ICS 35.030
CCS L 80

DB21

辽 宁 省 地 方 标 准

DB21/T 4171—2025

信息系统安全工程质量控制技术规范

Technical specification for quality control of information system security engineering

2025 - 08 - 30 发布　　2025 - 09 - 30 实施

辽宁省市场监督管理局　　发 布

目　　次

前　言

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

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。

本文件由辽宁省工业和信息化厅提出并归口。

本文件起草单位：北方实验室（沈阳）股份有限公司、辽宁鲲鹏生态创新中心有限公司、北京北实正安信息技术有限公司、辽宁北实网安信息技术有限公司、东北大学、沈阳市网络安全应急指挥中心。

本文件主要起草人：张健楠、丁琳、袁洪朋、李琳、张鏖、隋大智、郝瑞、蔡雨、魏凤娇、王健、姜海龙、赵奇、娄欣宇、郑宇、任鑫宇、李昂霄、赵鑫、孙鹏程、李佳伦、任庆峰、黄国城、李冰琪、王莹、姚羽、杨庆民。

本文件发布实施后，任何单位和个人如有问题和意见建议，均可以通过来电和来函等方式进行反馈，我们将及时答复并认真处理，根据实际情况依法进行评估及复审。

归口管理部门通讯地址：辽宁省工业和信息化厅（沈阳市皇姑区北陵大街45-2号），联系电话：024-86893258。

标准起草单位通讯地址：北方实验室（沈阳）股份有限公司（辽宁省沈阳市浑南区智慧三街199号），联系电话：400-664-5588。

信息系统安全工程质量控制技术规范

1 范围

本文件规定了信息系统安全工程需求调研、设计、实施和验收阶段的质量控制技术措施。

本文件适用于信息系统安全工程的需方、实施方、监理方等在需求调研、设计、实施、验收阶段的质量控制管理，其他有关各方也可参照使用。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 20282 信息安全技术 信息系统安全工程管理要求

GB/T 22081 信息技术 安全技术 信息安全控制实践指南

GB/T 25069 信息安全技术 术语

3 术语和定义

GB/T 25069、GB/T 22081、GB/T 20282、GB/T22032界定的以及下列术语和定义适用于本文件。

3.1

信息安全建设工程 information system security construction engineering

为确保信息系统的保密性、完整性、可用性等目标而进行的工程。

4 资格控制要求

4.1 人员资质要求

参与信息安全建设工程实施的人员应具备国家相关主管部门认可的安全服务人员、实施人员相应资质。

4.2 安全产品要求

信息安全建设工程所采用的安全产品应具有在国内生产、经营、销售的许可证，并符合相应等级。

5 需求调研阶段

5.1 目标

开展全面的需求调研和分析，识别安全风险，为工程后期的建设和质量控制提供重要依据。

5.2 内容

5.2.1 需求收集

本项控制措施包括：

a) 明确信息系统的业务目标、功能需求、性能需求，以及特定的安全需求，并加强数据安全需求的获取，确保需求的全面和准确；
b) 通过问卷调查、访谈、研讨会等方式，充分获取各利益相关方的安全需求；
c) 对收集到的需求进行整理、分类、汇总，并与各相关方确认，确保需求理解的一致性；
d) 根据安全需求确定系统的安全防护目标和级别。

5.2.2 风险评估

5.2.2.1 风险识别

本项控制措施包括：

a) 采用定性与定量相结合的方法，识别信息系统可能面临的信息安全威胁、脆弱性、影响及可能性，形成风险源列表；
b) 结合业务环境、系统架构、数据类型、用户行为等因素，全面考虑物理安全、网络安全、应用安全、数据安全、安全管理等方面的风险。

5.2.2.2 风险分析与评估

本项控制措施包括：

a) 对识别出的风险进行量化评分，计算风险值，确定风险等级；
b) 分析风险之间的关联性，识别可能引发连锁反应或放大效应的风险组合；
c) 评估风险对业务连续性、数据加密、数据完整性、隐私保护、合规性等方面的影响，形成风险评估报告。

5.2.2.3 风险应对策略制定

本项控制措施包括：

a) 根据风险评估结果，制定风险接受、转移、规避、减轻等应对策略，明确风险责任人及应对措施的具体实施计划；
b) 对于高风险项，应提出针对性强、可操作性强的缓解措施，并纳入项目实施计划。

5.2.3 需求分析与优先级排序

本项控制措施包括：

a) 对收集到的安全需求进行深入分析，识别其内在关联性、依赖关系及潜在冲突，形成清晰、具体的，包含风险评估结果、业务重要性、合规要求等内容的安全需求描述；
b) 明确项目中涉及的所有敏感数据类别，包含但不限于个人身份信息、健康记录、财务数据等，确保调研范围覆盖所有关键数据；
c) 根据风险评估结果、业务重要性、合规要求等因素，对安全需求进行优先级排序，综合分析脆弱性对系统的各类危害及潜在风险，确保资源投入与风险防控重点相匹配。

5.2.4 需求文档编制与审批

本项控制措施包括：

a) 编制需求文档材料，全面、系统、规范记录各项安全需求、风险分析、质量管理计划、验收规范标准，以及来源、描述、优先级与相关措施等信息，形成规范的送审版需求规格说明书；

b) 安排需求分析评审，组织专家评审或召开需求评审会议，对送审版需求规格说明书进行审查，确保需求的完整性、合理性和可行性；
c) 形成正式版需求规格说明书，并与各相关方确认，将需求规格说明书作为项目启动阶段的基础文档，为后续设计、实施、验收等阶段提供基本依据。

5.2.5 质量管理计划

5.2.5.1 质量管理框架

本项控制措施包括：
a) 根据项目特点和质量目标，选择适用的质量管理模型，构建项目质量管理框架；
b) 明确质量管理的组织结构、角色分工、工作流程、工具方法等基础要素。

5.2.5.2 质量控制需求

本项控制措施包括：
a) 在工程建设周期各阶段、关键任务、重大变更等环节明确控制需求，制定控制内容、控制标准、控制方法，并明确责任人；
b) 对于高风险、高复杂度的任务，应根据质量控制需求，增设专项质量控制措施。

5.2.5.3 质量检查与审计计划

本项控制措施包括：
a) 制定质量检查与审计计划，明确检查与审计的周期、内容、标准、方法、参与人员等，确保质量控制活动的常态化、制度化；
b) 针对关键里程碑、重要交付物等，安排专项质量检查或审计。

5.2.5.4 质量改进与应急响应机制

本项控制措施包括：
a) 建立质量问题跟踪与闭环管理机制，包括问题识别、原因分析、整改措施制定与执行、效果验证等环节的操作规程；
b) 制定应急响应预案，明确应急响应的触发条件、响应流程、责任分工、资源调配等内容，确保快速有效地应对质量问题或突发事件。

5.2.5.5 验收规范标准

验收标准规范制定的内容包括：
a) 合规性检查标准，项目验收标准应遵循相关的法律、规章、行业标准及内部政策要求；
b) 文档审查标准，要求审查项目过程中产生的所有文件记录，包括但不限于包括设计文档、过程文档、测试报告、运维手册等；
c) 功能验证标准，确保功能能够按照设计要求正确无误地执行，并响应需求；
d) 第三方评估的范围和内容，包含但不限于系统测试、等级保护测评、商用密码应用安全性评估、渗透测试等。

6 设计阶段

6.1 目标

应完成系统的架构设计、详细设计、接口设计和安全整体设计等，决定组成系统的配置项，确定系统指标，并完成设计的评审和审核工作。

6.2 内容

6.2.1 信息安全建设工程设计

6.2.1.1 需求理解与确认

本项控制措施包括：

a） 进行需求分析，以需求规格说明书及相关文档为基础，综合分析业务需求、功能需求、性能需求、安全需求、合规需求等，深入调研系统详细设计所需的相关参数，明确需求之间的关系和优先级；

b） 完成需求确认，与需方、安全团队、合规团队等进行深入沟通，澄清模糊、冲突、遗漏的设计需求，确保需求的准确和完整，并将结果以设计需求文档形式得到相关方的书面确认，确保工作优先级并保持关注。

6.2.1.2 系统架构设计

本项控制措施包括：

a） 首先完成架构选型，根据业务特点、技术发展趋势、成本效益分析等因素，选择合适的系统架构模式等；

b） 进行架构设计，绘制系统架构图，明确系统组成、组件关系、数据流向、安全域划分等关键要素，实现合理、可扩展以及安全合规的架构设计；

c） 开展架构评审，组织架构评审会，邀请业务专家、技术专家、安全专家等，对架构设计进行多角度、多层次的审查，确保架构设计科学、合理。

6.2.1.3 详细设计

本项控制措施包括：

a） 模块设计方面的要求，根据系统架构，细化各模块的功能、接口、数据、算法等设计，模块设计完整，并支持模块的重用；

b） 界面设计要求基于易用性需求设计用户界面、管理界面、监控界面等；

c） 开展详细设计评审，组织详细设计评审会，邀请业务专家、技术专家、安全专家等，对详细设计进行多角度、多层次的审查，确保详细设计的完整性和可行性。

6.2.1.4 接口设计

本项控制措施包括：

a） 明确接口定义，设计接口的名称、类型、参数、返回值、错误码、调用方式等信息，同时明确接口间的逻辑关系、接口和系统的逻辑关系、接口数值要求等，实现规范的、与架构一致的接口设计，并支持接口扩展；

b） 编写接口文档，包括接口说明、接口示例、接口测试、接口变更记录等内容，满足文档的完整性要求；

c） 开展接口设计评审，组织接口评审会，邀请业务专家、技术专家、安全专家等，对接口设计进行多角度、多层次的审查，确保接口设计满足数据交互和安全要求。

6.2.1.5 安全整体设计

本项控制措施包括：

a） 安全策略设计，制定访问控制策略、数据保护策略、网络安全策略、安全运维策略等，实现安全策略的设计完整、合理，并满足安全标准规范要求；

b） 安全机制设计，设计身份认证、授权管理、审计跟踪、数据加密、防火墙、入侵检测、反病毒等安全机制，采用交叉设计的策略，确保安全机制有效；

c） 运维流程设计，设计系统部署、系统升级、系统监控、系统备份、系统恢复、系统应急等运维流程，实现运维流程的规范设计，并且支持审计等安全管理要求；

d） 开展安全设计评审，组织安全设计评审会，邀请业务专家、技术专家、安全专家等，对安全设计进行多角度、多层次的审查，进一步落实安全设计科学合理和合规。

6.2.1.6 安全域划分

本项控制措施包括：

a） 根据系统架构的特点，如分布式系统、微服务架构、云计算环境等，确保安全域划分适应系统架构的特性，有效控制内部系统间以及与外部系统的交互；

b） 根据威胁模型分析和风险评估结果进行安全域划分，识别潜在威胁来源、攻击路径、脆弱点及可能的影响；

c） 根据业务流程、数据敏感性和重要性、服务功能以及系统间的依赖关系，将具有相似业务逻辑、密切交互或共享资源的系统划分为同一安全域，确保业务流程顺畅且安全控制措施得以有效实施。

6.2.1.7 访问控制设计

本项控制措施包括：

a） 实现身份认证、授权管理、审计跟踪等功能，确保只有合法用户才能访问授权资源；

b） 采用多因素认证、动态口令、生物特征识别等技术，增强身份认证的安全性；

c） 实施细粒度的访问控制策略，如基于角色、基于属性、基于风险的访问控制。

6.2.1.8 数据保护设计

本项控制措施包括：

a） 数据加密机制，根据数据敏感度，采用国密算法或国标算法，对传输和存储的数据实施强制加密，确保数据在不同环境下的保密；

b） 数据脱敏策略，对处理个人或敏感信息时，实行数据最小化原则，采用脱敏技术如数据混淆、泛化等，保护个人信息隐私，降低数据泄露风险；

c） 数据备份与恢复方案，建立定期自动备份机制，采用冗余存储技术，确保数据有多个副本。制定灾难恢复计划，确保在系统故障或数据丢失情况下，数据可迅速恢复至最近状态，保障业务的连续；

d） 可用性保障措施，实施负载均衡、高可用架构设计，确保服务在面临大量访问或单点故障时仍能稳定运行。

6.2.1.9 商用密码应用设计

本项控制措施包括：

a) 密码算法选型标准，商用密码系统应基于国家密码管理局批准的国密算法，确保算法的安全强度符合国家密码管理要求，为数据加密提供坚实基础；
b) 密钥管理体系，构建多层次、分布式的密钥管理系统，实现密钥的全生命周期管理，包括生成、分发、存储、更新、撤销和销毁，确保密钥的安全存储和高效使用；
c) 密码协议应用，在数据传输和认证过程中，采用符合要求的协议标准，结合国密套件，确保通信双方的身份验证、数据完整性及保密性，防范中间人攻击等安全威胁；
d) 密码安全审计，实施定期的密码应用安全审计，评估密码系统的有效性、合规性和潜在风险，包括密码算法的正确使用、密钥管理的合规性以及系统对密码攻击的抵抗能力，确保持续改进密码安全策略。

6.2.1.10 网络安全设计

本项控制措施包括：

a) 实现防火墙、入侵检测、入侵防御、分布式拒绝服务攻击防御、反病毒等功能，防止外部攻击、内部滥用、恶意软件传播等威胁；
b) 采用虚拟局域网、网络隔离区、子网划分等技术，实现网络隔离、访问控制、流量管理等目标；
c) 实施网络监控、日志分析、安全事件响应等措施，及时发现、处置网络安全事件。

6.2.1.11 安全支撑环境设计

本项控制措施包括：

a) 选择、配置、部署安全设备、软件、服务，形成安全防护支撑环境；
b) 实施安全设备的定期更新、升级、补丁管理、配置审计等运维工作，确保安全支撑环境的稳定性和有效性。

6.2.1.12 设计文档编制

本项控制措施包括：

a） 设计文档编制阶段，编制系统设计说明书、详细设计说明书、接口设计说明书、安全设计说明书、运维设计说明书等设计文档，实现设计文档规范、完整编制；
b） 开展设计文档审核，组织设计文档审核会，邀请业务专家、技术专家、安全专家等，对设计文档进行多角度、多层次的审查，确保设计文档能够满足用户需求规格说明书及相关文档的设计要求，符合信息安全技术和规范的发展方向。

6.2.1.13 设计变更控制

本项控制措施包括：

a） 首先进行变更申请，当设计需要变更时，应填写设计变更申请表，明确变更原因、变更内容、变更影响、变更方案等信息，提交审批；
b） 进行变更审批，组织设计变更评审会，邀请业务专家、技术专家、安全专家等，对设计变更进行多角度、多层次的审查，决定是否批准变更申请；

c） 管控变更实施，设计团队应根据批准的变更方案，修改设计文档、调整设计成果、更新设计评审记录等，确保设计变更的及时、准确、合规。

6.2.2 设计方案评审流程

6.2.2.1 设计评审组织

本项控制措施包括：

a) 建立跨部门、跨专业的设计评审小组，成员应包括业务专家、技术专家、安全专家、系统分析师、系统架构设计师等；
b) 设计评审小组负责制定评审计划、确定评审标准、组织评审会议、记录评审意见、跟踪整改情况等。

6.2.2.2 设计评审原则

本项控制措施包括：

a) 遵循最小权限原则、纵深防御原则、默认安全原则、安全即服务原则等，确保系统设计的安全性；
b) 采用成熟、公认的安全技术、产品、方案，避免使用未经验证的新技术、新产品、新方案。

6.2.2.3 设计评审步骤

本项控制措施包括：

a) 预审阶段设计人员自查设计文档，确保内容完整、格式规范、逻辑清晰，满足设计输入要求；
b) 初审阶段评审小组对设计文档进行初步审查，提出修改意见，设计人员进行修订；
c) 正式评审阶段评审小组召开评审会议，设计人员进行方案讲解，与会人员提问、讨论、投票，形成评审决议；
d) 复审阶段，针对初审或正式评审提出的重大问题，设计人员进行修改后，评审小组进行再次审查，直至问题解决。

6.2.2.4 设计评审内容

本项控制措施包括：

a) 功能与性能设计评审，功能设计应满足业务需求，性能设计应达到预期目标，不存在冗余、冲突、遗漏等问题；
b) 安全设计评审，评估安全控制措施覆盖所有识别风险情况，应符合安全需求规格说明书、安全基线、最佳实践等要求，不存在设计缺陷、安全隐患；
c) 合规性设计评审，核查设计符合相关法律法规、行业标准、组织政策等合规要求情况，应具备必要的合规证明材料。

6.2.2.5 设计评审输出

本项控制措施包括：

a) 输出评审报告，记录评审过程、评审意见、整改情况、评审结论等信息，作为设计阶段质量控制的重要证据；

b） 输出修订后的设计文档，根据评审意见修订的设计方案，应明确标识修改内容、修改原因、修改人、修改日期等信息。

7 实施阶段

7.1 目标

采取适合的质量控制措施保证信息安全建设工程在实施阶段达到各项质量目标要求。

7.2 内容

7.2.1 标准化与规范遵循

本项控制措施包括：

a） 标准与规范识别，根据项目特点和业务需求，识别适用的国际、国内及行业信息安全标准与规范；

b） 标准融入工程，在项目规划、设计、实施、运维各阶段，明确标准要求的具体落实措施，将其融入项目管理流程和文档体系；

c） 合规审计与监控，定期进行内部合规审计，检查项目执行符合选定的标准与规范情况；利用自动化工具进行实时合规监控，及时发现并纠正偏离标准的行为。

7.2.2 代码审查与安全测试

开展代码审查和安全测试的主要控制措施包含：

a） 代码审查，采用静态代码分析工具进行自动审查，配合人工审查，查找并修复代码中的安全缺陷。严格执行编码规范，避免常见编程错误；

b） 单元测试，针对模块功能和边界条件进行安全性测试，确保模块内部逻辑正确，无安全漏洞；

c） 集成测试，验证模块间交互的安全性，检查权限控制、数据隔离、通信加密等机制是否有效；

d） 系统测试，模拟真实环境，测试系统整体安全性能，包括身份认证、访问控制、数据保护、日志审计等功能；

e） 渗透测试，聘请专业安全团队或使用自动化工具，模拟黑客攻击，检验系统的实际防御能力；

f） 安全修复与回归测试，对发现的安全问题进行及时修复，并进行回归测试，确保修复措施有效且未引入新的安全问题。

7.2.3 供应商安全管理

本项控制措施包括：

a） 供应商评估与选择，制定供应商评估标准，考察供应商的安全资质、产品安全特性、安全服务体系等因素，选择符合项目安全要求的供应商；

b） 供应链监控与风险管理，定期获取供应商的安全更新、漏洞报告、合规证明等信息，评估供应链风险，制定应对策略。对关键供应商进行现场审计，确保其安全管理水平；

c） 软件成分分析，使用专用工具识别软件包中的开源组件、依赖库及其版本，检查是否存在已知漏洞、过期版本或不安全许可协议，及时进行更新或替换。

7.2.4 变更管理与配置控制

本项控制措施包括：

a） 管理变更流程，建立包含变更申请、评估、审批、实施、验证、回滚等环节的变更管理流程，确保所有变更操作有序进行；
b） 配置管理数据库，建立配置管理数据库，记录系统组件、配置项、版本、关系、责任人等信息，作为变更管理的基础；
c） 配置审计要求，定期进行配置基线对比、配置合规性检查，确保系统配置符合安全策略和标准要求。对异常变更进行调查，防止恶意篡改。

7.2.5 安全风险管理

本项控制措施包括：
a） 风险识别，结合业务场景、威胁情报、历史数据等，识别项目可能面临的信息安全风险，如数据泄露、系统中断、恶意攻击等；
b） 风险评估，运用定量与定性方法，对风险进行评估，确定优先级；
c） 风险应对，制定风险应对策略，明确责任人、完成时间、所需资源，纳入项目计划。对高风险事项进行重点监控，及时调整应对措施；
d） 风险沟通与报告，定期向项目组、管理层、利益相关者通报风险状况，确保各方对风险有清晰认识，支持决策。

7.2.6 培训与意识提升

本项控制措施包括：
a） 制定安全培训计划，根据人员岗位、技能水平、业务需求，制定个性化安全培训计划，涵盖基础安全知识、岗位特定安全技能、最新安全威胁与防护等内容；
b） 培训实施与考核，采用线上课程、线下讲座、实战演练、知识竞赛等多种形式进行培训。通过考试、问卷、行为观察等方式评估培训效果，并完善培训计划；
c） 开展持续安全教育，定期发布安全公告、案例分析、最佳实践等资料，提升全员安全意识。

7.2.7 文档管理与知识转移

本项控制措施包括：
a） 文档体系构建，包含项目计划、设计文档、测试报告、运维手册、应急预案、培训材料等在内的完整文档体系，确保信息准确、完整、易于检索；
b） 文档版本控制，使用文档管理系统，对文档进行版本控制，记录修改历史，确保人员访问最新版本。对重要文档进行备份，防止丢失；
c） 知识转移管理，在项目交接、人员变动、技能传承等场景，通过面对面讲解、书面材料、在线问答、实战辅导等方式，确保信息安全知识和经验顺利传递。

8 验收阶段

8.1 目标

确保信息安全建设工程满足安全需求和安全保障措施，以便为后续的信息安全建设工程运行与维护提供依据。

8.2 内容

8.2.1 验收依据

本项控制措施包括：

a） 合规性检查，对照信息安全相关的法律法规、标准等，对工程进行全面合规性审查；

b） 技术指标验证，核实系统在计算环境、区域边界、通信网络、数据保护、应急响应、安全管理等方面是否满足合规性要求和设计指标要求。

8.2.2 文档审查

本项控制措施包括：

a） 设计文档审查，检查设计文档完整性，包括系统架构图、安全设计说明书、风险评估报告、安全控制设计等，确保设计符合信息安全原则和标准要求；

b） 测试报告审查，审查功能测试、性能测试、安全测试报告，确认测试覆盖范围、发现问题及修复情况，评估系统安全性；

c） 运维手册审查，检查运维手册中关于安全运维的规定，包含但不限于系统监控、日志管理、应急响应、安全更新等流程应完备、可行。

8.2.3 系统功能验证

本项控制措施包括：

a） 安全功能测试，对系统的关键安全功能进行实操验证，如身份认证、访问控制、数据加密、安全审计；

b） 安全配置检查，使用配置核查工具或手动检查，确保系统配置符合安全基线要求，不存在默认口令、未授权开放的服务等安全隐患。

8.2.4 风险与漏洞复评

本项控制措施包括：

a） 更新风险评估基线，基于验收阶段的实际情况，重新评估已识别风险，考虑是否有新增风险，调整风险应对措施，确保风险处于可接受水平；

b） 漏洞扫描与修复，使用漏洞扫描工具进行全面扫描，对发现的高危漏洞立即修复，并重新扫描确认，直至无严重漏洞存在。

8.2.5 系统性能与稳定性测试

本项控制措施包括：

a） 压力测试，模拟高并发访问、大数据量处理等场景，验证系统在极限条件下的性能表现和稳定性，确保安全功能在高负载场景继续生效；

b） 故障恢复测试，模拟硬件故障、网络中断、系统崩溃等故障场景，验证系统的容错能力、备份恢复机制和业务连续性计划的有效性。

8.2.6 第三方评估与认证

本项控制措施包括：

a） 独立安全评估，聘请独立第三方机构进行安全评估，包含但不限于网络安全等级保护测评、密码应用安全性评估、网络安全风险评估等，提供客观、专业的安全审查报告，增强验收结论的公信力；
b） 认证准备与申请，如果项目需要获得信息安全认证，确保项目成果符合认证要求，项目各方配合完成认证申请与现场审核。

8.2.7 用户培训与知识转移

本项控制措施包括：
a） 安全操作培训，对系统使用者进行安全操作培训，包括安全登录流程、权限使用规则、数据保护措施、应急响应步骤等，确保用户知晓并遵守安全规定；
b） 运维人员交接，对运维团队进行详细的技术交接，包括系统架构、运维工具、故障排查方法、安全更新流程等，确保运维团队具备独立运维能力。

8.2.8 验收报告与改进计划

本项控制措施包括：
a） 验收报告编制，编写详细的验收报告，记录验收过程、测试结果、发现的问题及整改情况，给出验收结论。报告应包括对系统安全性的综合评价及改进建议；
b） 制定持续改进计划，基于验收结果，制定后续的系统优化、安全加固、运维改进等持续改进计划，支撑系统在运行过程中持续提升信息安全水平。