ICS 91.120.25
CCS L77

DB21

辽 宁 省 地 方 标 准

DB21/T XXXX—XXXX

信息化工程监理实施方法 第5部分:信息化工程安全

Implementation method of information engineering supervision—
Part 5: Information engineering safety supervision

（征求意见稿）

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 3
2 规范性引用文件 3
3 术语和定义 3
4 一般要求 4
5 招标阶段 4
5.1 监理目标 4
5.2 监理内容 4
5.3 监理要点 5
6 设计阶段 5
6.1 监理目标 5
6.2 监理内容 6
6.3 监理要点 6
7 实施阶段 7
7.1 监理目标 7
7.2 监理内容 7
7.3 监理要点 8
8 验收阶段 9
8.1 监理目标 9
8.2 监理内容 9
8.3 监理要点 10
附 录 A （资料性） 信息系统工程安全合规性要求 11
附 录 B （资料性） 信息收集调研表模板 13
附 录 C （资料性） 信息系统工程安全监理工作表单 20

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“5招标阶段”，包括：“5.1监理要求”、“5.2监理服务内容和要点”、“5.3监理文档”；

b） 增加“6设计阶段”，包括：“6.1监理要求”、“6.2监理服务内容和要点”、“6.3监理文档”；

c） 将“7 实施阶段”、“8 验收阶段”中的“工程实施阶段”修改为“监理服务内容和要求”并细化相关内容；

d） 删除原“工程实施阶段”、“工程验收阶段”的“输出文档”内容；

e） 增加“附 录 A （资料性） 信息系统工程安全合规性要求”内容；

f） 增加“附 录 B （资料性） 信息收集调研表模板”内容；

g） 增加“附 录 C （资料性） 信息系统工程安全监理工作表单”内容；

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、辽宁省信息中心、沈阳德西企业管理服务有限公司、辽宁省市场监管事务服务中心、辽宁省标准化研究院。

本文件主要起草人：白杨、张健楠、李国良、袁洪朋、李海涛、刘强、刘文志、郝博、赵兴彦、隋大智、张建宇、王海涛、刘兴华、段晓祥、尧忠雍、张昊、王长亮、邱学思。

本文件所代替标准的历次版本发布情况为：

——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：辽宁省沈阳市浑南新区三义街6-1号21层，联系电话：024-83785843。

信息化工程监理实施方法 第5部分:信息化工程安全

1 范围

本文件规定了信息化工程项目新建、升级、改造过程中实施及验收阶段不同专业安全监理的监理目标、监理工作内容、监理要点及实施方法。

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。

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—2011 计算机场地安全要求

GB/T 19668.1—2014 信息化工程监理规范 第1部分：总则

GB/T 19668.4—2017 信息化工程监理规范 第4部分：信息安全监理规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

信息安全 information security

保持信息的保密性、完整性、可用性；另外也可包括诸如真实性、可核查性、不可否认性和可靠性等。

3.2

信息安全监理 information security surveillance

依据信息安全方面的标准和要求，在工程建设各阶段向业主单位提供相关咨询，并协助业主单位对 承建单位在工程建设中的信息安全实施服务、控制和管理的一种专业化服务活动。

注：包括对信息系统运维阶段的其他信息安全实施服务进行监理。

3.3

安全工程 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过程。

注： 安全工程的例子包括信息系统工程(含云服务类的信息系统)建设和运维阶段的安全集成。

3.4

风险评估 risk assessment

依据有关信息安全技术与管理标准，对信息系统及其处理、传输和存储的信息的保密性、完整性和可用性等安全属性进行评价的过程。

注： 风险评估是确定信息安全需求的重要途径。

3.5

安全需求 security requirement

为保证组织业务战略的正常运作而在安全措施方面提出的要求。

3.6

等级保护 classified protection

按照信息系统业务信息和系统服务的重要性，对信息系统分等级实行安全保护。

3.7

安全控制措施 security controls

管控安全风险的方法，为满足一组已定义的安全要求所需的任何过程、策略、设备、实践或其他行为。

3.8

合规性 compliance

信息系统工程应符合国家信息安全法律、法规、政策和标准。

3.9

安全策略 security policy

有关管理、保护和发布敏感信息的法律、规定和实施细则。

注： 安全策略是指在一个特定的环境里，为保证提供一定级别的安全保护所必须遵守的规则。

4 一般要求

本文件遵循GB/T 19668.1和GB/T 19668.4的一般原则和要求，重点描述信息化工程项目不同工程类别设计阶段、实施阶段和验收阶段的安全监理工作要点、输出方法。

在信息化工程项目的安全监理工作中，应同时使用GB/T 19668.1、GB/T 19668.4和本文件。

5 招标阶段

5.1 监理目标

监理机构通过监理工作，应实现如下目标：

a) 审核招标文件中涉及安全的条款是否满足安全需求，并符合相关法律法规、政策和标准；

b) 审核承建合同中所提供的安全产品和服务是否满足招标文件要求；

c) 审核承建合同中与安全相关的条款在技术、经济上是否合理有效。

5.2 监理内容

工程招标阶段的主要监理内容如下：

a) 监理机构应检查招标文件中工程的安全目标、安全需求、工作范围，以及相关的产品及服务等技术要求是否明确；

b) 监理机构宜参与招标答疑工作，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，会议纪要按 GB/T 19668.1—2014 中表 B.6 要求执行；

c) 监理机构应参与承建合同的签订过程，检查承建合同中安全功能、技术要求、测试标准、验收要求和质量责任条款的合理性，在承建合同中应明确要求承建单位接受监理机构的监理；

d) 若发现安全需求缺失或不当，应及时告知业主单位；

e) 若工程中涉及内部敏感信息，监理机构应促使各方(业主单位、承建单位、监理机构、测评机构等)签署保密协议。

5.3 监理要点

5.3.1 招标文件

监理机构应从如下方面对招标文件提出监理意见：

a) 信息安全技术要求，应能满足既定的安全目标与安全需求；

b) 投标单位的资质要求，如信息安全服务和信息系统集成等资质、类似成功案例等；

c) 投标单位项目组人员的资格要求，如信息安全领域的相关资格、工作年限和项目经验等；

d) 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；

e) 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；

f) 投标文件应符合国家信息安全相关法律法规、政策和标准。

5.3.2 承建合同

监理机构应参与承建合同的签订，协助业主单位对承建合同的如下内容进行检查，并提出监理意见：

a) 信息安全相关建设内容和技术要求应与投标文件一致；

b) 保密条款、安全风险控制和安全责任条款；

c) 项目验收和安全测评的标准、方法及文档交付；

d) 工程变更和扩展引发安全问题的处理方法。

6 设计阶段

6.1 监理目标

监理机构通过监理工作，应实现如下目标：

a)协助业主单位和承建单位进行充分沟通，形成安全需求；

b)督促承建单位对信息系统工程的安全技术要求进行规范化描述，形成安全设计方案(包括体系结构设计和详细设计)；

c)确保安全设计方案满足安全需求且具有可验证性，符合相关的法律法规、政策和标准，并与信息系统工程整体建设相符；

d)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 监理内容

工程设计阶段的主要监理内容如下：

a) 监理机构应根据监理规划、承建合同、安全设计方案等文档编制监理细则；

b) 监理机构应促使业主单位和承建单位就工程安全需求进行专门的讨论，对信息系统工程的安全需求形成一致的理解；

c) 监理机构应建议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安全设计，在此期间若发现新的风险或安全需求，应及时通知业主单位和承建单位；

d) 如适用，对已确定将要实行等级保护的系统，监理机构应审核设计方案是否符合相应等级保护所对应的安全技术要求，若不满足及时通知承建单位修改；

e) 监理机构应审核承建单位的体系结构设计和详细设计，确保设计依据合规见表 C.1、安全控制措施能满足安全技术要求；

f) 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；

g) 监理机构应建议承建单位在进行安全设计时，充分考虑新建项目对现有系统和目标系统安全性可能造成的影响，并在设计方案中有所体现；

h) 要求承建单位提交工程设计方案和工程实施组织设计方案按 GB/T19668.1 — 2014 的表 A.1 执行,监理机构对其中的安全设计内容进行审核后提出监理意见；

i) 监理机构宜协助业主单位调动适当的资源，配合承建单位完成工程设计前的安全需求调查和分析工作；

j) 监理机构应就设计阶段的各种变更对工程安全性的可能影响提出监理意见。

6.3 监理要点

6.3.1 体系结构设计

监理机构应从如下方面对系统体系结构设计进行审核，并提出监理意见：

a) 安全设计与安全目标和安全需求的一致性；

b) 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；

c) 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；

d) 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；

e) 安全性检验应具有可操作性和有效性；

f) 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。

6.3.2 详细设计

监理机构应从如下方面对系统详细设计进行审核，并提出监理意见：

a) 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；

b) 安全控制措施应考虑计算机设备、设施(包括机房建筑、供电、空调等)、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；

c) 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)；

d) 安全产品采购和使用应符合国家的有关规定；

e) 如适用，可预先对产品进行选型测试；

f) 工程实施组织设计，相关的操作指南或手册；

g) 为系统用户和管理员提供安全运行指南；

h) 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详细设计的合理性和正确性进行论证和审定。

7 实施阶段

7.1 监理目标

监理机构通过监理工作，应实现如下目标：

a) 确保工程实施方案合规、合理、可操作和可核查，与设计方案相符，具体见附录 B；

b) 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；

c) 确保工程中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，具体见附录 A 和附录 B；

d) 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；

e) 确保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 监理内容

工程实施阶段的主要监理内容如下：

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；

b) 监理机构应对工程实施方案进行审核见表 C.2,检查实施方案与承建合同、设计方案的一致性，并提出监理意见；

c) 监理机构应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；

d) 在工程实施中，监理机构应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；

e) 监督承建单位按照规范进行安全控制措施的落实和监控；

f) 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表 C.3;

g) 监督对安全设备的到货验收；

h) 督促承建单位按照规范进行系统和设备的安装与调试；

i) 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；

j) 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。

7.3 监理要点

7.3.1 工程实施方案

监理机构应从如下方面对承建单位提交的工程实施方案提出监理意见：

a) 实施方案与设计方案的符合性；

b) 详细的工程实施计划和工程控制过程；

c) 安全设备安装调试计划，包括各类安全设备的采购、进场、配置、调试和管理的计划等；

d) 工程实施组织中的安全，如工程实施人员安全管理措施、工程实施步骤安全管理措施等；

e) 如适用，项目分包工程实施的安全管理措施；

f) 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；

g) 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工程实施方案的合理性和正确性进行论证和审定。

7.3.2 安全控制措施

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。

7.3.3 安全设备验收

监理机构应从如下方面对主要安全设备进行到货和部署验收，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) 如适用，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。

7.3.4 工程实施中的安全管理

监理机构应从如下方面对工程实施中的安全管理进行监督：

a) 督促承建单位指定或授权专门的部门和人员负责工程实施过程的安全管理；

b) 督促承建单位严格按照审批通过的实施方案进行施工，确保实施过程与实施方案的一致；

c) 如适用，督促承建单位按其能力成熟度级别执行安全工程过程；

d) 对工程实施方面的管理制度(实施过程的控制方法、人员行为准则等)进行审查；

e) 对承建单位施工人员的身份与资格进行审查；

f) 督促承建单位在施工中严格遵守业主单位的相关安全管理规定。

8 验收阶段

8.1 监理目标

监理机构通过监理工作，应实现如下目标：

a) 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；

a) 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；

b) 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；

c) 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 监理内容

验收阶段的主要监理内容如下：

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) 协助业主单位建立验收工作机构，组织最终的项目验收会议；

c) 协助验收工作机构审核承建单位提供的工程验收方案，并提出监理意见；

d) 协助业主单位对承建单位提供的项目验收申请资料进行评审，并提出监理意见；

e) 协助业主单位收集工程设计和实施中的各种关键文档；

f) 建议业主单位委托第三方机构进行安全测评和风险评估；

g) 督促承建单位及时整改发现的问题。

8.3 监理要点

8.3.1 测试

监理机构应从如下方面开展测试中的监理工作：

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：

   1) 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；

   2) 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。

8.3.2 工程验收方案

监理机构应从如下方面对承建单位提交的工程验收方案提出监理意见：

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、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。

8.3.3 工程验收管理

监理机构应从如下方面开展工程验收管理中的监理工作：

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验收；

c) 如适用，对介入工程第三方工作(如风险评估、等级测评、软件评测等)过程进行监理。

附 录 A
（资料性）
信息系统工程安全合规性要求

A.1 风险评估

风险评估可包括如下内容：

a) 应以保障组织业务使命为导向，开展信息安全风险评估工作，以风险评估作为安全需求的输入；

b) 信息安全风险评估应贯穿信息系统的规划、设计、实施、运行维护以及废弃各个阶段；

c) 应按照 GB/T 20984—2007,制定风险评估流程，覆盖风险评估准备、资产识别、威胁识别、脆弱性识别、已有安全措施确认、风险分析、风险处置等环节；

d) 应确保并持续改进风险评估模型、方法和工具的合理性和适用性。

A.2 等级保护

等级保护可包括如下内容：

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；

b) 应按照“自主定级、自主保护”的原则，参照 GB/T 25058—2010,开展等级保护的定级、备案、建设、测评、整改等工作；

c) 应参照 GB/T 22239—2008 中相应等级的技术和管理要求，选择并落实安全控制措施；

d) 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。

A.3 信息安全技术体系

信息安全技术体系可包括如下内容：

a) 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；

b) 安全技术体系应符合“深度防御”和“动态保障”等基本原则；

c) 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)；

d) 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。

A.4 信息安全管理体系

信息安全管理体系可包括如下内容：

a) 应参照 GB/T 22080—2008 和 GB/T 22081—2008 进行信息安全管理体系的建立、实现、维护和持续改进；

b) 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；

c) 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；

d) 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；

e) 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。

A.5 信息系统安全测评

信息系统安全测评可包括如下内容：

a) 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；

b) 应协调信息系统各相关方配合测评机构开展测评工作；

c) 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；

d) 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。

A.6 应急管理

应急管理可包括如下内容：

a) 应参照 GB/Z20986—2007 对信息安全事件进行分类、分级；

b) 应参照 GB/Z 20985—2007 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；

c) 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；

d) 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。

A.7 业务连续性

业务连续性可包括如下内容：

a) 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(BIA)；

b) 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；

c) 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；

d) 应根据业务连续性计划和指标，建立业务连续性保障能力。

A.8 网络安全审查

网络安全审查可包括如下内容：

a) 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；

b) 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；

c) 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；

d) 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。

附 录 B
（资料性）
信息收集调研表模板

B.1 物理安全

物理安全可包括如下内容：

a) 电子设备机房的安全设计应符合 GB/T 9361—2011 的规定。

b) 机房物理位置选择应考虑以下因素：

   1) 机房和办公场地应选择在具有防震、防风和防雨等能力的建筑内；
   2) 等级保护第三级以上系统，机房场地应避免设在建筑物的高层或地下室，以及用水设备的下层或隔壁。

c) 物理访问控制：

   1) 等级保护第三级以上系统，应对机房进行区域划分，区域和区域之间设置物理隔离装置，在重要区域前设置交付或安装等过渡区域；
   2) 等级保护第三级以上系统，重要区域应配置电子门禁系统，控制、鉴别和记录进入的人员。

d) 防盗窃防破坏：

   1) 应将主要设备放置在机房内，将设备或主要部件进行固定，并设置明显的不易除去的标记；
   2) 应将通信线缆铺设在隐蔽处，可铺设在地下或管道中；
   3) 等级保护第三级以上系统，机房应安装利用光、电等技术设置机房防盗报警系统；
   4) 等级保护第三级以上系统，机房应设置监控报警系统。

e) 防雷击：

   1) 机房建筑应设置避雷装置；
   2) 机房应设置交流电源地线，机房配电柜/配电箱应有地线；
   3) 等级保护第三级以上系统，应在供配电系统上设置防浪涌保护装置，防止感应雷，同时建议在使用电缆的重要弱电设备端口安装防浪涌保护装置。

f) 防火：

   1) 机房应设置火灾自动报警系统，能够自动检测火情、自动报警；
   2) 等级保护第三级以上系统，机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火；
   3) 机房内安装的灭火系统不能为普通喷淋灭火系统，应使用二氧化碳、七氟丙烷或氮气的气体灭火系统，或其他对机房设备不会造成不良影响或影响轻微的灭火系统；
   4) 等级保护第三级以上系统，机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料和装饰材料；
   5) 等级保护第三级以上系统，机房应采取区域隔离防火措施，将重要设备与其他设备隔离开，物理隔断在吊顶之上和防静电地板以下应安装防火板与建筑结构闭合。

g) 防水和防潮：

1) 水管安装，原则上不建议穿过机房屋顶和活动地板下，如因环境限制和不可抗因素，机房内屋顶或活动地板下需要穿越水管，需要在水管表面做好防水隔热包覆，在水管安装的路径上安装流水检测探头或检测绳；
2) 如机房因环境限制存在连接其他区域的窗户，应采取措施防止雨水通过机房窗户渗透，机房的屋顶、地板和墙面建议粉刷防水涂料；
3) 等级保护第三级以上系统，应在存在水管穿越的区域，以及安装精密空调的区域，应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。

h) 防静电：
1) 等级保护第三级以上系统的机房，地面应采用防静电地板；
2) 机房区域内应设置铜质材料均压环，并使用铜带或扁铁连接至机房所在建筑的接地系统；
3) 机房内的所有桥架、金属线管线槽、金属桥架、机柜和防静电地板，都应使用至少 4mm 线径的铜质线缆连接至机房均压环进行接地；
4) 机房机柜内安装的关键设备都应使用至少 4mm 线径的铜质线缆连接到机房均压环进行单独接地，等级保护第三级以上系统，应对主要设备进行接地；
5) 机房区域内的操作台面建议使用静电耗散材料(使用金属材质的操作台面，应在操作台表面包覆防静电橡胶)。

i) 温湿度控制：
1) 机房应设置必要的温、湿度控制设施，使机房温、湿度的变化在设备运行所允许的范围之内；
2) 等级保护第三级以上系统，机房应设置温、湿度自动调节设施，使机房温、湿度的变化在设备运行所允许的范围之内。

j) 电力供应：
1) 应在机房供配电系统上配置稳压器和过电压防护设备；
2) 机房应配置 UPS 不间断电源系统，至少满足主要设备在断电情况下的正常运行 30min 要求；
3) 等级保护第三级以上系统，应设置冗余或并行的电力电缆线路为计算机系统供电，有条件的建议机房所在建筑部署备用供电系统(如柴油/汽油发电机)。

k) 电磁防护：
1) 为了防止干扰，电源电缆要与通信电缆分开，通信线缆中的高频信号线缆(如手机信号覆盖线缆)应保证其电磁屏蔽性能，无过量电磁泄漏；
2) 等级保护第三级以上系统，应保证机房采用接地方式防止外界电磁干扰和设备寄生耦合干扰；
3) 等级保护第三级以上系统，应对关键设备和磁介质进行电磁屏蔽(使用屏蔽机柜安装关键设备，使用电磁屏蔽防潮柜存放磁介质)。

l) 机房环境监控：
1) 机房应安装环境动力监控系统，对机房内的视频监控系统、防盗报警系统、电子门禁系统、精密空调系统、消防自动报警和自动灭火系统进行集中控制，并对温湿度，供配电系统电力电压、漏水检测等进行集中监测，对以上所有系统涉及的记录进行集中保存，并提供分类查询功能；
2) 机房应有专人值守，如因条件限制无人值守的机房，出现报警时，应通过短信邮件等手段将报警信息及时发送给相关管理人员。

m) 对于涉及敏感数据或关键的系统链路，还应考虑以下的措施：

1) 在检查点、终接点处和室外直接埋地的线缆安装金属铠装电缆管道和上锁的房间或盒子；
2) 使用光纤或屏蔽线布缆，使用屏蔽线缆布线需配合支持屏蔽接口的终端设备，并进行良好接地。

B.2 网络安全

网络安全可包括如下内容：

a) 各种服务器及网络核心设备宜放置在专门的电子设备机房。

b) 信息网络平台中涉及的防火墙、防病毒系统等网络安全软硬件设备应通过国家相关安全测评认证机构的认证。

c) 结构安全：
   1) 网络全局和结构设计应保证关键网络设备的业务处理能力具备冗余空间，满足网络各个部分业务高峰期需要，等级保护第三级以上系统应保证主要网络设备的以上能力；
   2) 应绘制与实际部署情况相符的网络拓扑结构图，需标识出所有服务器、网络设备和安全设备，及相应的设备型号、IP 地址和连接端口等，标识出安全区域划分情况；
   3) 等级保护第三级以上系统，应在业务终端与业务服务器之间进行路由控制建立安全的访问路径，如使用静态路由，或启用加密认证的 OSPF;
   4) 等级保护第三级以上系统，应避免将重要网段(如服务器区，数据存储区)部署在网络边界处且直接连接外部信息系统，重要网段与其他网段之间采取可靠的技术隔离手段(防火墙、UTM、网闸等);
   5) 等级保护第三级以上系统，应按照对业务服务的重要次序来指定带宽分配优先级别，保证在网络发生拥堵的时候优先保护重要主机，在核心交换机或边界设备上配置并启用 QOS 策略；
   6) 应根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段。

d) 访问控制：
   1) 应在网络边界处部署访问控制设备(如防火墙、UTM、SG 等),启用访问控制功能，并配置合理的访问控制策略；
   2) 应能根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，控制粒度为网段级，等级保护第三级以上系统要求控制粒度为端口级；
   3) 等级保护第三级以上系统，应对进出网络(Internet 边界)的信息内容进行过滤，实现对应用层 HTTP、FTP、TELNET、SMTP、POP3 等协议命令级的控制；
   4) 网络应具备会话超时中断，最大并发数限制功能；
   5) 重要网段应采取 IP/MAC 地址绑定，或其他防地址欺骗手段；
   6) 应按用户和系统之间的允许访问规则，决定允许或拒绝用户对受控系统进行资源访问，控制粒度为单个用户；
   7) 如网络提供了拨号接入功能，需要对拨号用户数量进行限制。

e) 网络设备防护：
   1) 应对登录网络设备的用户进行身份鉴别，网络设备的管理用户标识应具有唯一性；
   2) 应对网络设备的管理员登录地址进行限制；
   3) 管理用户的身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求并定期更换，设备具备口令复杂度限制和口令生存周期限制功能的，应启用；

4) 等级保护第三级以上系统的网络中，网络设备与安全设备应对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别；
5) 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；
6) 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，如启用 SSH、https 等安全协议进行远程管理登录。

f) 安全审计：
1) 应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录，审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
2) 等级保护第三级以上系统应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等，并能够根据记录数据进行分析，并生成审计报表。

g) 边界完整性：
1) 应部署终端管理类系统对内部网络用户私自联到外部网络(如越权访问、连接非授权的无线网络和私自安装 3G 上网卡连接 Internet 的行为进行检查，并对其进行有效阻断；
2) 等级保护第三级以上系统应部署基于 802.1X 等认证的网络准入控制系统对非授权设备私自联到内部网络(如非授权的终端，服务器及网络设备)的行为进行检查，并对其进行有效阻断。

h) 入侵防范：
1) 应在网络边界处部署 IPS、UTM 等设备，或在网络核心部署 IDS 设备，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
2) 等级保护第三级以上系统应在检测到攻击行为时，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。

i) 恶意代码防范：
1) 等级保护第三级以上系统应在网络边界处部署网络反病毒设备(防毒墙、UTM 等),对恶意代码进行检测和清除；
2) 等级保护第三级以上系统网络反病毒设备应具备恶意代码库自动升级和检测系统更新功能。

B.3 主机安全

主机安全可包括如下内容：

a) 身份鉴别：
1) 应对登录操作系统和数据库系统的用户进行身份标识和鉴别；
2) 管理用户的身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求并定期更换，设备具备口令复杂度限制和口令生存周期限制功能的，应启用；
3) 当对服务器进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听，如启用 SSL、SSH 等安全协议进行远程登录；
4) 应为操作系统和数据库系统的不同用户分配不同的用户名，确保用户名具有唯一性，避免操作系统与数据库系统共享同一账号进行认证；
5) 等级保护第三级以上系统重要服务器应采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别。

b) 访问控制：

1) 应启用访问控制功能，依据安全策略控制用户对资源的访问；
2) 应实现操作系统和数据库系统特权用户的权限分离；
3) 应限制默认账户的访问权限，重命名系统默认账户，修改这些账户的默认口令，并及时删除多余的、过期的账户，避免共享账户的存在；
4) 等级保护第三级以上系统应根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限；
5) 等级保护第三级以上系统应对重要信息资源设置敏感标记，并依据安全策略严格控制用户对有敏感标记重要信息资源的操作。

c) 安全审计：
1) 审计范围应覆盖到服务器和重要客户端上的每个操作系统用户和数据库用户；
2) 审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件，审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等；
3) 等级保护第三级以上系统应保护审计进程，避免受到未预期的中断，并保护审计记录，避免受到未预期的删除、修改或覆盖等；
4) 等级保护第三级以上系统应能够根据记录数据进行分析，并生成审计报表。

d) 剩余信息保护：
1) 等级保护第三级以上系统应保证操作系统和数据库系统用户的鉴别信息所在的存储空间，被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；
2) 等级保护第三级以上系统应确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前得到完全清除。

e) 入侵防范：
1) 操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，并通过设置升级服务器等方式保持系统补丁及时得到更新；
2) 等级保护第三级以上系统应部署 HIDS 类系统，检测到对重要服务器进行入侵的行为，能够记录人侵的源 IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警；
3) 等级保护第三级以上系统所属服务器应能够对重要程序的完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施。

f) 恶意代码防范：应安装杀毒软件，建议使用企业版杀毒软件，等级保护第三级以上系统应使用与网络防恶意代码产品具备不同的恶意代码库，能够进行病毒库升级。

g) 资源控制：
1) 应通过设定终端接入方式、网络地址范围等条件限制终端登录，并根据安全策略设置登录终端的操作超时锁定；
2) 应部署 ITMN 监控系统，对服务器和网络设备的运行状况进行监测。其中对包括监视服务器的 CPU、硬盘、内存、网络等资源，网络设备的 CPU、内存、端口状态和带宽的使用情况等。

B.4 应用系统安全

应用系统安全可包括如下内容：

a) 身份鉴别：

1) 应提供专用的登录控制模块对登录用户进行身份标识和鉴别，启用身份鉴别、用户身份标识唯一性检查功能，并根据安全策略配置相关参数；
2) 应提供用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被冒用；
3) 应提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施，登录失败处理功能，并根据安全策略配置相关参数；
4) 等级保护第三级以上系统，重要应用系统应对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别。

b) 访问控制：
1) 应提供访问控制功能，依据安全策略控制用户对文件、数据库表等客体的访问；
2) 访问控制的覆盖范围应包括与资源访问相关的主体、客体及它们之间的操作；
3) 应由授权主体配置访问控制策略，并严格限制默认用户的访问权限，授予不同账户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系；
4) 等级保护第三级以上系统，应具有对重要信息资源设置敏感标记的功能，并依据安全策略严格控制用户对有敏感标记重要信息资源的操作。

c) 安全审计：
1) 应提供覆盖到每个用户的安全审计功能，对应用系统重要安全事件进行审计，审计记录的内容至少应包括事件日期、时间、发起者信息、类型、描述和结果等；
2) 等级保护第三级以上系统应保证无法单独中断审计进程，无法删除、修改或覆盖审计记录；
3) 等级保护第三级以上系统应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能。

d) 通信完整性和保密性：
1) 应采用校验码技术，等级保护第三级以上系统需要采用密码技术，或其他等效手段保证通信过程中数据的完整性；
2) 在通信双方建立连接之前，应用系统应利用密码技术进行会话初始化验证，等级保护第三级以上系统，应对通信过程中的整个报文或会话过程进行加密，保证通信过程中数据的保密性。

e) 剩余信息保护：
1) 等级保护第三级以上系统，应保证用户鉴别信息所在的存储空间被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；
2) 等级保护第三级以上系统，应保证系统内的文件、目录和数据库记录等资源所在的存储空间被释放或重新分配给其他用户前得到完全清除。

f) 抗抵赖：等级保护第三级以上系统应采用数字签名或其他等效手段，为数据原发者或接收者提供数据原发证据和数据接收证据。

g) 软件容错：
1) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的数据格式或长度符合系统设定要求；
2) 等级保护第三级以上系统应提供自动保护功能，当故障发生时自动保护当前所有状态，保证系统能够进行恢复。

h) 资源控制：

1) 应用系统应具备会话超时断开，最大并发连接数限制和单点登录控制功能；
2) 应提供服务优先级设定功能，并在安装后根据安全策略设定访问账户或请求进程的优先级，根据优先级分配系统资源。

B.5 数据备份与灾难恢复

数据备份与灾难恢复可包括如下内容：

a) 数据完整性：
   1) 应能够检测到系统管理数据、鉴别信息在传输过程中完整性受到破坏，等级保护第三级以上系统还应对重要业务数据进行检测，并在检测到完整性错误时采取必要的恢复措施；
   2) 应能够检测到系统管理数据、鉴别信息在存储过程中完整性受到破坏，等级保护第三级以上系统还应对重要业务数据进行检测，并在检测到完整性错误时采取必要的恢复措施。
b) 数据保密性：
   1) 应采用加密或其他保护措施实现鉴别信息的存储保密性，等级保护第三级以上系统还应采用加密或其他保护措施实现系统管理数据、鉴别信息和重要业务数据存储保密性；
   2) 应采用加密或其他保护措施实现鉴别信息的传输保密性，等级保护第三级以上系统还应采用加密或其他保护措施实现系统管理数据、鉴别信息和重要业务数据传输保密性。
c) 备份和恢复：
   1) 应能够对重要信息进行备份和恢复，等级保护第三级以上系统应提供本地数据备份与恢复功能，完全数据备份至少每天一次，备份介质场外存放；
   2) 等级保护第三级以上系统应提供异地数据备份功能，利用通信网络将关键数据定时批量传送至备用场地；
   3) 应提供关键网络设备、通信线路和数据处理系统的硬件冗余，保证系统的可用性，等级保护第三级以上系统应提供主要网络设备、通信线路和数据处理系统的硬件冗余，保证系统的高可用性；
   4) 等级保护第三级以上系统应采用冗余技术设计网络拓扑结构，避免关键节点存在单点故障。

附 录 C
（资料性）
信息系统工程安全监理工作表单

表 C.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			
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—2008 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—2007 信息安全技术 信息安全风险评估规范	□是 □否	
	GB/Z 20985—2007 信息技术 安全技术 信息安全事件管理指南	□是 □否	
	GB/Z 20986—2007 信息安全技术 信息安全事件分类分级指南	□是 □否	
	GB/T 22080—2008 信息技术 安全技术 信息安全管理体系要求	□是 □否	
	GB/T 22081-2008 信息技术 安全技术 信息安全管理实用规则	□是 □否	
	GB/T 22239—2008 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—2010 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—2012 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—2010 信息安全技术 信息安全产品类别和代码	□是 □否	
	GB/T 20261—2006 信息技术 系统安全工程 能力成熟度模型	□是 □否	
	GB/T 30283—2013 信息安全技术 信息安全服务 分类	□是 □否	
其他依据			

承建单位代表： 年 月 日	监理机构代表： 年 月 日	业主单位代表： 年 月 日

表 C.2　信息系统工程信息安全文档检查清单

序号	文档名称	审核或监理关注点	备注
1	风险评估报告		
2	安全需求报告		
3	承建合同		
4	安全设计方案		
5	工程实施组织设计方案(安全部分)		
6	工程实施方案(安全部分)		
7	工程实施计划(安全部分)		
8	测试技术方案(安全部分)		
9	测试报告(安全部分)		
10	工程验收方案(安全部分)		
11	其他		
审查意见： 年　　月　　日			

表 C.3　安全子系统功能与性能符合性检查报告

<table>
<tr><td>工程名称</td><td colspan="5"></td></tr>
<tr><td>安全子系统</td><td colspan="5"></td></tr>
<tr><td>业主单位</td><td colspan="5"></td></tr>
<tr><td>承建单位</td><td colspan="5"></td></tr>
<tr><td>监理单位</td><td colspan="5"></td></tr>
<tr><td>检查时间</td><td colspan="5"></td></tr>
<tr><td>检查人员</td><td colspan="5"></td></tr>
<tr><td>功能/性能名称</td><td>功能/性能要求</td><td>检测内容
（功能点/性能点）</td><td>要求来源</td><td>是否通过</td><td>备注</td></tr>
<tr><td rowspan="3"></td><td rowspan="3"></td><td></td><td rowspan="3">合同要求
额外增加
需求变更</td><td>□是　□否</td><td></td></tr>
<tr><td></td><td>□是　□否</td><td></td></tr>
<tr><td></td><td>□是　□否</td><td></td></tr>
<tr><td colspan="2">承建单位：

年　月　日</td><td colspan="2">监理机构：

年　月　日</td><td colspan="2">业主单位：

年　月　日</td></tr>
</table>

注：本表格一式三份，业主单位、监理单位、承建单位各一份