ICS 35.030
CCS L80

DB21

辽 宁 省 地 方 标 准

DB21/T XXXX—XXXX

信息安全工程质量控制技术规范

Technical specification for quality control of information security engineering

XXXX - XX - XX 发布 XXXX - XX - XX 实施

辽宁省市场监督管理局 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 信息安全工程质量控制措施 1
4.1 资格控制 1
4.1.1 系统集成资质要求 1
4.1.2 人员资质要求 2
4.1.3 安全产品要求 2
4.1.4 工程监理要求 2
4.1.5 法律、法规、政策符合性要求 2
4.2 招标阶段 2
4.2.1 目标 2
4.2.2 内容 3
4.3 设计阶段 4
4.3.1 目标 4
4.3.2 内容 4
4.3.3 总结 ..... 错误！未定义书签。
4.4 实施阶段 6
4.4.1 目标 6
4.4.2 工程实施质量控制 6
4.4.3 项目实施质量控制 8
4.5 验收阶段 9
4.5.1 目标 9
4.5.2 验收标准流程 9
4.5.3 验收阶段质量控制 10

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、

本文件主要起草人：XXX、XXX

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（沈阳市浑南新区三义街6-1号21层），联系电话：024-83785841/83785849。

信息安全工程质量控制技术规范

1 范围

本文件规定了信息安全工程生命周期中在招标、设计、实施和验收阶段的质量控制技术措施。

本文件适用于信息安全工程的需求方和实施方在招标、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 25069 信息安全技术 术语

GB/T 22081 信息技术 安全技术 信息安全控制实践指南

GB/T 20282—2006 信息安全技术 信息系统安全工程管理要求

3 术语和定义

GB/T 250691、GB/T 2208、GB/T 20282—2006界定的以及下列术语和定义适用于本文件。

3.1

信息安全工程 information security 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系统工程。

3.2

信息安全工程生命周期 information security engineering life cycle

在整个信息系统生命周期中执行的安全工程活动包括：概念形成、概念开发和定义、验证与确认、工程实施开发与制造、生产与部署、运行与支持和终止。

3.3

实施工作关注度 implementation focus

在整个信息系统安全工程实施阶段根据风险及影响程度优先级划分，而对实施工作产生的优先级、工作量以及工作注意力的不同程度。

3.4

脆弱性链 vulnerability chain

在系统工程脆弱性分析中，一个或多个可对系统造成影响或危害的脆弱性指标组合的总称。

4 信息安全工程质量控制措施

4.1 资格控制

4.1.1 系统集成资质要求

国家相关主管部门认可的系统集成相应资质。

4.1.2 人员资质要求

国家相关主管部门认可的安全服务人员、实施人员资质。

4.1.3 安全产品要求

信息安全产品应具有在国内生产、经营、销售的许可证，并符合相应的等级。

4.1.4 工程监理要求

a） 应具备信息安全系统建设工程实施监理管理制度；
b） 监理公司具有国家主管部门认可监理资质证书。

4.1.5 法律、法规、政策符合性要求

系统应符合国家相关的法律、法规和政策，不应具有违法活动等不正当行为。

4.2 招标阶段

在信息安全工程项目招标阶段，主要是对安全需求进行分析和确定，然后编写详细的招标文件，包括招标公告、技术规格书、合同等。该阶段需要明确项目的技术要求、安全要求、服务要求、项目实施时间、预算等内容。

在招标阶段，需要进行公开招标，向供应商发送招标文件，并邀请他们提交报价书。招标人需要对报价书进行评估和比较，选择最有利于项目的供应商。

招标阶段应进行供应商的资格审查，确保符合资格条件，防止出现不合格供应商参与竞标。

招标人应保证招标过程的公正、公平、透明，确保最终选择的供应商能够按照合同要求履行义务，保证项目的质量和安全。

4.2.1 目标

4.2.1.1 了解需求

在这个阶段，项目招标人应充分了解项目的业务需求、技术要求、安全要求、服务要求、预算等方面的要求。编写招标文件

招标文件应清晰明确地阐述项目需求，以便供应商能够理解项目需求并提交合适的报价书。招标文件的编写也应符合相关法律法规和标准的要求，以确保公正、公平、透明。

4.2.1.2 公开招标

在符合相关法律法规和标准的前提下，向潜在的供应商发送招标文件，并邀请其提交报价书。

4.2.1.3 报价书评估和比较

对供应商提交的报价书进行评估和比较，选择最有利于项目的供应商。

报价书评估和比较的内容包括报价书的价格、质量、技术方案等方面。

这个过程需要严格按照招标文件的规定进行，确保评估和比较的公正性、公平性和透明性。

4.2.1.4 供应商资格审查

进行供应商的资格审查，确保符合资格条件，防止出现不合格供应商参与竞标。

供应商资格审查的内容包括供应商的注册资质、业绩、信用度等方面。

4.2.1.5 招标过程管理

确保招标过程的公正、公平、透明，遵守相关法律法规和招标文件的规定，确保最终选择的供应商能够按照合同要求履行义务，保证项目的质量和安全。

招标过程管理应严格执行招标文件的规定，确保公正公平，同时应对供应商进行管理，确保他们能够按照合同要求履行义务。

4.2.1.6 项目实施保障

项目实施保障应制定详细的实施计划，并对项目实施过程进行管理和监控，以确保项目的顺利实施

4.2.1.7 风险控制

4.2.2 内容

包括但不限于招标文件的编制、公开招标、供应商评估、合同签订、招标过程管理和风险控制等方面的工作。

4.2.2.1 招标文件的编制

4.2.2.1.1 项目需求的明确

项目招标人应充分了解项目的业务需求、技术要求、安全要求、服务要求、预算等方面的要求，明确项目需求，为编制招标文件提供基础。

4.2.2.1.2 招标文件的编制

招标文件应包括招标公告、技术规格书、合同等内容，招标文件应清晰明确地阐述项目需求，以便供应商能够理解项目需求并提交合适的报价书。招标文件的编写应符合相关法律法规和标准的要求，以确保公正、公平、透明。具体包括：

a) 招标公告：应包括招标项目的基本情况、投标人应提交的文件、报价要求、投标保证金、评标方法、开标时间和地点等信息。招标公告应发布在指定的媒体上，确保公开透明；

b) 技术规格书：应详细阐述招标项目的技术要求、安全要求、质量要求和验收标准等；

c) 合同：应明确项目实施计划、实施进度、合同金额、质量标准、验收标准等方面的要求。合同应经过项目招标人和供应商双方的协商和签字确认。

4.2.2.1.3 招标文件的审核

内容包括：

a） 招标文件的完整性和准确性：内容是否完整、准确、清晰，是否与项目需求一致；

b） 评审标准和评分标准的合理性：审核人员应检查评审标准和评分标准是否符合项目需求和招标文件的规定；

c） 其他要求：审核人员应检查招标文件是否符合相关法律法规和标准的要求，是否具有可操作性和可实施性。

4.2.2.2 公开招标

4.2.2.2.1 公开招标的要求

在符合相关法律法规和标准的前提下，向潜在的供应商发送招标文件，并邀请他们提交报价书。

4.2.2.2.2 公开招标的程序

，包括但不限于公告发布、报名、资格审查、答疑、评标、中标公示等程序，具体包括：

a） 公告发布：项目招标人应在指定的媒体上发布招标公告，公告应包括招标项目的基本情况、投标人应提交的文件、报价要求、投标保证金、评标方法、开标时间和地点等信息；

b） 报名：供应商应按照招标文件的规定，提交报名文件，包括供应商的基本情况、业绩、资质证书等；

c） 资格审查：项目招标人应根据招标文件的规定，对供应商进行资格审查；

d） 答疑：项目招标人应按照招标文件的规定，组织答疑会议；

e） 评标：评审委员会应根据项目需求和招标文件的规定，制定评审标准和评分标准，并对供应商提交的报价书进行评估和比较，确定最终的供应商；

f） 中标公示：项目招标人应在指定的媒体上公示中标结果，并通知中标供应商签订合同。

4.2.2.3 供应商评估

4.2.2.3.1 评审委员会的组建

评审委员会应由专业人员组成，成员具有相关的技术、管理和法律知识和经验，，制定评审标准和评分标准，并对供应商提交的报价书进行评估和比较。

4.2.2.3.2 报价书评估和比较

内容包括报价书的价格、质量、技术方案等方面。

评审委员会应对供应商提交的报价书进行评估和比较，并根据评审标准和评分标准，确定最终的供应商。具体包括：

a） 价格评估：评审委员会应对供应商的报价进行评估和比较，确定最优的报价

b） 质量评估：评审委员会应根据招标文件的要求，对供应商的质量承诺和质量管理体系进行评估和比较；

c） 技术方案评估：评审委员会应对供应商的技术方案进行评估和比较。

4.3 设计阶段

4.3.1 目标

制定出可行的质量控制技术规范，确保信息系统的安全性、可靠性、可用性和完整性；

应完成完成系统的顶层设计、初步设计和详细设计，决定组成系统的配置项，确定系统指标。

4.3.2 内容

4.3.2.1 确定质量目标

质量目标的确定应根据项目的特点和用户的需求，确定信息安全工程质量目标和质量管理计划，并制定相应的质量指标和验收标准。

质量验收目标可通过客户满意度调查、产品性能测试、质量控制图等方式来确定。

4.3.2.2 制定质量规范

主要包括以下方面：质量目标和要求、质量管理的基本原则、组织结构和职责、质量管理体系的组成部分、运作方式和相应的程序、质量管理的各个环节和流程、文件记录、内部审核和管理评审等。

4.3.2.3 制定质量流程

包括以下步骤：

a） 明确质量流程的目标和范围，确定流程所涉及的环节和步骤；

b） 收集和分析相关数据和信息，了解当前流程的瓶颈和问题；

c） 制定流程图和流程文档，明确流程的各个环节和步骤，以及流程的输入和输出；

d） 制定流程的管理和控制措施，确保流程的可控性和可操作性；

e） 进行流程的评估和改进，根据实际情况和数据分析，制定改进措施和计划，以不断提高流程的效率和质量水平。

4.3.2.4 定义质量工具

定义质量工具的要求主要包括：

a)应根据问题和数据类型选择合适的工具进行分析和处理；；

b）需要遵循科学的方法和标准，对数据进行准确和全面的收集、整理和分析；

c）可进行数据可视化处理，采用图表、图形等方式，直观清晰地展示数据分析结果；

d）应对数据进行持续监控和分析，及时发现和解决问题，进行持续改进。

定义质量工具的方法主要包括以下步骤：

a） 了解不同的质量工具及其适用范围和优缺点，包括统计工具、图表工具、流程图和关系图、质量检查表和问卷调查等；

b） 根据实际情况和需求，选择合适的质量工具，明确使用目的和方法；

c） 进行质量工具的培训和掌握，包括理论知识和实践操作；

d） 建立质量工具的管理和使用制度，确保质量工具的规范化和标准化；

e） 定期对质量工具进行评估和改进，根据实际使用情况和效果，确定改进措施和计划，提高质量工具的效率和可靠性。

4.3.2.5 实施质量控制

实施质量控制的方法主要包括以下步骤：

a） 建立质量控制的体系和流程，包括质量标准、质量计划、质量检查和测试等；

b） 进行质量控制的前期准备工作，包括确定控制点、制定控制方法和标准、培训员工等；

c） 进行质量控制的执行和监控，包括收集数据、分析问题、制定改进方案等；

d） 进行质量控制的反馈和调整，包括对控制标准和方法进行评估和改进，及时进行调整和纠正；

e） 进行质量控制的总结和持续改进,包括对整个质量控制过程进行评估和分析,发现问题和不足，制定改进计划和目标，实现持续改进和成果导向。

4.3.2.6 进行质量评估

进行质量评估的要求主要包括以下方面：

a） 明确评估目标和范围，确定评估的内容和重点，以确保评估的准确性和实用性；

b） 收集和分析数据，采用客观、科学的方法进行数据收集和处理，确保数据的可靠性和准确性；

c） 制定评估标准和方法，建立评估体系和指标体系，确保评估结果的客观性和公正性；

d） 进行评估和分析，结合实际情况和数据分析，进行综合评价和分析，深入挖掘问题和原因，为制定改进措施提供依据；

e） 制定改进措施和计划，结合评估结果和实际情况，制定可行的改进措施和计划，以实现持续改进和创新。

4.3.2.7 不断改进

包括以下几个方面：

a） 以客户为中心，不断满足客户需求和期望，提高产品或服务的质量水平和客户满意度；

b） 以数据为依据，进行全面和系统的质量管理，注重数据的分析和应用，以实现质量的可持续发展；

c） 以持续为目标，不断总结和应用改进经验，推动组织的可持续发展；

d） 以团队为主体，建立高效的团队合作机制，强化团队意识和创新能力，为改进提供强大的支持和保障。

4.4 实施阶段

4.4.1 目标

4.4.2 工程实施质量控制

4.4.2.1 管理安全质量控制

4.4.2.1.1 阶段目标

应确保系统在管理层面已按照规定及设计要求进行了合法合规履行。

4.4.2.1.2 具体措施

a） 建立安全控制措施相关制度职责并对全体成员发布；

b） 确保安全责任人员已获得领导小组授权，保证安全控制措施明确且可被广泛应用；

c） 确保实施人员具有相应信息系统安全工程实施资质（包括但不限于职业资格证书，认证证书等）；

d） 确保对实施组织全体成员进行安全意识培训和教育并统一管理相关安全意识、培训和教育大纲；

e） 确保该实施组织已设立安全责任领导小组，确保其管理责任明确；

4.4.2.2 风险与影响评估质量控制

4.4.2.2.1 阶段目标

应确保对该系统有关系的影响、发现影响的可能性、运行该系统的安全风险进行了有效评估及优先级的划分，确保工作优先级及实施工作关注度。

4.4.2.2.2 具体措施

a） 应确保其已正确对在系统中起关键作用的运行、业务或任务的能力进行标识、分析和按优先级划分，且具有相应标识、划分清单；

b） 选择用于分析、评估和比较给定环境中系统安全风险所依据的方法、技术和准则；

c） 标识每个风险出现的可能性以及估与每个风险有关的风险。

4.4.2.3 威胁与脆弱性评估质量控制

4.4.2.3.1 阶段目标

应对威胁与脆弱性评估中的各项指标（依据 GB/T 20282—2006 中 7.4 和 7.5 节内容）进行质量排查评估，判断其可用及可行性。

4.4.2.3.2 具体措施

a） 威胁评估中的自然威胁应判断其是否为不可抗力等非人为因素造成的威胁，而人为威胁应为是否由人为偶然原因引起的威胁与故意行为引起的威胁；

b） 对可能在特定位置中出现的预料事件，应根据具体情况建立最大和最小测量单位范围；

c） 对于威胁影响的结果，应确定该系统被黑客攻击后进一步利用该威胁进行破坏的潜在能力；

d） 通过多方面评估由人为原因引起的威胁影响的动因和结果（恶意/非恶意利用等）；

e） 应准确评估出现威胁事件的可能性（根据人为及自然因素进行多方面评估）；

f） 应及时收集系统脆弱性数据（包括但不限于系统缺陷等）；

g） 应常态化定期对现有威胁、脆弱性及其特征进行监视，可由该系统工程具体情况自行确定频率为每日或每周一次，并应在相关安全规章文件中明确体现该频率；

h） 应选择一种对一确定环境中系统威胁及安全脆弱性进行标识和特征化的方法、技术和标准，不宜过多；

i） 分析脆弱性链对系统的危害及对系统造成危害的可能性并综合分析，确保质量控制完善。

4.4.2.4 协同工作质量控制

4.4.2.4.1 阶段目标

应监督其协调并保持安全工程所涉及到安全组织、其他工程组织和外部组织之间的关系，保证高效率协同工作，确保实施工作质量。

4.4.2.4.2 具体措施

a） 应建立协同工作机制，确保涉及到的安全组织、其他工程组织和外部组织之间均适用该机制；

b） 各组织负责人应协商定义和建立与其他组织之间的联系和义务关系；这些关系应被全体参与部门所接受，以达到保质保量目的；

c） 各协同组织应建立统一质量管理责任制度，确保质量责任到人，与各负责人有对应关系；设置问责制度与问责级别，亦要规定质量责任与问责级别的对应关系，做好要素间相互对应并严格执行；

d） 在处理优先级不等的各类组织之间的沟通中可能出现的质量工作机制冲突和争议时，需采用适宜且富有成效的策略以解决，而并非使用优先级等因素直接判断。

e） 应在各种安全工程组织、其他工程组织、外部实体及其他合适的部门中沟通安全建议，并据此严格去协调有关安全的建议。

4.4.2.5 监视安全态势质量控制

4.4.2.5.1 阶段目标

应监督其标识并报告所有的安全违规行为；监视外部和内部环境中可能影响系统安全的所有因素；探测和 跟踪内部和外部与安全有关的事件。根据策略制定响应突发事件的措施；根据安全目标标识并处理运行安全态势的变化。

4.4.2.5.2 具体措施

a） 通过监视威胁、脆弱性、影响、风险方面的变化，查找可能影响当前安全状态有效性的任何变化；

b） 应制定安全突发事件判定及处置流程，应急预案流程，确保安全突发事件从判定开始就具备相关标准，应记录时间详细情况，发生原因，各系统工程应按实际情况制定是否形成安全事件报告，推荐使用安全突发事件的影响或破坏级别作为判定依据，有关安全的突发事件可利用历史事件的数据、系统配置数据、完整性工具和其他系统信息诊断；

c） 定期检查检测安全防护措施的执行情况，保证安全防护措施执行到位；

d） 记录其安全防护措施对系统工程的影响程度（包括但不限于性能及有效性，若发现无效或性能占用过多，应及时调整策略）；

e） 制定安全应急计划，要求标识出系统失效的最长时间、系统正常工作的基本元素；制定一个可恢复策略和计划，测试并维护该计划；

f） 确保与安全监视有关的设备得到有效保护，应形成保护日常记录，及时完成与安全监视有关的监视活动（包括但不限于括封存和归档相关的日志、审计报告和相关分析结果）。

g） 根据上述信息及时出具更正整改单，确保系统安全态势高质量稳步运行；

4.4.2.6 其他质量控制

4.4.2.6.1 阶段目标

在前序章节的基础上，保障系统工程的安全性和可靠性。

4.4.2.6.2 具体措施

a） 制定出与安全相关的指南并提供给系统用户和管理员（运行安全指南内容应包含用户和管理员在以安全模式进行安装、配置、运行和终止系统时应做的内容）；

b） 形成与安全相关的工程问题的解决办法选项；解决办法可以多种形式提供（技术支持等方式）

c） 应了解知悉实施人员对安全要求的理解，收集其所有用于全面理解需求方安全要求所需的信息，必要时予以培训及关注；

d） 应明确总体的、面向安全的指导思想，包括任务、职责信息流、资产、资源、人员保护以及物理保护的指导思想。

4.4.3 项目实施质量控制

4.4.3.1 基本质量控制

4.4.3.1.1 阶段目标

确保项目实施基本工作与系统工程过程定义一致。

4.4.3.1.2 具体措施

a） 确保项目实施按照已经定义的系统工程过程实施并定期检查一致性情况，形成检查记录；

b） 对项目实施与系统工程过程不一致的，要及时与所定义的过程相偏离以及该偏离所带来的影响记录下来； 确保所定义的系统工程过程在系统生命周期中是稳定的；差异较大的还应提请专家组重新审议，并经通过后方可进行；

c） 建立项目实施基本工作办法（对项目人员、基本原则等），确保实施工作按章进行，有据可查；

d） 应运用所设计的评估工作产品的方法来检验工作产品是否能符合需求方或工程的需求；根据测量结果对工作产品进行评价；

e） 对项目所使用的系统工程过程的质量进行测量；

f） 发起以发现的质量问题或质量改进问题为主题的相关报告活动。

4.4.3.2 建设中测试质量控制

4.4.3.2.1 阶段目标

完成对建设过程中的信息系统安全工程测试和质量测量。

4.4.3.2.2 具体措施

a） 制定详细的测试计划，明确测试的范围、测试方法、测试环境、测试人员等要素，确保测试过程有序进行；

b） 根据系统需求和功能设计相关的测试用例，确保测试能够覆盖系统的各项功能和性能要求；

c） 建立完善的测试管理机制，包括测试进度管理、测试成本管理、测试风险管理等，确保测试过程的有效性和可控性；

d） 应对产品、过程和项目执行所获得的测试和测量数据进行仔细检查进而找到问题的原因，并将这些信息用于改进产品和过程的质量；

e） 对测试结果进行反馈和追踪，及时跟踪缺陷的修复和问题的解决情况，确保系统的安全性和质量要求；

f） 应指定专人追踪测试结果的反馈情况，并及时完成缺陷问题的整改与提交；

4.4.3.3 移交与试运转测试质量控制

4.4.3.3.1 阶段目标

在系统即将移交及试运转期间，完成对各项功能的实施情况进行测试。

4.4.3.3.2 具体措施

a） 开发者与承建者应共同拟定测试内容、测试指标、测试结果说明、测试仪器及方法等内容，并报告给需求方和投资者审查通过；

b） 承建者实施方应做好用户设置、网络配置、操作注意事项等测试前准备工作，召集相关技术人员配合进行测试系统工作，相关人员应具备软件测试资质；

c） 移交及试运转测试时应对交换机等核心设备各项功能在运转时情况、服务器各项功能在运转时状况、对各终端运行情况记录，了解各终端在使用时，是否有障碍及发生的概率，并生成对应报告；

d） 相关测试结果应经过需求方审查，若有未达到要求项，双方及时商讨解决方案解决（按合同约定内容或按双方商讨一致结果）。

4.5 验收阶段

4.5.1 目标

确保信息安全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工程运行与维护提供依据。

4.5.2 验收流程

应在主管部门的主持下，按照以下流程完成：

a） 需求方向相应的主管部门提出验收申请；

b） 主管部门委托国家授权的信息安全测评机构对申请验收的信息系统实施系统安全性测评并提出测评结论；

c） 在主管部门主持下，召开系统验收会议，参加单位一般包括需求方、投资者、承建者、安全工程监理方等。

4.5.3 验收阶段质量控制

4.5.3.1 阶段目标与指引

对信息系统进行全面的测试和评估,确保系统的质量和可靠性，防止信息泄露、破坏、篡改等安全事件的发生，应对测试报告、安全策略、安全配置、安全漏洞、系统性能、用户培训和技术支持等方面进行审查和测试,以验证系统是否高质量地满足安全要求。

4.5.3.2 前置测试报告审查

4.5.3.2.1 应审查测试报告的测试范围和测试方法。

4.5.3.2.2 应审查测试报告的测试结果和问题。

4.5.3.2.3 应对测试报告中提出的问题进行跟踪和解决。

4.5.3.2.4 应关注测试报告中涉及的测试周期和资源情况。

4.5.3.2.5 应该对测试报告中的测试计划和测试用例进行审查。

4.5.3.2.6 应对测试报告中未提及的内容和遗留问题进行补充和完善。

4.5.3.3 验收标准的制定

应确定验收内容和标准，在项目启动阶段，明确系统的需求和目标，制定验收标准和验收依据。包括系统功能、性能、安全等方面的标准。

应制定验收方法，根据系统的特点和需求，确定验收的方法和流程。包括测试方法、评估方法、审核方法等。

应确定验收责任人，明确各个参与方的责任和角色，指定验收责任人，确保验收过程的顺利进行。

4.5.3.4 审查安全策略和配置

4.5.3.4.1 应审查安全配置的完整性和一致性。

4.5.3.4.2 应审查安全配置的可行性和适用性，应按设备性质、设备用途、工作层等具体情况设置不同的安全策略和配置，不应对所有设备设施使用相同策略。

4.5.3.4.3 应对安全配置的执行进行监控和评估，以确保安全配置能够长期有效地保护信息系统的安全。

4.5.3.5 安全漏洞检测

包括：

a）手工测试。通过手工操作系统来发现安全漏洞，不借助其他自动化工具，可覆盖系统的所有部分；

b）自动化测试。通过工具来发现安全漏洞；

c)模拟攻击则。通过模拟黑客攻击系统的手法发现安全漏洞，可以检测系统的实际安全性

相关系统验收时应按照实际情况经需求方和实施方商讨后自行选择测试方法，在影响情况较小时，推荐使用模拟攻击方式。

4.5.3.6 用户培训和技术支持

培训内容包括但不限于提供系统的基本知识和操作技巧等；

培训材料包括但不限于提供系统的详细说明和操作步骤，系统安全策略的配置等；

培训形式包括但不限于在线培训、线下培训等；

培训过程记录包括但不限于培训记录签到、照片、演示文稿等；

培训考核结果包括但不限于人员考核成绩结果、相应成绩是否对应了相应的流程（重新学习、可开始使用系统等处理结果）。

技术支持可通过多种方式实现，包括电话支持、邮件支持和现场支持等。电话支持、邮件支持应提供详细的技术说明，现场支持应提供专业的技术服务。

4.5.3.7 验收测试方法

验收测试包括用户验收测试和专家验收测试等。

a）用户验收测试是由系统的最终用户进行测试，以确保系统符合用户的实际需求和要求。

b）专家验收测试是由专业的测试人员进行测试，以确保系统的质量和可靠性。

4.5.3.8 文档报告审查

审查需求文档，确认系统的需求和目标是否清晰明确。

审查设计文档，确认系统的架构和设计是否符合要求。

审查测试文档，确认测试的方法和结果是否符合要求。

审查用户手册，确认用户手册的内容是否准确、完整。

4.5.3.9 验收结果确认

4.5.3.9.1 确认交付物

确认信息系统安全工程的交付物（包括但不限于系统、设备配置、系统有关的文档材料等）是否完整、准确和规范，是否已按照合同约定交付完整的交付物。

4.5.3.9.2 确认验收结论

根据测试结果和评估，确认信息系统安全工程是否符合验收标准和合同要求，以便确认系统的质量和安全性达到预期要求。

对整个工程确定验收结论，以便对系统进行进一步的优化和改进，并高质量完成验收。