将传达什么。

— 何时沟通。

— 与谁沟通。

— 如何沟通。

— 在传播之前，对信息的敏感性进行评估。

7.5 记录的信息

7.5.1 一般

该组织的安全管理系统应包括。

a) 本文件所要求的文件化信息。

b) 由组织确定为安全管理系统有效性所必需的文件化信息。

记载的信息应说明实现安全管理目标和指标的责任和权限，包括实现这些目标和指标的手段和时限。

注意 安全管理系统的文件化信息的范围可能因不同的组织而不同。

— 组织的规模及其活动、流程、产品和服务的类型。

— 过程的复杂性和它们的相互作用。

— 人的能力。

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 创建和更新文件化的信息

在创建和更新记录的信息时，组织应确保适当的。

— 识别和描述（例如，标题、日期、作者或参考号）。

— 格式（如语言、软件版本、图形）和媒体（如纸张、电子）。

— 审查和批准是否合适和充分。

7.5.3 对文件资料的控制

安全管理系统和本文件所要求的文件化信息应是
控制，以确保。

a) 在需要的地方和时间，它是可用的并适合使用的。

b) 它得到充分的保护（例如，防止失去保密性、不当使用或失去完整性）。

c) 定期审查并在必要时进行修订，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意外使用。

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。

对于文件化信息的控制，组织应酌情处理以下活动。

— 分发、访问、检索和使用。

— 储存和保存，包括保存可读性。

— 对变化的控制（如版本控制）。

— 保留和处置。

应酌情识别和控制由组织确定的、对安全管理系统的规划和运行来说是必要的外部来源的文件信息。

注意 访问权可以意味着关于只查看文件信息的权限，或查看和改变文件信息的权限和权力的决定。

8 运作

8.1 业务规划和控制

组织应通过以下方式计划、实施和控制满足要求所需的过程，并实施第6条中确定的行动。

— 为这些过程制定标准。

— 根据标准实施对过程的控制。

应在必要的范围内提供有记录的信息，以使人们相信这些过程已按计划进行。

8.2 确定过程和活动

该组织应确定那些为实现以下目标所必需的过程和活动。

a) 遵守其安全政策。

b) 遵守法律、法定和监管的安全要求。

c) 其安全管理目标。

d) 其安全管理系统的交付。

e) 供应链所需的安全水平。

8.3 风险评估和治疗

该组织应实施并保持风险评估和处理程序。

注意 : 风险评估和处理的过程在ISO 31000中涉及。

该组织应该：

a) 确定其与安全有关的风险，将它们与安全管理所需的资源进行优先排序。

b) 分析和评估已确定的风险。

c) 确定哪些风险需要治疗。

d) 选择并实施应对这些风险的方案。

e) 准备和实施风险处理计划。

注 本子条款中的风险与组织及其相关方的安全有关。与管理体系的有效性有关的风险和机会在6.1中处理。

8.4 控制措施

8.2中所列的流程应包括对人力资源管理的控制，以及酌情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、翻新和修改。如果对现有的安排进行了修订，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。要考虑的新的或修订的安排应包括：1:

a) 修订组织结构、角色或责任。

b) 培训、宣传和人力资源管理。

c) 修订安全管理政策、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) 酌情引进新的承包商、供应商或人员。

g) 对外部供应商的安全保证的要求。

组织应控制计划中的变更，并审查非预期变更的后果，必要时采取行动以减轻任何不利影响。

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 安全战略、程序、过程和处理

8.5.1 确定和选择战略和治疗方法

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。在这种脆弱性和威胁分析以及随之而来的风险评估的基础上，组织应确定并选择一种安全战略，其中包括一个或多个程序、过程和处理方法。

识别的依据应该是战略、程序、过程和处理的程度。

a) 维护本组织的安全。

b) 减少出现安全漏洞的可能性。

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) 规定提供足够的资源。

选择应基于战略、过程和治疗的程度。

— 满足保护组织安全的要求。

— 考虑本组织可能或不可能承担的风险数量和类型。

— 考虑相关的成本和效益。

8.5.2 所需资源

组织应确定实施所选安全程序、流程和处理方法的资源要求。

8.5.3 实施治疗

该组织应实施和维护选定的安全处理。

8.6 安全计划

8.6.1 一般

组织应根据选定的战略和处理方法，制定并记录安全计划和程序。组织应实施并维护一个响应结构，以便能够及时有效地警告并向有关方面通报与安全和迫在眉睫的安全威胁或正在发生的安全违规行为有关的漏洞。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团队负责应对与安全有关的漏洞和威胁。指定人员或每个小组的作用和责任以及这些人员或小组之间的关系应明确确定、沟通和记录。

集体而言，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) 需要采取的计划行动。

e) 以生命安全为第一优先，确定优先事项。

f) 监测与安全有关的漏洞的任何变化的影响，威胁者的意图和能力的变化或安全侵犯，以及组织的反应。

g) 激活安全处理。

h) 与有关各方、当局和媒体沟通。

i) 为沟通管理的沟通计划做出贡献。对于每个指定的人或团队来说，应

该有。

— 确定的工作人员，包括具有履行其指定职责的必要责任、权力和能力的候补人员。

— 指导其行动的成文程序，包括应对措施的启动、运作、协调和沟通的程序。

8.6.3 警告和沟通

该组织应记录并维护以下程序：

a) 向有关各方进行内部和外部沟通，包括沟通的内容、时间、对象和方式。

注意组织可以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记录下来，并加以维护。

b) 接收、记录和回应有关各方的来文，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、出现漏洞或威胁时通信手段的可用性。

d) 促进与安全威胁和/或违规行为应对者的结构化沟通。

e) 提供本组织在发生安全违规事件后的媒体反应细节，包括沟通策略。

f) 记录违反安全规定的细节、采取的行动和作出的决定。在适用的情况下，还应该考虑

并执行以下内容： 1:

— 提醒可能受到实际或即将发生的安全违规事件影响的有关各方。

— 确保多个响应组织之间的适当协调和沟通。

警告和通信程序应作为组织的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

组织应记录并维护安全计划。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) 各小组将采取的行动的细节，以。

   1) 继续或恢复商定的安全状态。

   2) 监测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) 参考预设的阈值和激活反应的过程。

c) 恢复组织的安全的程序。

d) 管理安全漏洞和威胁或实际或即将发生的安全违规行为的直接后果的细节，并适当考虑到： 1:

   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）损失或无法使用。每项计划应包括：

— 其目的、范围和目标。

— 实施该计划的团队的作用和责任。

— 实施解决方案的行动。

— 激活（包括激活标准）、操作、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。

— 一个退役的过程。

每个计划都应该是可用的，并在需要的时间和地点提供。

8.6.5 恢复

组织应拥有记录在案的流程，以便从安全违规行为发生之前、期间和之后采取的任何临时措施中恢复组织的安全。

9 业绩评估

9.1 监测、测量、分析和评价

该组织应确定：

— 需要监测和测量的内容。

— 监测、测量、分析和评价的方法（如适用），以确保有效的结果。

— 应在何时进行监测和测量。

— 应对监测和测量的结果进行分析和评估。

应提供有记录的资料作为结果的证据。

组织应评估安全管理系统的性能和有效性。

9.2 内部审计

9.2.1 一般

组织应按计划的时间间隔进行内部审计，以提供关于安全管理系统是否存在的信息。

a) 符合。

   1) 组织本身对其安全管理系统的要求。

   2) 本文件的要求。

b) 有效地实施和维护。

9.2.2 内部审计方案

该组织应计划、建立、实施和维持（一个）审计方案，包括频率、方法、责任、规划要求和报告。

在制定内部审计方案时，组织应考虑相关流程的重要性和以往审计的结果。

该组织应：

a) 确定每项审计的审计目标、标准和范围。

b) 选择审计员并进行审计，以确保审计过程的客观性和公正性。

c) 确保将审计结果报告给相关管理人员。

d) 核实安全设备和人员是否得到适当的部署。

e) 确保无不当拖延地采取任何必要的纠正措施，以消除所发现的不符合要求的情况及其原因。

f) 确保后续审计行动包括对所采取的行动进行核查并报告核查结果。

应提供有记录的信息，作为实施审计方案和审计结果的证据。

审计程序，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计的结果。审计程序应涵盖范围、频率、方法和能力，以及进行审计和报告结果的责任和要求。

9.3 管理审查

9.3.1 一般

最高管理层应按计划的时间间隔审查组织的安全管理系统，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系统有关的需求或机会，并作为持续改进的一部分加以解决。

注意 组织可以利用安全管理系统的流程，如领导、计划和绩效评估，来实现改进。

9.3.2 管理审查投入

管理审查应包括。

a) 以往管理审查的行动状况。

b) 与安全管理系统有关的外部和内部问题的变化。

c) 与安全管理系统有关的有关各方的需求和期望的变化。

d) 关于安全性能的信息，包括以下方面的趋势。

   1) 不符合要求的情况和纠正措施。

   2) 监测和测量结果。

   3) 审计结果。

e) 持续改进的机会。

f) 对遵守法律要求和本组织同意的其他要求的审计和评估结果。

g) 来自外部相关方的通信，包括投诉。

h) 基金会的安全性能。

i) 目标和指标的实现程度。

j) 纠正行动的状况。

k) 以往管理审查的后续行动。

l) 不断变化的情况，包括与安全方面有关的法律、法规和其他要求的发展（见4.2.2）。

m) 改进建议。

9.3.3 管理审查结果

管理审查的结果应包括与持续改进机会有关的决定和对安全管理系统的任何修改需要。

应提供有记录的信息作为管理审查结果的证据。

10 改进

10.1 持续改进

组织应不断改进安全管理系统的适宜性、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 不合格品和纠正措施

当发生不符合要求的情况时，组织应： 1:

a) 对不符合要求的情况作出反应，并视情况而定。

   1) 采取行动来控制和纠正它。

   2) 处理后果。

b) 评估是否需要采取行动，消除不符合要求的原因，以使其不再发生或在其他地方发生，方法是：

   1) 审查不符合要求的情况。

   2) 确定不符合要求的原因。

   3) 确定是否存在或可能发生类似的不符合规定的情况。

c) 实施任何需要的行动。

d) 审查所采取的任何纠正措施的有效性。

e) 如有必要，对安全管理系统进行修改。

纠正措施应与所遇到的不符合项的影响相适应。应提供文件化的信息，作为以下方面的证

据。

— 不符合要求的性质和随后采取的任何行动。

— 任何纠正行动的结果。

— 对安全方面的调查。

   — 失败，包括近乎失误和错误警报。

   — 事件和紧急状况。

   — 不符合规定的情况。

— 采取行动，减轻此类故障、事故或不符合要求的情况所产生的任何后果。

程序应要求在实施前通过安全相关风险的评估过程对所有拟议的纠正行动进行审查，除非立即实施可以防止生命或公共安全面临的紧迫风险。

为消除实际和潜在的不符合要求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称。

书目

[1] ISO 9001，*质量管理体系-要求*

[2] ISO 14001，*环境管理系统--要求与使用指南ance*

[3] ISO 19011，*管理体系审计指南*

[4] ISO 22301，*安全和复原力--业务连续性管理系统--要求*

[5] ISO/IEC 27001，*信息技术-安全技术-信息安全管理系统-要求*

[6] ISO 28001，*供应链安全管理体系--实施供应链安全的最佳实践，评估和计划--要求和指导*

[7] ISO 28002，*供应链的安全管理系统--供应链中弹性的发展--要求与使用指南*

[8] ISO 28003，*供应链安全管理系统--对提供供应链安全管理系统审计和认证的机构的要求*

[9] ISO 28004-1，*供应链安全管理系统--ISO 28000的实施指南--第1部分。一般原则*

[10] ISO 28004-3，*供应链安全管理系统--ISO 28000实施指南--第3部分：中小型企业（非海港）采用ISO 28000的补充具体指导。*

[11] ISO 28004-4，*供应链安全管理体系--ISO 28000的实施指南--第4部分：如果遵守ISO 28001是一个管理目标，那么实施ISO 28000的补充具体指导。*

[12] ISO 31000，*风险管理--指南*

[13] ISO 45001，*职业健康与安全管理体系--要求与使用指南*

[14] ISO指南73，*风险管理 - 词汇表*

学会03.100.01; 03.100.70
基于20页的价格