安全和弹性-要求 安全管理系统

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。

本文件适用于打算建立、实施、维护和改进安全管理体系的所有类型和规模的组织（例如商业企业、政府或其他公共机构和非营利组织）。它提供了一种整体和通用的方法，而不是特定于行业或部门的。

本文件可在组织的整个生命周期中使用，并可应用于所有级别的内部或外部活动。

2 规范性引用

在文中引用下列文件时，其部分或全部内容构成本文件的要求。对于带日期的参考文献，仅引用的版本适用。对于未注明日期的参考文献，适用最新版本的参考文件（包括任何修订）。

ISO 22300, 安全性和弹性 - 词汇

3 术语和定义

出于本文件的目的，ISO 22300 和以下给出的术语和定义适用。 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/obp

IEC Electropedia：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个人或一群人（11）

条目注释 1：组织的概念包括但不限于个体经营者、公司、公司、公司、企业、权威机构、合伙企业、慈善机构或机构，或部分或组合其中，无论她是否合并，公共或私人。

条目注释 2：如果组织是较大实体的一部分，则术语“或组织”仅指更大实体范围内的部分安全管理系统（11）。

3.2
利益相关方（首选术语）的利益
相关者（admitted term）
个人或组织（11）可以影响、受其影响或认为自己受其影响的决定或活动

3.10
权限
运用知识和技能实现预期结果的能力

3.11
文件化信息
组织（11）需要控制和维护的信息及其包含的介质

条目注释 1：文件化信息可以采用任何格式和媒体，也可以来自任何来源。注 2：成文信息可指：

管理体系[3..i)，包括相关流程(3..2)；

为组织运作而创建的信息（文档）；已取得成果的证据（记录）。

3.12
表现
可衡量的结果

条目注释 1：性能可以与定量或定性发现相关联。

条目注 2：绩效可能与管理活动、流程（3..2)、产品、服务、系统或*组织（.11）*。

3.13
持续改进
提高绩效的经常性活动（.3. 1.2)

3.14
效力
计划活动的实现程度和计划结果的实现程度

3.15
要求
明示的、通常暗示的或强制性的需要或期望

条目注 1："通常暗示"是指组织（.3..1）的习惯或惯例，并且利益相关方（11）所考虑的需要或期望是隐含的。

条目注释 2：指定的要求是规定的要求，例如在文件化信息（1J..1）中。

3.16
一致性
满足要求（.3.15.）

3.17
不合格
未满足要求（ ）

3.18
纠正措施
采取措施消除不合格（.3.J1.）的原因并防止再次发生

3.19
审计
系统和独立的过程（1.2），用于获取证据并对其进行客观评价，以确定满足审计标准的程度

注 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）。

注 2：内部审核由组织本身进行，或由外部方代表组织进行。

注 3："审核证据"和审核标准"在 ISO 19011 中定义。

3.20
测量
过程（1.2）确定一个值

3.21
监控
确定系统、过程（1.2）或活动的状态

注 1：为了确定状态，可能需要检查、监督或严格观察。

4 组织背景

4.1 了解组织及其背景

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（包括其供应链要求）的能力的外部和内部问题。

4.2 了解相关方的需求和期望

4.2.1 一般的

组织应确定：

与安全管理体系相关的利害关系方；这些利害关系方的相关要求；

这些要求中的哪些将通过安全管理系统得到解决。

4.2.2 法律、法规和其他要求

组织应：

a) 实施和维护一个流程，以识别、访问和评估与其安全相关的适用法律、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这些适用的法律、法规和其他要求；

c) 记录此信息并保持更新；

d) 酌情将此信息传达给相关利益方。

4.2.3 原则

4.2.3.1 一般的

组织内安全管理的目的是创造价值，尤其是保护价值。

组织应应用图 2 中给出的原则和 4.2.3.2 至 4.2.3.9 中描述的原则。

图 2 – 原则

4.2.3.2 领导力

各级领导要树立统一的宗旨和方向。他们应该创造条件，使组织的战略、政策流程和资源保持一致，以实现其目标。条款 5 解释了与此原则相关的要求。

4.2.3.3 基于最佳可用信息的结构化综合过程方法

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产生一致和可比较的结果，当活动被理解和管理为作为一个连贯系统运行的相互关联的过程时，这些结果将更加有效和高效地实现。

4.2.3.4 定制

安全管理系统应该根据组织的外部和内部环境和需求进行定制和相称。它应该与其目标相关。

4235 人们的包容性参与

组织应及时适当地让相关方参与。它应该适当地考虑他们的知识、观点和看法，以提高对知情安全管理的认识并促进知情安全管理。组织应确保所有级别的每个人都受到尊重和参与。

4236 综合方法

安全管理是所有组织活动的组成部分。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——都应该集成到安全管理系统中。

4237 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，应对变化并在组织的外部和内部环境发生变化时创造新的机会。

4238 考虑人文因素

人类行为和文化显着影响安全管理的所有方面，应在每个级别和阶段加以考虑。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、更有信心，并且更有可能产生预期的结果。应考虑个人看法。

4239 关系管理

为了持续成功，组织应管理其与所有相关方的关系，因为它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立其范围。

在确定此范围时，组织应考虑： U 中提到的外部和内部问

题；

在 U 中提到的要求。

该范围应作为文件化信息提供。

当组织选择从外部提供影响其安全管理体系符合性的任何过程时，组织应确保此类过程受到控制。此类外部提供过程的必要控制和职责应在安全管理体系中加以识别。

4.4 安全管理系统

组织应根据本文件的要求，建立、实施、保持并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

5.1 领导者的臂部和承诺

最高管理者应通过以下方式展示对安全管理体系的领导和承诺：

确保安全策略和安全目标的建立并与组织的战略方向相一致；

确保组织相关方的要求和期望得到识别和监控，并采取适当的及时行动来管理这些期望，以确保将安全管理体系要求整合到组织的业务流程中；

确保将安全管理体系要求整合到组织的业务流程中；

确保安全管理系统所需的资源可用；

传达有效安全管理和符合安全管理体系要求的重要性；

确保安全管理体系达到预期结果；确保安全管理目标、指标和方案的可行性；

确保从组织的其他部分生成的任何安全程序补充安全管理系统；

指导和支持人员为安全管理体系的有效性做出贡献；

促进组织安全管理体系的持续改进；

支持其他相关角色，以展示其领导者在其职责范围内的时尚。

笔记　本文档中对“业务”的引用可以广义地解释为那些活动核心是组织存在的目的。

5.2 安全政策

5.2.1 建立安全策略

最高管理层应制定安全政策：

a) 不适合组织的宗旨；

b) 提供设定安全目标的框架；

c) 包括满足适用要求的承诺；

d) 包括对持续改进安全管理系统的承诺；

e) 考虑安全策略、目标、目标、计划等可能对组织的其他方面产生的不利影响。

5.2.2 安全政策要求

安全政策应：

与其他组织政策保持一致；

与组织的整体安全风险评估保持一致；

在收购或合并其他组织，或组织的业务范围发生其他变化时，可能影响安全管理体系的连续性或相关性的情况下，规定其审查；

描述和分配结果的主要问责制和责任；可作为文件化信息使用；

在组织内传达；

酌情提供给感兴趣的各方。

注：组织可以选择内部使用的详细安全管理政策，这将提供足够的信息和方向来驱动安全管理系统（部分内容可以保密），并有一个总结（非保密）版本，其中包含传播给他们感兴趣的各方的广泛目标。

5.3 角色、职责和权限

最高管理者应确保相关角色的职责和权限在组织内得到分配和沟通。

最高管理者应分配职责和权限：

a) 确保安全管理体系符合本文件的要求；

b) 向最高管理层报告安全管理体系的绩效。

6 规划

6.1 应对风险和机遇的行动

6.1.1 一般的

在策划安全管理体系时，组织应考虑 i1 中提到的问题和 i1 中提到的要求，并确定需要解决的风险和机遇：

保证安全管理系统能够实现其预期结果；防止或减少不良影响；

实现持续改进。

组织应策划：

a) 应对这些风险和机遇的行动；

b) 如何：

将这些措施整合并实施到其安全管理系统流程中；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。风险管理应纳入安全管理体系。与组织及其利益相关方的安全相关的风险在 .8.1 中说明。

6.1.2 确定与安全相关的风险并识别机会

确定与采矿安全相关的风险并识别和利用机会需要进行主动的风险评估，其中应包括但不限于以下方面的考虑：

a) 物理或功能故障以及恶意或犯罪行为；

b) 环境、人文和文化因素以及其他内部或外部环境，包括组织无法控制的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、知识和沟通管理；

e) 与安全威胁和漏洞相关的信息；

f) 供应商之间的相互依赖性。

6.1.3 解决与安全相关的风险并利用机会

对已识别的安全相关风险的评估应为（但不限于）提供输入：

a) 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) 确定充足的资源，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计划

6.2.1 建立安全目标

组织应在相关职能和层次建立安全目标。安全目标应：

a) 与安全政策保持一致；

b) 可衡量（如果可行）；

c) 考虑适用的要求；

d) 被监控；

e) 被传达；

f) 适当更新；

g) 可作为文件化信息。

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： 将做什么；

需要什么资源；谁来负责；

什么时候完成；

如何评估结果。

在建立和评审其安全目标时，组织应考虑：

a) 技术、人力、行政和其他选择；

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 变更计划

当组织确定需要更改安全管理体系时，包括第 10 条中确定的那些。变更应有计划地进行。

组织应考虑：

a) 变更的目的及其潜在后果；

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所需的资源。安全管理体系的实施、维护和持续改进。

7.2 权限

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和培训的基础上能够胜任。或经验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；

应提供适当的文件化信息作为能力的证据。

笔记 适用的行动可以包括，例如：提供培训，指导。或当前雇用人员的重新分配；或聘用或签约有能力的人员。

7.3 意识

在组织控制下工作的人员应了解：安全政策；

他们对安全管理系统有效性的贡献，包括提高安全性能的好处；

不符合安全管理体系要求的后果；

他们在遵守安全管理政策和程序以及安全管理系统的要求（包括应急准备和响应要求）方面的作用和责任。

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：

关于它将传达什么；何时沟通；

与谁沟通；

如何沟通；

传播前信息的敏感性。

7.5 文件化信息

7.5.1 一般的

组织的安全管理体系应包括：

a) 本文件要求的文件化信息；

b) 组织确定的为安全管理体系的有效性所必需的文件化信息。

文件化信息应描述实现安全管理目标和目标的职责和权限，包括实现这些目标和目标的方法和时间表。

笔记 由于以下原因，安全管理体系的文件化信息的范围可能因组织而异：

组织的规模及其活动、流程、产品和服务的类型；过程及其相互作用的复杂性；

人的能力。

组织应确定信息的价值，并建立完整性要求的级别和安全控制以防止未经授权的访问。

7.5.2 创建和更新文件化信息

在创建和更新文件化信息时，组织应确保适当的：

- 标识和描述（例如标题、日期、作者或参考编号）；

格式（例如语言、软件版本、图形）和媒体（例如纸质、电子）；审查和批准

适当性和充分性。

7.5.3 文件化信息的控制

应控制安全管理体系和本文件要求的文件化信息，以确保：

a) 在需要的时间和地点可用并适合使用；

b) 它得到充分保护（例如，防止失去机密性、不当使用或失去完整性）；

c) 根据需要定期审查和修订，并由授权人员批准其充分性；

d) 过时的文件、数据和信息被及时从所有问题点和使用点移除，或以其他方式保证不会被意外使用；

e) 为法律或知识保存目的或两者而保留的档案文件、数据和信息被适当地识别。

对于文件化信息的控制，适用时，组织应处理以下活动：

分发、访问、检索和使用；

存储和保存，包括保持易读性；变更控制（例如版本控制）；

保留和处置。

组织确定的安全管理体系的策划和运行所必需的外部来源的文件化信息应予以识别、适当和控制。

注：访问可能意味着决定只允许查看文件化信息，或查看和更改文件化信息的许可和授权。

8 手术

8.1 1 运营计划和控制

组织应策划、实施和控制满足要求所需的过程，并通过以下方式实施第 6 条中确定的措施：

为过程建立标准；

根据标准实施过程控制。

文件化信息应在必要的范围内可用，以确信过程已按计划进行。

8.2 过程和活动的识别

组织应识别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、法规和监管安全要求；

c) 其安全管理目标；

d) 交付其安全管理系统；

e) 供应链所需的安全级别。

8.3 风险评估和处理

组织应实施并保持风险评估和处理过程。

笔记　　风险评估和处理过程在 ISO 31000 中有所规定。

组织应该：

a) 识别其与安全相关的风险，将它们优先于其安全管理所需的资源；

b) 分析和评估已识别的风险；

c) 确定哪些风险需要处理；

d) 选择并实施解决这些风险的方案；

e) 制定和实施风险处置计划。

注：本子条款中的风险与组织及其利益相关方的安全有关。与管理体系有效性相关的风险和机遇在 il 中进行了说明。

8.4 控件

B. . 2 中列出的过程应包括对人力资源管理的控制，以及与安全相关的设备、仪器和信息技术项目的设计、安装、操作、翻新和修改（如适用）。如果修订现有安排或引入可能对安全管理产生影响的新安排，组织应在实施前考虑相关的安全相关风险。需要考虑的新的或修订的安排应包括：

a) 修改后的组织结构、角色或职责；

b) 培训、意识和人力资源管理；

c) 修订后的安全管理政策、目标、指标或方案；

d) 修改后的流程和程序；

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) 酌情引入新的承包商、供应商或人员；

g) 外部供应商的安全保证要求。

组织应控制计划的变更并评审非预期变更的后果，必要时采取措施减轻任何不利影响。

组织应确保与安全管理体系相关的外部提供的过程、产品或服务受到控制。

8.5 安全策略、程序、过程和处理

8.5.1 识别和选择策略和治疗

组织宜实施和维护系统化过程，以分析与安全相关的漏洞和威胁。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、过程和处理。

识别应基于策略、程序、过程和治疗的程度：

a) 维护组织的安全；

b) 减少安全漏洞的可能性；

c) 减少威胁被实现的可能性；

d) 缩短任何安全处理缺陷的持续时间并限制其影响；

e) 提供充足的资源。

选择应基于策略、过程和处理的程度： 满足保护组织安全的要求；

考虑组织可能承担或不承担的风险的数量和类型；考虑相关的成本和

收益。

8.5.2 资源要求

组织应确定实施选定安全规程、过程和处理的资源需求。

8.5.3 实施治疗

组织应实施和维护选定的安全措施。

8.6 安全计划

8.6.1 一般的

组织应根据选定的策略和处理方法建立并记录安全计划和程序。组织应实施和维护一个响应结构，该结构将能够及时有效地向相关方发出与安全相关的漏洞和迫在眉睫的安全威胁或持续的安全违规行为的警告和沟通。响应结构应提供在迫在眉睫的安全威胁或持续的安全违规期间管理组织的计划和程序。

8.6.2 响应结构

组织应实施和维护一种结构，确定指定人员或一个或多个团队负责响应与安全相关的漏洞和威胁。指定人员或每个团队的角色和职责以及人员或团队之间的关系应明确识别、传达和记录。

总的来说，团队应该有能力：

a) 评估安全威胁的性质和程度及其潜在影响；

b) 根据预定义的阈值评估影响，这些阈值证明启动正式响应是合理的；

c) 启动适当的安全响应；

d) 计划需要采取的行动；

e) 以生命安全为第一要务，确立优先次序；

f) 监控与安全相关的漏洞的任何变化的影响、威胁行为者的意图和能力的变化或安全违规行为以及组织的响应；

g) 启动安全处理；

h) 与相关利益方、当局和媒体进行沟通；

i) 与沟通管理一起制定沟通计划。对于每个指定的人或团队，应该

有：

确定的工作人员，包括具有履行其指定职责所需的责任、权力和能力的候补人员；

指导他们行动的书面程序，包括响应的启动、操作、协调和沟通的程序。

8.6.3 警告与沟通

组织应记录和维护以下程序：

a) 与相关方进行内部和外部沟通，包括沟通内容、时间、与谁以及如何沟通；

笔记 组织可以记录和维护有关组织如何以及在什么情况下与员工及其紧急联系人进行沟通的程序。

b) 接收、记录和回应来自相关方的通信，包括任何国家或地区风险咨询系统或同等系统；

c) 确保在安全违规、漏洞或威胁期间通信手段的可用性；

d) 促进与应对安全威胁和/或违规行为的人员进行结构化沟通；

e) 提供组织在安全违规后的媒体响应的详细信息，包括通信策略；

f) 记录安全违规的详细信息、采取的行动和做出的决定。在适用的情况下，还应

考虑并实施以下内容：

提醒可能受到实际或即将发生的安全违规影响的相关方；确保多个响应组织之间的适当协调和沟通。

警告和沟通程序应作为组织测试和培训计划的一部分来执行。

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，以协助团队对安全漏洞、威胁和/或违规行为做出响应，并协助组织做出响应并恢复其安全性。

总体而言，安全计划应包含：

a) 团队将采取的行动详情：

1) 继续或恢复商定的安全状态；

2) 监控实际或即将发生的安全威胁、漏洞或违规的影响以及组织对其的响应；

b) 参考预定义的阈值和激活响应的过程；

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违规的直接后果的详细信息，其中应适当考虑：

1) 个人福利；

2) 资产、信息和人员的价值可能受到损害 d;

3) 防止核心活动（进一步）损失或不可用。每个计划应包

括：

其宗旨、范围和目标；

将实施该计划的团队的角色和职责；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赖；它的资源需

求；

其报告要求；一个站下来

的过程。

每个计划都应该在需要的时间和地点可用和可用。

8.6.5 恢复

组织应有文件化的过程，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 绩效评估

9.1 监测，测量，分析和评价

组织应确定：

需要监控和测量的内容；

监测、测量、分析和评估的方法（如适用）以确保有效的结果；

何时进行监测和测量；

何时应对监视和测量的结果进行分析和评价。

记录的信息应作为结果的证据提供。

组织应对安全管理体系的绩效和有效性进行评价。

9.2 内部审计

9.2.1 一般的

组织应按计划的时间间隔进行内部审核，以提供有关安全管理体系是否：

a) 符合：

1) 组织自身对其安全管理体系的要求；

2) 本文件的要求；

b) 得到有效实施和维护。

9.2.2 内部审计计划

组织应策划、建立、实施和保持审核方案，包括频率、方法、责任、策划要求和报告。

在制定内部审核方案时，组织应考虑相关过程的重要性和以前审核的结果。

组织应：

a) 确定每次审计的审计目标、标准和范围；

b) 选择审核员并进行审核以确保审核过程的客观性和公正性；

c) 确保将审核结果报告给相关管理人员。

d) 验证安全设备和人员是否得到适当部署；

e) 确保采取任何必要的纠正措施而不会无故拖延，以消除检测到的不合格及其原因；

f) 确保后续审计行动包括对所采取行动的验证和验证结果的报告。

应提供已记录的信息作为实施审核方案和审核结果的证据。

审核方案（包括任何时间表）应基于组织活动的风险评估结果和先前审核的结果。审计程序应包括范围、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 管理评审

9.3.1 一般的

最高管理者应按计划的时间间隔评审组织的安全管理体系，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输出，以确定是否有与业务或安全管理系统相关的需要或机会应作为持续改进。

注：组织可以使用安全管理体系的过程，如领导、策划和绩效评价，来实现改进。

9.3.2 管理评审输入

管理评审应包括：

a) 以前管理评审的行动状态；

b) 与安全管理体系相关的外部和内部问题的变化；

c) 与安全管理体系相关的相关方需求和期望的变化；

d) 有关安全性能的信息，包括以下方面的趋势：

1) 不符合项和纠正措施；

2) 监测和测量结果；

3) 审核结果；

e) 持续改进的机会；

f) 符合法律要求和组织同意的其他要求的审核和评估结果；

g) 来自外部利益相关方的沟通，包括抱怨；

h) 组织的安全性能；

i) 目标和目标的实现程度；

j) 纠正措施的状态；

k) 先前管理评审的后续行动；

l) c 悬而未决的情况，包括法律、法规和其他要求的发展（见 ）与安全方面有关；

m) 改进建议。

9.3.3 管理评审结果

管理评审的结果应包括与持续改进机会相关的决定以及对安全管理体系的任何变更需求。

文件化信息应作为管理评审结果的证据提供。

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，即使不是由与安全相关的漏洞和迫在眉睫的安全威胁或对相关方的持续安全违规行为引起的。

10.2 不合格和纠正措施

当发生不符合时，组织应：

a) 对不合格作出反应，并在适用时：

1) 采取措施加以控制和纠正；

2) 处理后果；

b) 通过以下方式评估采取行动消除不合格原因的必要性，以使其不再发生或在别处发生：

1) 审查不符合项；

2) 确定不合格的原因；

3) 确定是否存在或可能发生类似的不合格；

c) 实施所需的任何行动；

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更改。

纠正措施应与所遇到的不合格的影响相适应。文件化信息应作为以下证据提供：

不合格的性质和采取的任何后续行动；

任何纠正措施的结果；安全相关

的调查：

故障，包括未遂事故和误报；事件和紧急情

况；不合格；

采取行动减轻此类故障、事件或不合格引起的任何后果。

程序应要求所有建议的纠正措施在实施之前通过安全相关风险的评估过程进行审查，除非立即实施可以防止对生命或公共安全的迫在眉睫的暴露。

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称。