

ICS

T/GXDSL

团 体 标 准

T/GXDSL 296—2025

信息安全管理体系实施指南

Guideline for Implementation of Information Security Management Systems

征求意见稿

2025 - - 发布

2025 - - 实施

广西电子商务企业联合会 发布

目 次

前 言 II

1 范围1

2 规范性引用文件1

3 术语和定义1

4 核心原则1

5 实施框架与流程2

6 关键控制措施实施指南 5

前 言

本文件依据GB/T 1.1-2020 《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由广西产学研科学研究院提出。

本文件由广西电子商务企业联合会归口。

本文件起草单位：

本文件主要起草人：

本文件为首次发布。

信息安全管理体系实施指南

1 范围

本标准规定了信息安全管理体系（ISMS）的建立、实施、运行、监视、评审、保持和改进的全流程要求，包括核心原则、实施框架、关键过程、工具方法、评价指标及应用示例。

本标准适用于各类组织（包括企业、事业单位、政府部门、社会组织等），无论其规模、行业属性、信息化程度如何，均可依据本标准建立和优化信息安全管理体系，也可作为第三方机构开展 ISMS 咨询、审核、评估的参考依据。

本标准填补当前市场中 ISMS 实施缺乏“行业适配 + 落地细节”的空白，针对不同场景（如数字化转型组织、远程办公场景、供应链协同环境）提供差异化实施路径，解决现有标准过于通用、可操作性不足的问题。

2 规范性引用文件

下列文件对于本文件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文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

- GB/T 22080-2016 信息技术 安全技术 信息安全管理体系 要求
- GB/T 22081-2016 信息技术 安全技术 信息安全管理体系 实践指南
- ISO/IEC 27001:2022 信息技术 安全技术 信息安全管理体系 要求
- ISO/IEC 27002:2022 信息技术 安全技术 信息安全控制实用规则
- ISO/IEC 27003:2017 信息技术 安全技术 信息安全管理体系 指南
- ISO/IEC 27005:2022 信息技术 安全技术 信息安全风险管理
- NIST SP 800-30 Rev.1 风险管理框架指南
- 网络安全法（中华人民共和国主席令第五十三号）
- 数据安全法（中华人民共和国主席令第八十四号）
- 个人信息保护法（中华人民共和国主席令第九十一号）

3 术语和定义

GB/T 22080-2016、ISO/IEC 27001:2022、ISO/IEC 27002:2022 界定的以及下列术语和定义适用于本文件。

3.1 信息安全管理体系（ISMS）

组织在整体或特定范围内建立信息安全方针和目标，以及实现这些目标所用方法的体系，包括组织结构、职责、惯例、程序、过程和资源。

3.2 风险处置

选择并实施措施以修改风险的过程，包括规避、转移、降低、接受等方式。

3.3 控制措施

为应对风险而采取的政策、程序、技术、方法或组织安排。

3.4 适用性声明（SoA）

组织为说明其信息安全管理体系符合本标准要求，以及所选择和实施的控制措施满足其特定信息安全需求而编制的文件。

3.5 持续改进

根据内部审核结果、管理评审结论、外部反馈、法律法规变化等，对 ISMS 进行定期优化和完善的过程。

4 核心原则

4.1 战略对齐原则

ISMS 的建立和实施应与组织的业务战略、发展目标保持一致，确保信息安全为业务发展提供支撑，而非形成阻碍。组织应识别业务流程中的核心信息资产，将信息安全要求融入业务全生命周期。

4.2 风险导向原则

以风险管理为核心，基于对内外部环境的分析和风险评估结果，确定控制措施的优先级，确保资源投入到高风险领域，实现风险的可控可管。

4.3 全员参与原则

信息安全并非仅由 IT 部门负责，而是需要组织所有部门、所有岗位人员共同参与。应建立全员信息安全意识培养机制，明确各岗位的信息安全职责。

4.4 持续适配原则

ISMS 应具备动态调整能力，随着组织业务变化、技术发展、法律法规更新、威胁态势演变，及时调整方针、目标、控制措施，确保体系的有效性和适用性。

4.5 合规性原则

ISMS 的实施应符合国家相关法律法规、行业监管要求以及组织自身的规章制度，确保信息处理活动合法合规，规避法律风险。

5 实施框架与流程

5.1 实施框架

ISMS 实施遵循“策划 - 实施 - 运行 - 监视 - 评审 - 改进”（PDCA）的循环框架，具体包括 6 个阶段：启动与准备、风险评估与规划、体系设计与文件编制、体系实施与运行、监视与评审、持续改进，形成闭环管理。

5.2 阶段 1：启动与准备

5.2.1 成立实施团队

明确 ISMS 负责人（建议由高层管理者担任），组建跨部门实施团队，包括 IT、法务、人力资源、业务部门等代表，明确各成员的职责和分工。

示例：某制造企业成立以总经理为组长，IT 总监、法务经理、生产部门负责人为副组长，各部门安全员为成员的 ISMS 实施小组，负责体系建设全流程推进。

5.2.2 现状调研与差距分析

调研组织当前的信息安全管理现状，包括现有制度、流程、技术措施、人员意识、IT 基础设施等。对照本标准及相关法律法规要求，识别存在的差距，明确改进方向和重点。

工具：现状调研问卷、差距分析表（见附录 A）。

5.2.3 获得高层支持

向高层管理者汇报 ISMS 建设的必要性、预期目标、资源需求及预期效益，争取高层对体系建设的认可和支持，确保资源投入和跨部门协调。

5.3 阶段 2：风险评估与规划

5.3.1 资产识别与分类

采用“自上而下 + 自下而上”结合的方式，识别组织的信息资产，包括硬件、软件、数据、服务、人员、文档、无形资产等。

对识别的资产进行分类分级（如核心资产、重要资产、一般资产），明确资产的所有者、保管者、使用范围和重要性程度。

工具：资产清单模板（见附录 B）、资产分级标准（见附录 C）。

5.3.2 威胁与脆弱性识别

威胁识别：结合行业特点和外部环境，识别可能对信息资产造成损害的潜在因素，包括人为威胁（如恶意攻击、内部泄露、操作失误）、自然威胁（如地震、洪水、火灾）、技术威胁（如系统漏洞、软件故障、设备老化）。

脆弱性识别：分析信息资产在技术、管理、流程等方面存在的薄弱环节，如缺乏访问控制机制、未定期进行漏洞扫描、员工安全意识薄弱等。

工具：威胁清单（见附录 D）、脆弱性评估表（见附录 E）。

5.3.3 风险分析与评价

风险分析：评估威胁发生的可能性、脆弱性被利用的程度，以及威胁发生后对组织造成的影响（包括财务损失、声誉损害、业务中断、合规风险等），计算风险值。

风险评价：根据组织的风险承受能力（风险准则），对分析后的风险进行分级（如高风险、中风险、低风险），确定需要处置的风险。

方法：可采用定性分析（如风险矩阵法）、定量分析（如数值计算法）或两者结合的方式。

工具：风险矩阵（见附录 F）、风险评价表（见附录 G）。

5.3.4 风险处置计划制定

针对高、中风险，制定风险处置方案，选择合适的风险处置方式：

规避：停止可能引发高风险的业务活动或流程；

转移：通过购买保险、签订服务协议等方式将风险转移给第三方；

降低：实施控制措施，降低威胁发生的可能性或影响程度；

接受：对于低风险，在风险准则允许的范围内，可选择接受风险，但需定期监控。

明确风险处置的责任部门、责任人、实施期限、资源需求和预期效果。

5.4 阶段 3：体系设计与文件编制

5.4.1 信息安全方针制定

由高层管理者批准发布信息安全方针，明确组织的信息安全目标、承诺和总体要求，方针应具有可理解性、可执行性和可评审性。

示例：“本组织承诺保障信息资产的机密性、完整性和可用性，遵守相关法律法规和合同约定，建立并持续改进信息安全管理体系，保护客户、员工和组织的合法权益。”

5.4.2 目标与指标设定

基于信息安全方针，设定具体的信息安全目标和指标，目标应符合 SMART 原则（具体、可衡量、可实现、相关、有时限）。

示例：“202X 年底前，完成全员信息安全培训覆盖率 100%；重要系统漏洞修复及时率 $\geq 95\%$ ；未发生重大信息安全事件。”

5.4.3 组织结构与职责划分

明确信息安全管理组织结构，界定各部门、各岗位的信息安全职责，形成“高层负责、部门协同、全员参与”的责任体系。

关键职责包括：ISMS 负责人职责、IT 部门安全职责、业务部门安全职责、人力资源部门安全培训职责、法务部门合规审核职责等（见附录 H）。

5.4.4 文件体系编制

ISMS 文件体系分为四个层级，确保文件的系统性、协调性和可操作性：

一级文件（方针文件）：信息安全方针、目标；

二级文件（程序文件）：规定关键过程的流程和要求，如风险评估程序、访问控制程序、事件管理程序、变更管理程序等；

三级文件（作业指导书）：具体的操作步骤和方法，如设备操作手册、漏洞扫描指南、应急处置预案等；

四级文件（记录表单）：用于记录体系运行过程中的相关信息，如资产清单、风险评估报告、培训记录、审核报告等。

适用性声明（SoA）编制：明确适用的控制措施、不适用的控制措施及理由，说明控制措施如何满

足组织的信息安全需求。

5.5 阶段 4：体系实施与运行

5.5.1 全员培训与意识提升

针对不同岗位人员，开展分层分类的信息安全培训：

高层管理者：重点培训 ISMS 的战略意义、管理职责和评审要求；

中层管理者：重点培训部门安全职责、风险处置和团队管理；

普通员工：重点培训安全基础知识、岗位安全操作规范、应急处理流程；

技术人员：重点培训安全技术防护、漏洞修复、事件响应等专业技能。

建立常态化培训机制，每年至少开展 1 次全员培训，新员工入职必须接受安全培训。

工具：培训教材模板（见附录 I）、培训效果评估表（见附录 J）。

5.5.2 控制措施落地

按照文件体系要求，落实各项控制措施，包括：

技术控制：访问控制、加密技术、防火墙、入侵检测 / 防御系统、漏洞扫描、数据备份与恢复等；

管理控制：制度执行、流程管控、权限审批、变更管理、供应商管理、应急管理等；

物理控制：机房安全、设备防护、环境监控、门禁管理等。

针对不同行业和场景的特殊要求，补充差异化控制措施：

数字化转型组织：云安全管理、数据治理、API 安全、DevSecOps 流程融入；

远程办公场景：VPN 安全、终端安全管理、数据防泄露、远程访问权限控制；

供应链协同环境：供应商安全评估、数据共享安全协议、第三方访问控制。

5.5.3 内部沟通与协同

建立信息安全沟通机制，定期发布安全公告、风险预警、事件通报等信息，确保各部门之间的信息畅通。

针对跨部门的信息安全事项，建立协同工作机制，明确沟通流程和责任分工。

5.6 阶段 5：监视与评审

5.6.1 日常监视与记录

对 ISMS 的运行过程进行日常监视，记录关键活动和结果，包括：

控制措施执行情况：如访问权限审批记录、漏洞修复记录、备份执行记录等；

安全事件情况：如事件发生时间、原因、影响范围、处置过程和结果等；

培训情况：如培训次数、参与人数、考核成绩等；

合规性情况：如法律法规遵循情况、合同义务履行情况等。

5.6.2 内部审核

定期开展内部审核（建议每年至少 1 次），验证 ISMS 是否符合本标准要求、是否得到有效实施和保持。

组建内部审核团队（审核员应具备相应资质和能力），制定审核计划，明确审核范围、准则、方法和时间安排。

审核过程包括审核准备、现场审核、审核报告编制、纠正措施跟踪验证等环节。

工具：内部审核计划模板（见附录 K）、审核检查表（见附录 L）、审核报告模板（见附录 M）。

5.6.3 管理评审

由高层管理者主持开展管理评审（建议每年至少 1 次，可与年度经营评审结合），评价 ISMS 的有效性、充分性和适宜性。

管理评审的输入包括：内部审核结果、外部审核反馈、安全事件分析、风险评估更新结果、法律法规变化、业务变化、员工反馈、持续改进建议等。

管理评审的输出包括：ISMS 改进决策、方针和目标调整、资源配置优化、纠正和预防措施等，并

形成管理评审报告。

5.6.4 合规性评价

定期开展合规性评价（建议每半年至少 1 次），检查 ISMS 的实施是否符合相关法律法规、行业标准和合同要求，识别合规风险，及时采取整改措施。

5.7 阶段 6：持续改进

5.7.1 改进机会识别

通过内部审核、管理评审、安全事件分析、客户反馈、员工建议、技术发展、法律法规更新等多种渠道，识别 ISMS 的改进机会。

5.7.2 纠正与预防措施

针对发现的不符合项和潜在问题，分析根本原因，制定并实施纠正措施和预防措施，明确责任部门、责任人、实施期限和验证要求。

跟踪措施的实施效果，确保问题得到有效解决，防止类似问题再次发生。

5.7.3 体系优化升级

根据改进结果和内外环境变化，对 ISMS 的方针、目标、文件体系、控制措施等进行优化升级，持续提升体系的有效性和适用性。

建立持续改进的跟踪机制，记录改进过程和结果，形成改进案例库，为后续体系优化提供参考。

6 关键控制措施实施指南

6.1 访问控制

6.1.1 访问权限管理

遵循“最小权限原则”和“职责分离原则”，为每个用户分配必要的最小访问权限，避免权限重叠和过度授权。

建立访问权限申请、审批、变更、撤销的全流程管理机制，员工离职或岗位调整时，应及时撤销或调整其访问权限（最长不超过 24 小时）。

定期开展权限审计（至少每季度 1 次），清理冗余权限和无效账号。

6.1.2 身份认证与授权

核心系统和重要数据应采用多因素认证（如密码 + 动态口令、密码 + 生物识别），普通系统应采用强密码策略（密码长度 ≥ 8 位，包含大小写字母、数字、特殊字符，定期更换，周期不超过 90 天）。

建立分级授权机制，根据资产重要性和岗位职责，划分不同的授权等级，明确授权审批流程。

6.2 数据安全

6.2.1 数据分类分级

按照数据的敏感程度和重要性，将数据分为公开数据、内部数据、敏感数据、核心数据四个级别，明确各级数据的定义、标识和管理要求。

6.2.2 数据全生命周期安全

数据采集：确保采集渠道合法，获得必要的授权，明确数据采集范围和目的；

数据存储：核心数据和敏感数据应采用加密存储（如 AES-256 加密算法），定期进行数据备份（核心数据至少每天 1 次全量备份，实时增量备份），备份数据应异地存放；

数据传输：采用加密传输协议（如 SSL/TLS 1.2 及以上版本），避免数据在传输过程中被窃取或篡改；

数据使用：建立数据访问日志，记录数据使用情况，敏感数据的使用应进行审批和审计；

数据销毁：采用符合安全要求的销毁方式（如物理粉碎、多次覆写），确保数据无法恢复，销毁过程应留存记录。

6.3 安全事件管理

6.3.1 事件分类与响应流程

按照事件的严重程度，将信息安全事件分为特别重大事件、重大事件、较大事件、一般事件四个级别（见附录 N）。

建立事件响应流程，明确事件发现、报告、研判、处置、恢复、总结的各个环节的责任和要求，确保事件得到快速有效处置。
