ICS 91.120.25
CCS L 77

DB21

辽 宁 省 地 方 标 准

DB21/T 1712.5—2025
代替DB21/T 1712.5—2012

信息化工程监理实施方法
第5部分：信息安全

Implementation methods for information engineering supervision—
Part 5: Information security

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。

本文件是DB21/T 1712《信息化工程监理实施方法》的第5部分。DB21/T 1712已经发布了以下部分：

——第1部分：通用布缆系统工程监理实施方法；

——第2部分：电子设备机房系统工程监理实施方法；

——第3部分：计算机网络系统工程监理实施方法；

——第4部分：软件工程；

——第5部分：信息安全。

本文件代替DB21/T 1712.5—2012《信息化工程监理实施方法 第5部分：信息化工程安全监理实施方法》，与DB21/T 1712.5—2012相比，除结构调整和编辑性改动外，主要技术内容变化如下：

a） 增加“4一般要求”，包括“4.1概述”“4.2角色与职责”“4.3工作流程”“4.4实施措施”；

b） 增加“5招标阶段”，包括“5.1监理目标”“5.2监理工作流程和方法”；

c） 增加“6设计阶段”，包括“6.1监理目标”“6.2监理工作流程和方法”，并将监理工作流程和实施方法进行细化；

d） 增加“7实施阶段”，包括“7.1监理目标”“7.2监理工作流程和方法”，并将监理工作流程和实施方法进行细化；

e） 删除原“工程实施阶段”“工程验收阶段”的“输出文档”内容；

f） 增加“附录A（资料性）信息系统工程安全监理工作表单”内容；

g） 增加了引言部分。

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、辽宁省公安厅。

本文件主要起草人：张健楠、朱江、韩晓娜、李琳、丁显东、肖山、王双、郝博、张蔡玉、魏凤娇、李强。

本文件及其所代替文件的历次版本发布情况为：

——2012年首次发布为DB21/T 1712.5—2012；

——本次为第一次修订。

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。

文件起草单位通讯地址：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。

引　言

信息化工程监理是在项目的信息化建设过程中，对项目进行跟踪、监督和管理的一项重要工作，依靠信息技术手段实现将项目的各个环节、各个阶段的数据收集、处理、传递和应用等工作纳入统一的信息系统中进行管理和监控。随着信息技术的飞速发展和广泛应用，信息化工程监理在政府部门和企业中已成为共识，对于确保信息化项目的顺利实施和高效完成具有重要意义。在这方面，我省建立了信息化工程监理地方标准体系。在该标准体系中，DB21/T 1712《信息化工程监理实施方法》是指导我省信息化工程监理实施的基础性和通用性标准，由5个部分组成。

——第 1 部分：通用布缆系统工程监理实施方法。目的在于规范信息化监理在通用布缆系统工程建设中监理目标的实现方式。

——第 2 部分：电子设备机房系统工程监理实施方法。目的在于规范信息化监理在电子设备机房系统工程建设中监理目标的实现方式。

——第 3 部分：计算机网络系统工程监理实施方法。目的在于规范信息化监理在计算机网络系统工程建设中监理目标的实现方式。

——第4部分：软件工程。目的在于规范信息化监理在软件工程建设中监理目标的实现方式。

——第 5 部分：信息安全。目的在于规范信息化监理在信息化工程安全建设中监理目标的实现方式。

DB21/T 1712.5-2012《信息化工程监理实施方法 第 5 部分：信息化工程安全监理实施方法》自2012 年发布以来,对我省信息化工程监理的信息化工程安全起到了规范化的作用。鉴于我省信息工程监理业务的不断扩展,为了提高信息化工程监理的安全水平,进一步规范监理行业,对 DB21/T 1712.5-2012《信息化工程监理实施方法 第5部分：信息化工程安全监理实施方法》标准进行修订，旨在进一步规范我省信息工程监理业务，提高信息工程监理质量，适用于信息化工程监理中信息化工程安全实施工作。

信息化工程监理实施方法 第5部分：信息安全

1 范围

本文件规定了信息化工程项目新建、升级、改造过程中招标、设计、实施及验收阶段安全监理的工作目标、工作流程。

本文件适用于信息化工程监理中信息化工程安全实施工作，不适用于对信息化工程项目建设中涉及的安全产品、安全技术服务的技术规格和条件做出规定或要求，有关内容参见相应的产品或服务规范。

本文件适用于非涉密信息系统工程安全，不适用涉密信息系统工程安全。

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 9361 计算机场地安全要求

GB/T 19668.1 信息技术服务 监理 第1部分：总则

GB/T 19668.4 信息技术服务 监理 第4部分：信息安全监理规范

3 术语和定义

GB/T 19668.1和GB/T 19668.4界定的术语和定义适用于本文件。

4 一般要求

4.1 角色与职责

信息化监理过程中涉及到的单位和职责如下：

a) 业主单位：项目建设的主体单位，负责信息化工程项目管理及信息化工程项目监理服务的委托；

b) 承建单位：承接信息化工程项目建设的单位，依据国家有关法律法规、标准规范和技术合同开展技术实现，并按照国家有关网络安全、数据安全法律法规、标准规范开展网络安全建设工作；

c) 需求单位（使用单位）：使用信息工程的单位或提出软件工程中系统的功能、服务和运行约束的单位；

d) 监理单位：受业主单位委托，成立监理机构，依据国家有关法律法规、标准规范和监理合同，围绕信息化工程安全建设提供服务的单位；

e) 测评机构：指经国家有关部门培训考核和能力评估并获得推荐资质，从事对信息系统安全等级保护状况进行检测评估、商用密码应用安全评估或其他信息化测评的专业信息安全服务机构。

4.2 安全监理工作流程

监理单位接受业主单位的委托，对承建单位建设的信息化工程项目开展监理服务，从招标阶段、设计阶段、实施阶段、验收阶段环节围绕信息化工程安全规划、实施、运行开展监督管理服务，如表1所示。

表1　工作流程表

阶段	监理活动
招标阶段	协助评审招标文件、协助参与招评标过程、组织审查承建合同
设计阶段	评审安全需求、审核概要（结构）设计、审核详细设计、安全合规设计审查
实施阶段	审核实施方案、监督实施过程、核对安全设备、检查安全设备部署、检查应用系统安全、监督安全控制措施管理、实施安全合规性管理
验收阶段	督促开展测试、安全合规管理、工程验收方案安全审查、工程验收管理

4.3　实施措施

监理机构在各工作流程中实施如下措施：

a）　对信息系统工程项目的招标文件、承建合同、安全设计方案（包括体系结构设计和详细设计）和实施方案进行安全性方面的审查；

b）　依据安全法规对信息系统工程项目实施过程中的安全性进行检查。

5　招标阶段

5.1　安全监理目标

监理机构通过审核招标文件中涉及安全的条款确保信息化工程建设安全符合相关法律法规、政策和标准；审核承建合同中所提供的安全产品和服务满足招标文件要求，合同中的条款在技术、经济上合理有效。

5.2　安全监理工作流程和方法

5.2.1　协助评审招标文件

监理机构应组织专业安全监理工程师，辅助业主单位评审招标文件安全内容，形成监理意见，出具监理工作联系单（按GB/T 19668.1—2014中表B.9要求执行）：

a）　招标文件宜明确信息化工程项目的系统以及相关的产品及服务等技术级别要求及相关安全建设应符合国家信息安全相关法律法规、政策和标准；

b）　招标文件宜明确信息化工程项目的安全目标、安全需求、工作范围及各方职责边界；

c）　招标文件宜明确要求项目所采用的信息安全技术应满足GB/T 22239—2019中相应等级的技术和管理要求开展设计、实施，并满足既定的安全目标与安全需求；

d）　招标文件应根据项目实际需求明确投标单位的资质、资格要求，如信息安全服务和信息系统集成等资质、类似成功案例等；

e）　招标文件应根据项目实际需求明确投标单位项目组中安全人员的资格要求，如信息安全领域的相关资格、工作年限和项目经验等；

f）　招标文件应根据项目实际需求明确投标单位的服务过程管理、质量保障体系、应急响应能力等要求；

g）　招标文件应按照项目实际需求明确系统上线前及系统运行过程中所需网络安全等级测评和商用密码应用安全性评估工作的各方职责及任务分工；

h）　新建工程项目对原有信息系统安全性的可能影响及处理措施。

5.2.2　协助参与招评标过程

监理机构可按照业主单位要求辅助参与招标答疑工作，协助业主单位对工程所涉及的安全需求、技术指标和验收标准等向投标单位解释，并保存会议纪要和相关文件。

5.2.3　组织审查承建合同

监理机构应组织审查承建合同，从安全规范、安全合规等方面针对项目不同方面提出意见：

a）　监理机构应协助业主单位检查承建合同，对合同中安全功能、技术要求、安全测试标准、验收要求和网络安全、数据安全质量责任条款的合规性、合理性进行评审，形成监理意见，出具监理工作联系单（按GB/T 19668.1—2014中表B.9要求执行）；

b) 在承建合同中应明确要求承建单位接受监理机构的监理；
c) 在承建合同中应明确信息安全相关建设内容和技术要求，应符合国家信息安全相关法律法规、政策和标准，且应与投标文件一致；
d) 在承建合同中应明确保密条款、安全风险控制和安全责任条款；
e) 在承建合同中应明确项目所涉及的数据、个人信息、知识产权等归属责任条款；
f) 在承建合同中应明确项目验收和安全测评的标准、各方职责分工、测评方法及文档交付要求；
g) 在承建合同中应明确工程变更和扩展引发安全问题的处理方法；
h) 监理机构应结合工程内容按需促使各方(业主单位、承建单位、监理机构、测评机构等)签署保密协议。

6 设计阶段

6.1 监理目标

监理机构通过沟通协调，促使业主单位和承建单位对安全需求达成一致；督促承建单位规范化描述信息系统工程的安全技术要求及安全服务人员要求，形成安全设计方案(包括体系结构设计和详细设计)，并确保其满足安全需求并具有可验证性，符合相关的法律法规、政策和标准，与信息系统工程整体建设相符；督促承建单位提供与安全设计方案配套的其他安全输入。

6.2 监理工作流程和方法

6.2.1 评审安全需求

项目安全需求调研、分析阶段监理机构开展的主要工作如下：

a) 监理机构应促使业主单位和承建单位就工程安全需求组织召开专题会议，对信息系统工程的安全需求和安全人员需求进行充分沟通讨论，监理机构记录会议内容形成会议纪要（按GB/T 19668.1—2014中表B.6要求执行）；
b) 监理机构应促使业主单位充分考虑信息系统工程的信息安全总体规划设计，如已有信息化基础应建议业主单位基于现有业务开展风险评估工作，并要求承建单位根据信息安全风险评估报告和信息安全需求进行整体安全设计，明确信息系统工程建设的安全目标，明确安全需求；
c) 监理机构应要求承建单位编写项目信息化工程安全建设方案，并对其进行评估，形成监理意见，出具监理工作联系单（按GB/T 19668.1—2014中表B.9要求执行），确保信息安全相关建设内容与合同要求和实际需求一致，符合国家信息安全相关法律法规、政策和标准，满足网络安全等级测评和商用密码应用安全性评估相应级别要求。

6.2.2 审核概要（结构）设计

项目审核概要（结构）设计开展的主要工作如下。

a) 监理机构应组织专业安全监理工程师审核承建单位的概要（结构）设计中安全设计内容，确保设计依据GB/T 19668.1—2014中表B.1安全控制措施能满足安全技术要求进行审核，并提出监理意见，重点审核如下内容：
   1) 安全设计与安全目标和安全需求的一致性；
   2) 根据安全技术要求，选择安全模型进行安全体系结构设计的合理性，制定安全解决方案的针对性，设计安全控制措施的有效性，并考虑残余风险；
   3) 安全控制措施应覆盖物理、主机、网络、应用、数据和信息安全管理等方面；
   4) 对项目各阶段的安全风险分析和控制措施的全面性和合理性；
   5) 安全性检验应具有可操作性和有效性；
   6) 如适用，应督促承建单位组织相关部门和有关安全技术专家对体系结构设计的合理性和正确性进行论证和审定。
b) 监理机构应协助业主单位和承建单位与信息安全相关主管部门进行充分的沟通和协调，确保安全设计方案的合规性要求。

6.2.3 审核详细设计

项目审核详细设计的主要工作如下。

a) 监理机构应组织专业安全监理工程师审核承建单位的详细设计中安全设计内容，进行审核，并提出监理意见：
   1) 详细设计应遵循体系结构设计，确定并明晰系统安全设计要素，如安全功能和性能、系统接口(内部和外部)、安全控制措施、安全规范等；
   2) 安全控制措施应考虑计算机设备、设施(包括机房建筑、分区、门禁、监控、供电、空调、消防等)、通信与网络设备、存储设备、身份鉴别、访问控制、安全审计、系统和信息集成、产品和服务获取、配置管理、应急计划、事件响应、安全评估与认证、安全意识和培训等方面，以及针对特定需求的安全控制措施；
   3) 选择具体的安全产品和服务，设计安全产品和服务中应具备的安全机制(如配置策略等)；
   4) 安全产品采购和使用应符合国家的有关规定；
   5) 如适用，可预先对产品进行选型测试；
   6) 工程实施组织设计，相关的操作指南或手册；
   7) 为系统用户和管理员提供安全运行指南。
b) 监理机构应根据项目需要建议业主单位组织或要求承建单位组织相关部门和有关安全技术专家对详细设计的合理性和正确性进行论证和审定，并协助组织会议，记录会议内容。

6.2.4 安全合规设计管理

监理机构应组织专业安全监理工程师应开展的安全合规方面的监理工作如下：

a) 监理机构应审核承建单位的概要（结构）设计和详细设计，确保设计依据合规(审查表见附录A的图A.1)、安全控制措施能满足安全技术要求；
b) 监理机构应要求承建单位明确各系统的网络安全等级保护级别，督促业主单位开展等级保护定级；
c) 监理机构应对照相应等级保护的要求检查安全保护措施，核查所设计的安全控制措施是否全面且适当；评估安全建设和整改计划是否合理，确保满足对应等级保护要求；
d) 监理机构应协助业主开展信息安全技术体系设计技术架构审查，重点审查加密技术、访问控制机制、防火墙配置、入侵检测/防御系统、安全审计功能以及系统集成安全，检查各系统组件之间的接口安全、数据传输安全及互操作安全性的设计，审查备份与恢复方案，评估数据备份策略、灾难恢复计划和技术完备性；
e) 监理机构应协助业主开展信息安全管理体系设计政策与程序管理，督促开展信息安全政策、操作规程和指南的制定，督促业主单位或承建单位组织人员安全意识与培训，督促制定完备的内部审计机制，督促各方定期进行安全审查和持续改进。

7 实施阶段

7.1 监理目标

监理机构通过审核确保所使用的产品和服务符合设计方案及国家相关法律法规、政策和标准；工程实施方案合规性、合理性、可操作性和可核查性，确保与设计方案相符；确保工程中所集成的安全控制措施有效实现且达到设计要求；并督促承建单位明确工程实施计划，加强工程实施管理，规范执行安全工程过程；监督工程实施过程满足承建合同提出的建设内容和技术要求，并与安全设计方案、工程实施方案相符。

7.2 监理工作流程和方法

7.2.1 审核实施方案

监理机构在审核实施方案过程的主要工作如下。

a) 在工程实施前，监理机构应督促承建单位提供工程实施方案、工程实施计划、工程进度安排等文档，确定项目经理和实施人员组成，并对提交的材料进行审核，重点关注相关安全内容，并提出监理意见，出具监理工作联系单（按GB/T 19668.1—2014中表B.9要求执行）：

1) 实施方案与信息化工程安全建设方案、概要（结构）设计和详细设计方案安全内容的符合性；
2) 详细的工程实施计划和工程控制过程是应包括安全设备安装调试计划及相关安全配置过程计划等过程；
3) 对承建单位提交的工程进度安排进行审核，保证信息系统工程中的各项安全控制措施实施符合信息系统工程的总体时间安排；安全设备安装调试计划合理全面，包括各类安全设备的采购、进场、配置、调试和管理、测评、整改、安全验证的计划等；
4) 工程实施组织中的安全，如工程实施人员网络安全配置、工程实施人员安全管理措施、工程实施步骤安全管理措施应到位，且覆盖全面；
5) 依据体系结构设计和详细设计所采用的安全技术框架、安全管理策略，形成工程实施方案的配套文件。

b) 监理机构可督促承建单位组织相关部门和有关安全技术专家对工程实施方案的合理性和正确性进行论证和审定，组织专题安全技术会议，形成会议纪要（按GB/T 19668.1—2014中表B.6要求执行）。

7.2.2 监督实施过程

监理机构监督项目实施过程的主要工作如下：

a) 在工程实施中，监理机构应安排专业网络安全监理工程检查工程实施过程与实施方案的一致性，对工程实际建设中的变更进行记录并给出监理意见；
b) 监督承建单位按照确定的工程实施方案进行安全控制措施的落实和监控；
c) 监理机构应对安全子系统(或安全设备)进行功能与性能符合性检查见GB/T 19668.4—2017中表C.3；
d) 督促承建单位按照规范建设或使用基础环境，关注物理安全、网络安全建设基础；
e) 督促承建单位按照规范进行系统和设备的安装与调试；
f) 监理机构应促使业主单位和承建单位做好工程实施中的安全管理工作；
g) 监理机构应要求承建单位制定安全管理制度，明确说明建设开发过程的安全控制方法和人员行为准则；
h) 如工程实施中存在重大变更，监理机构应督促承建单位对系统安全性进行再评估。

7.2.3 开展安全设备验收

监理机构应安排专业网络安全监理工程师从如下方面对主要安全设备到货情况验收，并提出监理意见：

a) 设备及其配件、模块的类型和数量与到货清单的一致性；
b) 安全设备具有公安部颁发的销售许可证且在有效期内；
c) 安全设备及型号与销售许可证一致，产品销售所需的证书齐全；
d) 符合安全设计方案所规定的功能、性能；
e) 如必要，由第三方安全测试机构出具的测试报告；
f) 设备部署后运转正常，功能、性能达到合同要求和设计指标。

7.2.4 检查安全设备部署

监理机构应安排专业网络安全监理工程师按需对项目中必要的网络安全系统进行上电检查，形成网络安全系统检测记录见图A.2，如存在问题及时向业主单位汇报检查结果，提出监理意见：

a) 检查网络边界完整性：应能够对非授权设备私自联到内部网络的行为进行检查，准确定出位置，并对其进行有效阻断；应能够对内部网络用户私自联到外部网络的行为进行检查，准确定出位置，并对其进行 有效阻断；
b) 检查入侵防范设备，应在网络边界处监视以下攻击行为端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP碎片攻击和网络蠕虫攻击等；
c) 当检测到攻击行为时，应记录攻击源IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警；
d) 应在网络边界处对恶意代码进行检测和清除；

e) 应维护恶意代码库的升级和检测系统的更新；
f) 检查网络设备防护性，包含应对登录网络设备的用户进行身份鉴别，应对网络设备的管理员登录地址进行限制，网络设备用户的标识应唯一；
g) 主要网络设备应对同一用户选择两种或两种以上组合的认证技术来进行身份鉴别；
h) 应具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施；
i) 当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听；
j) 应实现设备特权用户的权限分离。

7.2.5 检查应用系统安全

监理机构在检查应用系统安全过程的主要工作如下。

a) 监理机构应安排专业网络安全监理工程师需对软件系统的安全设计方案及编码安全进行审查，并提出监理意见：
   1) 对软件系统的安全设计方案的应用系统安全进行审查，填写应用安全系统检测记录表见附录A的图A.3 ，提出监理意见，包括身份鉴别、 访问控制、安全审计、通信完整性和保密性、剩余信息保护、软件容错及资源控制；
   2) 对系统数据备份与灾难恢复的安全设计方案进行审查，提出监理意见，包括数据完整性、数据保密性、备份和恢复等内容。
b) 监理机构应对承建单位的编码规范的系统安全性进行审查，并根据编码规范进行代码抽查，并提出监理意见。

7.2.6 监督安全控制措施管理

监理机构应从如下方面对安全控制措施的实现提出监理意见：

a) 确认集成到信息系统工程中的安全控制措施及其配置；
b) 确认安全控制措施达到设计要求，有效降低风险；
c) 工程实施部署后，应督促承建单位对系统的运行情况进行监控，及时发现安全措施状态变化及安全事件，并进行适当的处置；
d) 如适用，应督促承建单位建立安全态势监控机制，监控安全防护措施的功能、性能的有效性；
e) 督促承建单位对系统用户和管理员进行相关的安全意识教育和技能培训；
f) 如适用，应督促承建单位建立安全控制措施的定期维护机制。

7.2.7 实施安全合规性管理

监理机构应从如下方面对实施过程安全合规性提出监理意见：

a) 应按照“谁主管谁负责、谁运营谁负责、谁使用谁负责”的要求，落实信息安全责任主体；应按照“自主定级、自主保护”的原则，参照GB/T 25058—2019开展等级保护的定级、备案、建设、测评、整改等工作；应参照GB/T 22239—2019中相应等级的技术和管理要求，选择并落实安全控制措施；应定期对信息系统安全状况、安全控制措施的符合情况进行自查，并按要求开展等级保护测评；
b) 落实安全管理技术措施，应建立有效的信息安全技术体系，部署安全产品，选取安全服务和安全机制，保障信息安全；安全技术体系应符合“深度防御”和“动态保障”等基本原则；应制定信息系统不同层面、不同产品和系统的安全配置基线(Baseline)和标准作业流程(SOP)；应建立持续的安全审计和安全监控机制，定期开展配置检查、漏洞扫描、渗透测试等技术检测；
c) 项目实施过程中开展业务连续性分析， 应以保护组织的核心业务、核心价值，保障组织的业务持续开展出发，开展业务影响分析；应基于风险评估和业务影响分析的结论，制定业务连续性计划和灾难恢复计划；应基于信息系统的不同层面、不同应用、不同资产，分别制定恢复时间目标(RTO)、恢复点目标(RPO)指标；应根据业务连续性计划和指标，建立业务连续性保障能力；
d) 应结合实际项目建设情况按需和按计划开展网络安全审查，关系国家安全和公共利益的系统所使用的重要技术产品和服务，应遵从国家网络安全审查制度；应依据产品和服务的安全性

与可控性的审查结论，从技术和背景两方面评估使用信息技术产品和服务的安全风险；应评估信息技术产品和服务的提供商及其供应链的安全风险；应按需要求信息技术产品和服务的提供商做出安全性承诺。

8 验收阶段

8.1 监理目标

监理机构督促承建单位明确工程验收方案(验收目标、责任双方、验收提交清单、验收标准、验收方式、验收环境等)的符合性及可行性；督促承建单位开展系统测试，逐一检测验证安全设计要求的实现，确保工程的最终安全性能和功能符合承建合同、法律法规、政策和标准的要求；确保承建单位所提供的工程各阶段形成的技术、管理和工程文档的内容和种类符合相关标准。

8.2 监理工作流程和方法

8.2.1 督促开展测试

监理机构应依据承建合同、安全设计方案、工程实施方案和实施记录、国家或地方相关标准和技术指导文件，督促承建单位进行系统测试和试运行，对信息系统工程进行安全符合性检查，以验证是否实现了工程安全设计目标和系统安全等级基本要求：

a) 监理机构应督促承建单位按照网络、主机、应用、数据等不同层面的安全功能和性能，采用不同的技术检测方法，设计详细的测试技术方案和控制流程，并对测试技术方案和控制流程进行审查；
b) 监理机构应督促承建单位对工程实施中安装的设备或产品进行单元测试，以评估是否符合业主单位或工程的安全要求；
c) 监理机构应督促承建单位在系统建设完成之后，在业主单位验收之前，进行总体安全性测试；
d) 监理机构应督促承建单位对安全测试的内容做详细的工作文档记录，包括安全工程测试方法、测试过程、测试指标结果等；
e) 如适用，监理机构应督促承建单位及时整改测试中发现的安全问题；
f) 监理机构应从以下方面对测试结果进行审查，并提出监理意见；
g) 系统安全功能，如用户身份鉴别、访问控制、安全审计、数据存储和传输加密等；
h) 系统安全性能，如系统可用性、密码算法强度、备份恢复策略等。

8.2.2 安全合规管理

验收阶段合规管理主要的工作和流程如下：

a) 依据承建合同、安全设计方案、工程实施方案和实施记录、国家或地方相关标准和技术指导文件，督促承建单位进行系统测试和试运行，对信息系统工程进行安全符合性检查，以验证是否实现了工程安全设计目标和系统安全等级基本要求；
b) 协助业主单位收集工程设计和实施中的各种关键文档，协助进行信息安全管理体系的建立、实现、维护和持续改进；确定信息安全管理体系范围，制定信息安全方针，明确信息安全管理职责；应以风险评估为基础，选择控制目标和控制措施来建立信息安全管理体系；应通过信息安全方针、程序文件或制度、操作规程、记录和表单等文件的建立和实施，持续改进信息安全管理体系；对信息系统工程的业主单位和承建单位，均应要求建立信息安全管理体系；
c) 建议业主单位委托第三方机构进行安全测评和风险评估，检查是否遵循了公认的风险评估标准进行风险识别、分析、评价和处理。验证评估范围是否合理，确认风险评估覆盖了所有关键资产、威胁源、脆弱性和影响，确保无遗漏。评估风险处理计划，检查风险降低措施是否合理、可行，应急响应计划是否完备；
d) 应做好与安全测评机构的沟通，在工程验收阶段和系统运行阶段按需开展安全测评；应协调信息系统各相关方配合测评机构开展测评工作；应做好安全测评过程中相关的技术准备、文档准备和人员准备；应对安全测评中发现的问题及时进行安全加固、安全优化等整改工作；
e) 建立应急管理体系，应参照GB／T20986—2023对信息安全事件进行分类、分级；应参照GB/T20986—2023建立应急响应小组，制定应急响应流程，实施信息安全事件管理各过程的主

要活动；应确保信息安全应急管理的人员、预案、操作、工具、资源的可用性；应制定信息系统总体应急预案和各类子预案，定期进行应急预案的培训、演练和修订。

8.2.3 工程验收方案安全审查

协助验收工作机构审核承建单位提供的工程验收方案安全内容，并提出监理意见：

a) 与安全需求、设计方案和实施方案的一致性；
b) 从技术、管理和工程方面保障信息安全，实现安全目标与安全需求；
c) 安全设计要求和指标，实现方法及其检测、验证手段；
d) 工程交付物清单(安全体系架构图、安全配置策略、安全应急响应方案、工程设计和实施文档等)齐全、完整，且与实际相符；
e) 如适用，验收步骤和验收程序可考虑信息安全测评和风险评估环节；
f) 如需，提醒业主单位要求承建单位提供的安全应急管理方案，建立应急响应小组，制定应急响应流程，定期进行应急预案的培训、演练和修订。

8.2.4 工程验收管理

监理机构应协助业主单位按照终验方案所规定的验收内容和方式组织验收，对安全验收内容结果进行确认：

a) 监理机构应督促承建单位在系统验收前先进行系统的测试和试运行，并进行详细的文档记录，对发现的问题进行及时整改；
b) 监理机构应建议业主单位和承建单位根据体系结构设计文件、详细设计文件及相关部门颁发的有关文件、相关信息技术和信息安全标准以及设计规范、建设规范和验收规范进行项目安全验收；
c) 协助业主单位收集工程设计和实施中的各种安全关键文档，并做好交接记录，纳入整体项目移交清单；
d) 督促业主单位按照国家相关法律及管理办法要求组织开展工程第三方工作(如风险评估、等级测评、软件测评等)，必要时协助业主评估第三方工作成果；
e) 如需，监理机构可督促承建单位结合工程内容更新优化信息安全技术体系、信息安全管理体系。

附 录 A

（资料性）

信息系统工程安全监理工作表单

A.1 信息系统工程信息安全设计依据合规性文档表

信息系统工程信息安全设计依据合规性文档表见报表 A.1。

表 A.1 信息系统工程信息安全设计依据合规性检查文档

工程名称	文档编号：		
业主单位			
承建单位			
监理单位			
检查时间			
检查人员			
信息系统工程信息安全建设依据	主要法律、法规、标准与规范名称	是否参考	备注
	GB/T 9361—2011 计算机场地安全要求	□是 □否	
	GB 17859—1999 计算机信息 系统安全保护等级划分准则	□是 □否	
	GB/T 18336—2015 信息技术 安全技术 信息技术安全性评估准则	□是 □否	
	GB/T 20282—2006 信息安全技术 信息系统安全工程管理要求	□是 □否	
	GB/T 20984—2022 信息安全技术 信息安全风险评估规范	□是 □否	
	GB/Z 20985—2017 信息技术 安全技术 信息安全事件管理 第 1 部分：事件管理原理	□是 □否	
	GB/T 20986—2023 信息安全技术 网络安全事件分类分级指南	□是 □否	
	GB/T 22080—2016 信息技术 安全技术 信息安全管理体系要求	□是 □否	
	GB/T 22081—2016 信息技术 安全技术 信息安全管理实用规则	□是 □否	
	GB/T 22239—2019 信息安全技术 信息系统安全等级保护基本要求	□是 □否	
	GB/T 25058—2019 信息安全技术 信息系统安全等级保护实施指南	□是 □否	
	GB/T 28448—2019 信息安全技术 信息系统安全等级保护测评要求	□是 □否	
	GB/T 25066—2020 信息安全技术 信息安全产品类别和代码	□是 □否	
	GB/T 20261—2020 信息技术 系统安全工程 能力成熟度模型	□是 □否	
	GB/T 30283—2022 信息安全技术 信息安全服务 分类	□是 □否	
	GB/T 43697—2024 数据安全技术 数据分类分级规则	□是 □否	
	GB/T 37988—2019 信息安全技术 数据安全能力成熟度模型	□是 □否	
	GB/T 37973—2019 信息安全技术 大数据安全管理指南	□是 □否	
	GB/T 43207—2023 信息安全技术 信息系统密码应用设计指南	□是 □否	
其他依据			
业主单位（签字） 日 期_____	承建单位（签字） 日 期_____	监理机构（签字） 日 期_____	

A.2 网络安全系统检测记录表

网络安全系统检测记录见表 A.2。

表 A.2 网络安全系统检测记录表

<table>
<tr><td colspan="4">工程名称：　　文档编号：</td></tr>
<tr><td colspan="2">日　　期：</td><td colspan="2">地　　点：</td></tr>
<tr><td colspan="4">参加人员：</td></tr>
<tr><td colspan="4">检测依据：
工程设计方案/实施方案
检测项目：
<table>
<tr><td>序号</td><td>名称</td><td>结果</td><td>备注</td></tr>
<tr><td>1</td><td>安全隔离与信息交换系统</td><td>☐ 通过 ☐ 不通过</td><td></td></tr>
<tr><td>2</td><td>信息安全综合审计系统</td><td>☐ 通过 ☐ 不通过</td><td></td></tr>
<tr><td>3</td><td>漏洞扫描系统</td><td>☐ 通过 ☐ 不通过</td><td></td></tr>
<tr><td>4</td><td>入侵检测系统</td><td>☐ 通过 ☐ 不通过</td><td></td></tr>
<tr><td>5</td><td>防火墙设备</td><td>☐ 通过 ☐ 不通过</td><td></td></tr>
<tr><td>6</td><td>防病毒软件</td><td>☐ 通过 ☐ 不通过</td><td></td></tr>
<tr><td>7</td><td>内网安全管理与补丁分发系统</td><td>☐ 通过 ☐ 不通过</td><td></td></tr>
<tr><td>8</td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
</table>
检测问题：
无

检测结论：

备注：

业主单位（签字）　　承建单位（签字）　　监理机构（签字）

日　　期_____　　日　　期_____　　日　　期_____</td></tr>
</table>

A.3 应用及数据安全系统检测记录表

应用及数据安全系统检测记录见表A.3。

表 A.3 应用及数据安全系统检测记录表

工程名称：　　文档编号：

日　　期：　　地　点：

参加人员：

检测依据：

工程设计方案/实施方案

检测项目：

序号	名称	结果	备注
一	应用系统安全		
1	身份鉴别	□ 通过 □ 不通过	
2	访问控制	□ 通过 □ 不通过	
3	安全审计	□ 通过 □ 不通过	
4	通信完整性和保密性	□ 通过 □ 不通过	
5	剩余信息保护	□ 通过 □ 不通过	
6	抗抵赖	□ 通过 □ 不通过	
7	软件容错	□ 通过 □ 不通过	
8	资源控制	□ 通过 □ 不通过	
二	数据备份与灾难恢复		
1	数据完整性	□ 通过 □ 不通过	
2	数据保密性	□ 通过 □ 不通过	
3	备份和恢复	□ 通过 □ 不通过	

检测问题：

无

检测结论：

备注：

业主单位（签字）　　承建单位（签字）　　监理机构（签字）

日　　期_____　　日　　期_____　　日　　期_____