数网信认证服务（北京）有限公司

信息安全服务规范

Information security service specification

文件编号：DNI-GZ-JS-10

技术规范编号：CTS DNIISV001-2022

文档版本：F/0

编制：技术部　　日期：2024.09.19

审核：杨舒　　日期：2024.09.19

批准：申爱萍　　日期：2024.09.19

受控状态：受控文件

发布日期：2022年10月20日

修订日期：2024年09月19日

实施日期：2024年09月19日

变更履历

日期	变更描述	版本/版次	审核	批准
2022.10.20	初始发布	A/0	李建文	秦忠河
2023.11.13	修改认证人员的能力评价文件	A/1	杨舒	李静
2024.02.01	扩展信息安全服务类别（增加信息系统灾难备份与恢复服务）	B/O	杨舒	李静
2024.09.19	组织架构及部门职责调整，文件版本与手册统一；扩展信息安全服务类别（增加工业控制系统安全服务）	F/0	杨舒	申爱萍

目　录

信息安全服务规范

1. 适用范围

本规范规定了信息安全服务提供者（简称服务提供者）在提供服务时应具备的组织级服务要求和项目级专业服务能力要求，主要对信息安全服务提供者的服务保障能力（组织级）和服务交付能力（项目级）进行评价，本规范的信息安全服务能力方向包括：信息安全风险评估服务、信息系统安全集成服务、信息安全应急处理服务、软件安全开发服务、信息系统安全运维服务、信息系统灾难备份与恢复服务、工业控制系统安全服务。

本标准适用于：

1) 信息安全服务提供者利用本标准建设自身信息安全服务能力，并进行评估和改进；
2) 信息安全服务需求者利用本标准对信息技术服务提供者信息安全服务能力进行评估；
3) 第三方机构依据本标准对信息安全服务提供者的信息安全服务能力进行客观评估。

2. 术语与定义

2.1 信息安全服务

由供应商、组织机构或人员执行的一个安全过程或任务。

（ISO/IECTR15443-1:2005《信息技术安全技术信息技术安全保障框架第一部分：总揽和框架》）

2.2 信息安全风险评估

对特定威胁利用单个或一组资产脆弱性的可能性以及由此可能给组织带来的损害进行识别、分析和评价的过程。

2.3 信息安全应急处理

为应对信息系统运行过程中突发/重大信息安全事件的发生所做的准备，在事件发生时，按照既定的程序对事件进行处理，以及在事件发生后所采取措施的过程。

2.4 信息系统安全集成

按照信息系统建设的安全需求，采用信息系统安全工程的方法和理论，将安全单元、产品部件进行集成的行为或活动。

2.5 软件安全开发

为解决软件产品的漏洞问题，而将安全活动集成到系统开发和软件质量保证活动中，在软件开发的每个关键点嵌入安全要素，通过安全需求分析、安全设计、安全编码、安全测试等专业手段，解决各阶段可能出现的安全问题，有效减少软件产品潜在的漏洞数量，提高软件产品安全质量的活动。

2.6 信息系统安全运维

从面向业务的运维服务出发，依据安全需求对信息系统进行安全运维准备、安全运维实施，并对实施安全运维服务的有效性进行评审，从而进行持续性改进，全过程、全生命周期地为信息系统运行提供安全保障的过程。

2.7 信息系统灾难备份与恢复

将信息系统的数据、数据处理系统、网络系统、基础设施、专业技术支持能力和运行管理能力进行备份，并在灾难发生时，将信息系统从灾难造成的故障或瘫痪状态恢复到可正常运行状态，将其支持的业务功能从灾难造成的不正常状态恢复到可接受状态的过程。

2.8 工业控制系统安全服务

工业控制系统安全服务围绕提升工业控制系统的高可用性和业务连续性，提升功能安全、物理安全和信息安全的保障能力为目标，涉及工业控制系统设计、建设、运维和技改各个阶段，主要包括系统集成、系统运维、应急处理、风险评估等工业控制系统安全服务，形成系统的、独立的、形成文件的过程。

3. 信息安全服务能力

3.1 能力维度域

信息安全服务能力从两个能力维度域进行评价，分别为信息安全保障能力（组织级）、信息安全服务交付能力（项目级）。

3.2 能力等级

信息安全服务能力的能力等级分为“三级”、“二级”、“一级”三个级别，其中一级最高。

表1 能力等级

能力等级	共性特征	说明
三级	组织对实施信息安全服务有基本的信息安全意识，在关键业务中初步建立了信息安全服务管理机制。	基本建成信息安全服务管理过程，有相关的制度，但没有形成体系化。
二级	组织对实施信息安全服务有较高的意识，信息安全服务全面覆盖业务和相关部门；组织对标准过程进行制度化，为组织定义标准化的文档。	相关制度较为完整，已基本形成体系化；在组织级别实现了信息安全过程的规范执行。
一级	组织的信息安全服务能力发展战略和目标清晰，形成了完善的能力管理体系；为组织的信息安全服务能力建立了可测量目标，以量化测量作为修正行动的基础。	相关制度完善，已完全体系化，要求通过 ISO27001 信息安全管理体系认证并获得证书；要求建立量化目标，相关过程可度量。

3.3 能力方向

信息安全服务能力方向包括：信息安全风险评估服务、信息系统安全集成服务、信息安全应急处理服务、软件安全开发服务、信息系统安全运维服务、信息系统灾难备份与恢复服务（资源服务类或技术服务类）、工业控制系统安全服务。注：每个方向均可加括号对范围进行限定。

4. 信息安全保障能力（组织级）

信息安全服务提供方应从组织控制、人员控制、物理控制和技术控制四个方面提升组织的信息安全保障能力。

4.1 组织控制

4.1.1 管理制度：应基于信息安全需求，建立日常管理活动中常用的信息安全管理制度；

4.1.2 岗位设置：应设立信息安全管理专业岗位，并定义各个岗位的工作职责。

4.1.3 信息安全策略：应制定组织信息安全策略和目标，进行组织级和项目级信息安全管理。

4.2 人员控制

4.2.1 专业能力：确定在组织控制下从事会影响组织信息安全绩效的工作人员的必要能力；

4.2.2 背景调查：在加入组织前，应对拟入职人员进行背景核查，考虑到适用的法律、法规和道德规范；

4.2.3 安全教育和培训：组织人员和相关利益方应接受适当的信息安全意识、教育和培训；

4.2.4 保密协议：员工和其他相关方应确定、记录、定期审查和签署反映组织信息保护需求的保密或不泄密协议；

4.2.5 违规处理：应正式制定并传达纪律程序，以对违反信息安全政策的人员和其他相关方采取行动；

4.2.6 离职管理：信息安全责任和义务在雇佣关系终止或变更后仍然有效，应予以定义、执行，并传达给相关人员和其他相关方。

4.2.7 相关方人员管理：对相关方人员（包括外包方、合作伙伴等）进行相应的信息安全管理，包括背景调查、安全教育和培训、退出管理等。

4.3 物理控制

4.3.1 物理环境：应建立物理环境管理措施，对组织信息和设施进行防护，防止丢失、未授权的物理访问、损坏和干扰；

4.3.2 介质管理：应建立介质管理措施，对介质的使用、标记和处置进行管理；

4.3.3 设备维护和处置：应建立设备维护流程，评估设备变更和维护的风险，审批维修和服务，监督维修过程；

4.3.4 存储设备维护和处置：含有存储介质的设备带出工作环境时其中重要信息应进行重点管控；含有存储介质的设备在报废或重用前，应进行完全清除或被安全覆盖。

4.4 技术控制

4.4.1 终端安全：应建立基本的终端管理措施，保护终端设备的安全；

4.4.2 系统操作安全：应建立基本的系统操作安全措施，包括权限管理、容量管理和恶意代码防护等；

4.4.3 网络安全：建立网络设备和设施的管理措施，以保障网络的安全和可用性。

5. 信息安全服务交付能力（项目级）

5.1 信息安全风险评估服务资质交付能力评价要求

信息安全风险评估服务资质交付能力评价要求参见附录 A。

5.2 信息系统安全集成服务资质交付能力评价要求

信息系统安全集成服务资质交付能力评价要求参见附录 B。

5.3 信息安全应急处理服务资质交付能力评价要求

信息安全应急处理服务资质交付能力评价要求参见附录 C。

5.4 软件安全开发服务资质交付能力评价要求

软件安全开发服务资质交付能力评价要求参见附录 D。

5.5 信息系统安全运维服务资质交付能力评价要求

信息系统安全运维服务资质交付能力评价要求参见附录 E。

5.6 信息系统灾难备份与恢复服务资质交付能力评价要求

信息系统灾难备份与恢复服务资质交付能力评价要求参见附录 F。

5.7 工业控制系统安全服务资质交付能力评价要求

工业控制系统安全服务资质交付能力评价要求参见附录 G。

附录 A（规范性附录）：信息安全风险评估服务资质交付能力评价要求

信息安全风险评估服务资质交付能力评价要求针对评估准备、风险识别、风险分析、风险处置四个过程进行，项目实施过程应形成文件，具体分级要求如下：

A1 三级要求

申请三级资质认证的单位，应具备完成的风险评估项目，具备从管理或（和）技术层面对脆弱性进行识别的能力，具备跟踪信息安全漏洞的能力。

A1.1 准备阶段 A1.1.1

服务方案制定

a)编制风险评估方案、风险评估模板，并在项目实施过程中按照模板实施。 b)应为风险评估实施活动提供总体计划或方案，方案应包含风险评价准则。

A1.1.2 人员和工具准备

a)应组建评估团队。风险评估实施团队应由管理层、相关业务骨干、IT 技术人员等组成。 b)应根据评估的需求准备必要的工具。

c)应对评估团队实施风险评估前进行安全教育和技术培训。 A1.2 风险识别阶段

A1.2.1 资产识别

a)参考国家或国际标准，对资产进行分类。 b)识别重要信息资产，形成资产清单。

c)对已识别的重要资产，分析资产的保密性、完整性和可用性等安全属性的等级要求。 d)对资产根据其在保密性、完整性和可用性上的等级分析结果，经过综合评定进行赋值。

A1.2.2 脆弱性识别

a) 应对已识别资产的安全管理或技术脆弱性利用适当的工具进行核查，并形成安全管理或技术脆弱性列表。

b) 应对脆弱性进行赋值。

A1.2.3 威胁识别

a) 应参考国家或国际标准，对威胁进行分类；

b)应识别所评估信息资产存在的潜在威胁； c)

应识别威胁利用脆弱性的可能性；

d)应分析威胁利用脆弱性对组织可能造成的影响。 A1.2.4 已有安全措施确认

a) 应识别组织已采取的安全措施；

b) 应评价已采取的安全措施的有效性。

A1.3 风险分析阶段

A1.3.1 风险分析模型建立

a) 应构建风险分析模型。风险分析模型应将资产、威胁、脆弱性三个基本要素及每个要素各自的属性进行关联。

b) 应根据风险分析模型对已识别的重要资产的威胁、脆弱性及安全措施进行分析。

c)应识别威胁利用脆弱性的可能性，分析威胁利用脆弱性对组织可能造成的影响。

d)应根据分析模型确定的方法计算出风险值。

A1.3.2 风险评价

a) 应根据风险评价准则确定风险等级。

A1.3.3 风险评估报告

a) 应向客户提供风险评估报告,报告应包括但不限于评估过程、评估方法、评估结果、处置建议等内容。

A2 二级要求

组织申报二级资质，除满足三级能力要求外，还应满足以下要求：申请二级资质认证的单位，针对多种类型组织，多行业组织，应具备完成的风险评估项目，具备从管理和技术层面对脆弱性进行识别的能力，具备跟踪、验证信息安全漏洞的能力。

A2.1 准 备 阶 段

A2.1.1 服务方案制定

a) 应进行充分的系统调研，形成调研报告。

b) 宜根据风险评估目标以及调研结果，确定评估依据和评估方法。

c)应形成较为完整的风险评估实施方案。

A2.1.2 人员和工具管理

a) 需采取相关措施，保障工具自身的安全性、适用性。

A2.2 风险识别阶段

A2.2.1 威胁识别

a) 应识别出组织和信息系统中潜在的对组织和信息系统造成影响的威胁。

A2.3 风险分析阶段

A2.3.1 风险计算方法确定

a) 在风险计算时应根据实际情况选择定性计算方法或定量计算方法。

A2.3.2 风险评价

a) 应对不同等级的安全风险进行统计、评价，形成最终的总体安全评价。

A2.3.3 风险评估报告

a) 风险评估报告中应对本次评估建立的风险分析模型进行说明，并应阐明本次评估采用的风险计算方法及风险评价方法。

b) 风险评估报告中应对计算分析出的风险给予比较详细的说明。

A2.4 风险处置阶段

A2.4.1 风险处置原则确定

a) 应协助被评估组织确定风险处置原则，以及风险处置原则适用的范围和例外情况。

A2.4.2 安全整改建议

a) 对组织不可接受的风险提出风险处置措施。

A3 一级要求

组织申报一级资质，除满足二级要求外，还应满足以下要求：申请一级资质认证的单位，能够在全国范围内，应具备完成的风险评估项目，具备从业务、管理和技术层面对脆弱性进行识别的能力，具备跟踪、验证、挖掘信息安全漏洞的能力。

A3.1 准备阶段

A3.1.1 人员和工具管理

a) 需采取相关措施，保障工具管理的规范性。

A3.2 风险识别阶段

A3.2.1 资产识别

a) 识别信息系统处理的业务功能，重点识别出关键业务功能和关键业务流程。

b)根据业务特点和业务流程识别出关键数据和关键服务。

c)识别处理数据和提供服务所需的关键系统单元和关键系统组件。 A3.2.2 威胁识别

a) 采用多种方法进行威胁调查。

A3.3 风险处置阶段

A3.3.1 组织评审会

a) 协助被评估组织召开评审会。

b) 依据最终的评审意见进行相应的整改，形成最终的整改材料。

A3.3.2 残余风险处置

a) 对组织提出完整的风险处置方案。

b)必要时，对残余风险进行再评估。

附录 B（规范性附录）：信息系统安全集成服务资质交付能力评价要求

信息系统安全集成服务资质交付能力评价要求针对集成准备、方案设计、建设实施、安全保障四个过程进行，应具备完成的安全集成项目，具体分级要求如下：

B1 三级要求

B1.1 集成准备阶段

B1.1.1 需求调研与分析

a) 调研客户背景信息，采集系统建设需求和建设目标，明确系统功能、性能及安全性要求。

b)基于系统建设需求，提出产品选型方案和建设预算。

c)结合系统建设和安全需求，与客户、设计、开发等人员充分沟通，达成共识并形成记录。 B1.2 方案设计阶段

a) 根据系统建设安全需求，编制安全集成技术方案。

b) 依据技术方案，编制安全集成实施方案，明确项目人员、进度、质量、沟通、风险等方面的要求。

c)结合技术方案和实施方案，与客户进行沟通，获得客户认可。

B1.3 建设实施阶段

B1.3.1 实施集成

a)依据已确认的安全集成项目技术方案和实施方案，按照时间和质量要求进行系统建设。 b)项目实施人员按时提交施工记录和工程日志，及时向项目经理汇报项目进度。

c) 建立安全集成项目协调机制，明确责任人，畅通信息沟通渠道，保障各相关方在项目实施过程中能够有效充分的沟通。

B1.4 安全保障阶段

B1.4.1 系统测试

a) 依据项目技术方案和测试计划，对系统进行联调和系统测试，完整记录测试过程相关信息。

b) 对于新建系统重点测试系统的功能、性能和安全性等；对于系统改造或升级项目，还需进行兼容性测试。

B1.4.2 系统试运行

a) 为测试系统运行的可靠性和稳定性，系统初验后需进行试运行，并记录系统运行状况。

b)基于系统运行相关记录，及时对系统设备进行调整和维护。

B1.4.3 验收

a) 根据合同约定，向客户提交完整的项目资料及交付物，并提出终验申请。

b)根据合同约定，配合组织项目验收，出具项目验收报告。

B1.4.4 运行维护

a) 根据合同约定，向客户提供维保服务，并形成维保记录。

B2 二级要求

组织申报二级资质，除满足三级能力要求外，还应满足以下要求：

B2.1 集成准备阶段

B2.1.1 需求调研与分析

a) 准确识别和综合分析系统在信息安全特性方面相适应的安全需求。

b)基于客户需求和投入能力，开展需求分析，编制需求分析报告。

B2.2 方案设计阶段

a) 结合需求分析和客户在保障系统安全方面的投入能力，提出系统建设安全设计说明书，明确系统架构、产品选型、产品功能、性能及配置等参数。

b) 组织客户及相关技术专家对技术方案和实施方案进行论证，确认是否满足系统功能、性能和安全性要求。

c) 结合技术方案，对项目组及第三方配合人员进行业务和技能培训。

B2.3 建设实施阶段

B2.3.1 实施集成

a) 产品、设备安装调试过程中，应完整妥善记录相关信息。

b)项目建设施工完成后，需向客户提交完工报告。

c)项目实施完成后，相关过程记录及时归档，并统一保管。

B2.4 安全保障阶段

B2.4.1 系统测试

a) 系统测试完成后，制定系统测试报告，并提交客户。

b) 结合项目需要提出初验申请，组织客户及相关方对项目进行初验，并提交初验报告。

B2.4.2 系统试运行

a) 系统进行了试运行。

b) 试运行结束后，项目组制定系统试运行报告，并提交客户。

B2.4.3 运行维护

a) 建立客户满意度调查机制，并对调查结果进行分析。

B3 一级要求

组织申报一级资质，除满足二级要求外，还应满足以下要求：

B3.1 集成准备阶段

B3.1.1 需求调研与分析

a) 协助客户有效识别系统建设过程中的政策、法律和约束条件，有效规避商业风险和泄密事件。

B3.2 方案设计阶段

a) 结合项目需要，编制安全集成项目施工手册和作业指导书。

b) 对于新建系统，建设实施过程应重点关注信息系统的功能、性能和安全性等方面要求。对于系统改造，还应考虑改造前技术测试验证及在实施失败后的回退措施。技术测试验证需要考虑新旧系统的兼容问题，包括网络兼容、系统兼容、应用兼容等。

c) 基于安全集成项目需求和进度计划，编制信息安全产品和工具定制开发计划。

B3.3 建设实施阶段

B3.3.1 实施集成

a) 建立项目变更管理程序，对项目实施过程中方案、资源变更进行有效控制，完整记录变更过程。

b)制定项目应急处置方案和恢复策略，对项目过程中的应急事件及时进行响应。

B3.3.2 监督管理

a) 定期对项目实施情况进行评审，采取适当措施，控制项目风险。

B3.4 安全保障阶段

B3.4.1 系统测试

a) 基于建设系统的安全要求，制定系统安全性测试方案，模拟攻击场景，对系统安全性进行测试。

B3.4.2 系统试运行

a) 制定系统试运行计划，建立应急响应服务保障团队，及时应对突发事件。

b) 综合分析系统运行状态，建立系统运行策略和安全指南，并对相关产品和设备设施进行配置管理。 c)提供试运行记录和报告。

B3.4.3 运行维护

a) 建立维保流程，制定维保方案，并按方案实施维保。

附录 C（规范性附录）：信息安全应急处理服务资质交付能力评价要求

信息安全应急处理服务资质交付能力评价要求针对准备、检测、抑制、根除、恢复、总结六个过程进行，应具备完成的应急处理项目，具体分级要求如下：

C1 三级要求

C1.1 准备阶段

组织申报三级资质，应具有处理一般信息安全事件的能力（注：参考国家标准 GB/Z 20985-2007《信息安全事件分类分级指南》，或参考组织所提供应急处理服务的对象所处的行业对信息安全事件的等级划分标准，主要考察有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件几类），具体见以下要求：

a) 明确客户的应急需求。

b) 了解客户应急预案的内容。

c) 向客户提供应急处理服务流程。

d)可提供本地应急响应服务能力。

e)配备有处理网络或信息安全事件的工具包，包括常用的系统命令、工具软件等。 f)工具包应定期更新。

g) 配备应急处理服务人员。

h) 对在应急处理服务过程中可能会采取的操作、处理等行为，获得用户的书面授权。

C1.2 检测阶段

a) 确定检测对象及范围。

b) 对发生异常的系统进行信息的收集与分析，判断是否真正发生了安全事件。

c)与客户共同确定应急处理方案。

d) 应急处理方案应明确检测范围与检测行为规范，其检测范围应仅限于客户已授权的与安全事件相关的数据，对客户的机密性数据信息未经授权不得访问。

e) 与客户充分沟通，并预测应急处理方案可能造成的影响。

f)检测工作应在客户的监督与配合下完成。

C1.3 抑制阶段

a) 与客户充分沟通，使其了解所面临的首要问题及抑制处理的目的。

b)在采取抑制措施之前，应告知客户可能存在的风险。

c)严格执行抑制处理方案中规定的内容，如有必要更改，须获得客户的书面授权。 d)抑制措施应能够限制受攻击的范围，抑制潜在的或进一步的攻击和破坏行为。

C1.4 根除阶段

a)协助客户检查所有受影响的系统，提出根除的方案建议，并协助客户进行具体实施。 b)应明确告知客户所采取的根除措施可能带来的风险。

c)找出导致网络或信息安全事件发生的原因，并予以彻底消除。 C1.5 恢复阶段

a)告知客户网络或信息安全事件的恢复方法及可能存在的风险。

b)（如需重建系统时适用该条款）对于不能彻底恢复配置和彻底清除系统上的恶意文件，或不能肯定系统经过根除处理后是否可恢复正常时，应选择重建系统。

c)（如需重建系统时适用该条款）应协助客户按照系统的初始化安全策略恢复系统。

d)（如需重建系统时适用该条款）应协助客户验证恢复后的系统是否运行正常，并确认与原有系统配置保持一致。

e)（如需重建系统时适用该条款）在帮助客户重建系统前需进行全面的数据备份，备份的数据要确保是没有被攻击者改变过的数据。

f)（不需重建系统时适用该条款）应建立重建系统的应急工作流程及规范，并开展重建系统的应急演练工作。

C1.6 总结阶段

a)应保存完整的网络或信息安全事件处理记录，并对事件处理过程进行总结和分析。 b)提供网络或信息安全事件处理报告。

c)提供网络或信息安全方面的建议和意见，必要时指导和协助客户实施。 C2 二级要求

组织申报二级资质，除满足三级要求外，还应满足具有处理较大信息安全事件的能力（注：参考国家标准 GB/Z20985-2007《信息安全事件分类分级指南》，或参考组织所提供应急处理服务的对象所处的行业对信息安全事件的等级划分标准，主要考察有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件几类），具体见以下要求：

C2.1 准备阶段

a) 在客户应急需求基础上制定应急服务方案。

b) 应急服务方案应涉及客户应急预案的启动与执行。

c)若客户未建立应急预案，可协助客户建立。

d)应急处理方案应包含实施方案失败的应变和回退措施。 e)提供满足客户要求的应急响应服务能力。

f)网络与信息安全事件工具包中应配备专业技术检测设备。 g)对工具包实行制度化管理。

C2.2 检测阶段

a)建立有针对常规应用系统、安全设备、常见网络与信息安全事件的检测技术规范。 b)协助客户确定安全事件等级。

c)应急处理方案应包含对安全事件的抑制、根除和恢复的详细处理步骤。 C2.3 恢复阶段

a) 与客户共同制定系统恢复方案，根据实际情况协助客户选择合理的恢复方法。

b)（如需重建系统时适用该条款）帮助客户为重建后的系统建立系统快照。

C2.6 总结阶段

a) 网络与信息安全事件处理记录应具备可追溯性。

b) 提供详实的网络与信息安全事件处理报告，完整展现应急处理服务的整个过程。

C3 一级要求

组织申报一级资质，除满足二级要求外，还应满足具有处理重大及特别重大信息安全事件的能力（注：参考国家标准 GB/Z20985-2007《信息安全事件分类分级指南》，或参考组织所提供应急处理服务的对 象所处的行业对信息安全事件的等级划分标准，主要考察有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件几类。监审时，如无处理重大及特别重大安全事件的服务项目案例，也可查验相关的 应急演练记录，或说明所提供应急保障服务的系统的重要程度），具体见以下要求：

C3.1 准备阶段

a)建立有体系化的应急处理服务流程。

b)可提供本地及外地应急响应服务能力。

c) 与客户之间建立安全保密的信息传输渠道。

d)具有自主开发专业检测工具的能力。

C3.2 检测阶段

a) 建立有完善的检测技术规范及具有对高技术入侵的检测技术能力。

b)具有挖掘系统设备及业务系统安全漏洞的能力。

c) 对确认的安全事件启动安全事件管理程序。

d) 应急处理方案中应对可能造成的影响进行分析，包括社会影响。

C3.3 抑制阶段

a) 应使用可信的工具进行安全事件的抑制处理，不得使用受害系统已有的不可信文件。

C3.4 根除阶段

a) 应使用可信的工具进行安全事件的根除处理，不得使用受害系统已有的不可信文件。

C3.5 恢复阶段

（如需重建系统时适用该条款）帮助客户对重建后的系统进行全面的安全加固。 C3.6 总结阶段

a) 对网络与信息安全事件进行总结和分析后，针对典型案例存入事件知识库。

b)提供关闭安全事件管理程序。

c)告知客户所发事件可能涉及到的法律诉讼方面的法律要求或影响。

附录 D（规范性附录）：软件安全开发服务资质交付能力评价要求

软件安全开发服务资质交付能力评价要求针对准备、需求、设计、编码、测试、验收和维保七个阶段进行，应具备完成的软件安全开发项目，具体分级要求如下：

D1 三级要求

D1.1 准备阶段

a)建立软件项目安全开发团队，明确各岗位、人员、职责。

b)制定软件项目安全开发管理计划，明确开发过程管控措施。 c)建立软件开发的配置管理计划，明确配置管理的安全要求。 d)建立变更控制制度，明确软件项目变更控制的安全要求。 e)制定软件项目安全培训计划，对相关人员进行安全培训。 f)建立独立的开发环境，确保开发环境与运行环境隔离。

D1.2 需求阶段

a) 调研项目背景信息，收集项目需求，明确软件功能、性能及安全方面的要求。

b)结合软件项目需求、安全需求，与用户充分沟通，达成共识并形成记录。

D1.3 设计阶段

a) 根据软件项目需求，编制软件设计说明书。

b) 软件设计说明书明确系统/子系统的功能和非功能设计要求。

c) 软件设计说明书明确包含安全功能要求，包括标识与鉴别、访问控制、安全审计和安全管理等。

D1.4 编码阶段

a) 制定统一的代码安全编码规范，确保开发人员参照规范安全编码。

b)依据详细设计说明书，对软件进行安全编码。

c)软件代码要经过安全检查、评审，对于发现的漏洞能有效修复。 D1.5 测试阶段

a) 依据软件设计说明书对软件功能、安全功能进行测试。

b)对测试发现的漏洞进行分析并有效修复。

D1.6 验收阶段

D1.6.1 系统试运行

a) 测试系统运行的可靠性、稳定性和安全性，进行试运行，并记录系统运行状况。

b) 基于系统试运行相关记录，及时对软件进行调整、维护。试运行结束后，制定系统运行报告。

D1.6.2 验收交付

a) 根据合同约定，向客户提交完整的项目资料及交付物，并提出验收申请。

b) 根据合同约定，进行项目验收，形成项目验收报告。

D1.7 维保阶段

a) 对于影响软件系统安全、稳定运行的缺陷，及时有效采取打补丁、版本升级等方式予以消除，并提供远程技术支持服务。

D2 二级要求

组织申报二级资质，除满足三级能力要求外，还应满足以下要求：

D2.1 准备阶段

a) 建立软件安全开发项目风险管理机制，对软件项目进行风险评估。

b)使用配置管理工具对软件项目进行配置管理。

c) 配备专职的测试人员。

d) 建立独立的测试环境，确保测试环境与开发环境隔离。

D2.2 需求阶段

a) 准确识别和综合分析软件项目在可用性、完整性、真实性、机密性、不可否认性、可控性和可靠性等方面的安全需求。

b) 对于数据采集、产生、使用，明确识别安全保护要求。

c) 基于客户需求，开展需求分析，编制具有软件安全需求的分析报告。

d)需求分析报告中明确项目开发中使用的安全技术标准、规范。

D2.3 设计阶段

D2.3.1 概要设计

a) 概要设计说明书应明确数据完整性和保密性、通信完整性和保密性、软件容错、资源控制等安全功能要求。

D2.3.2 详细设计

a) 详细设计说明书中应包含对数据产生、传输、存储、使用、处理和归档安全方面的详细设计。

D2.4 编码阶段

a) 软件代码的安全检查、评审工作应形成记录。

D2.5 测试阶段

D2.5.1 单元测试

a) 明确单元测试策略，制定单元测试计划。

b) 依据详细设计说明书和测试计划进行单元测试设计，并执行单元测试，形成测试记录。

D2.5.2 集成测试

a) 明确集成测试策略，制定集成测试计划。

b) 依据概要设计方案和测试计划进行集成测试设计，并执行集成测试，形成测试记录。

D2.5.3 系统测试

a) 制定包括系统安全性测试在内的测试计划，并执行系统测试，形成测试记录。

b) 基于软件安全功能的安全要求，制定脆弱性测试方案，对安全漏洞进行测试，形成测试记录。

c)对系统测试结果进行分析，形成分析报告。

D2.6 验收阶段

D2.6.1 系统试运行

试运行结束后，制定系统试运行报告，并提交客

户。 D2.6.2 验收交付

提交软件安全测评报告。

D2.7 维保阶段

a) 制定系统运行计划、安全事件响应计划、安全事件应急预案，建立应急响应服务保障团队。

b)及时应对突发安全事件，并向用户提供安全事件解决报告。

D3 一级要求

组织申报一级资质，除满足二级能力要求外，还应满足以下要

求： D3.1 准备阶段

a) 建立软硬件设备和工具等资源安全使用规范。

b)配备安全管理人员。

c)建立变更控制委员会。

D3.2 需求阶段

a) 应基于软件安全威胁开展需求分析。

b) 基于软件项目需求分析建立软件安全开发模型。

D3.3 设计阶段

D3.3.1 概要设计

a) 概要设计说明书中应明确基于软件安全威胁分析的安全要求。

b) 当开发场景适用时，概要设计说明书中应明确抗抵赖、安全标记、可信路径等安全功能要求。

D3.3.2 详细设计

依据安全要求和概要设计说明书，明确基于软件安全威胁分析进行详细设计。 D3.4 编码阶段

采用自动化工具对代码安全漏洞进行审查，对于发现的漏洞能有效修复，并形成审查报告。 D3.5 测试阶段

D3.5.1 单元测试

对单元测试结果进行分析，形成分析报

告。 D3.5.2 集成测试

对集成测试结果进行分析，形成分析报

告。 D3.5.3 系统测试

基于软件项目的安全要求，制定系统渗透性测试方案，模拟攻击场景，对系统安全性进行测试，并形成分析报告。

D3.6 验收阶段

D3.6.1 系统试运行

a) 提供试运行记录和报告。

b) 综合软件系统试运行状态，建立软件系统运行策略和安全指南。

D3.6.2 验收交付

提交软件产品第三方安全测评报告或安全认证证

书。 D3.7 维保阶段

a) 制定软件健康检查计划、方案，定期实施，提交相应的系统健康检查报告、巡检报告。

b)根据健康检查报告进行分析，持续优化系统。

附录 E（规范性附录）：信息系统安全运维服务资质交付能力评价要求

信息系统安全运维服务资质交付能力评价要求针对服务准备、服务设计、服务实施、服务报告四个阶段进行，应具备完成的安全运维项目，具体分级要求如下：

E1 三级要求

E1.1 服务准备阶段

E1.1.1 需求调研与分析

a) 调研客户信息系统安全现状，采集客户安全服务需求与目标，明确客户对信息系统安全运维服务时间、服务期限、服务内容以及服务方式的需求。

b) 进行信息系统运维预算，定义运维服务。

c)与客户进行沟通，达成共识并形成记录。

E1.1.2 签订服务协议

a) 与客户签订服务协议，明确范围、目标、时间、内容、金额、质量和输出等。

b) 明确安全运维的方式，方式包括但不限于：驻场值守方式，定期巡检方式，远程值守方式。

E1.2 服务方案设计阶段

a) 根据系统安全运维需求，编制安全运维服务方案，明确安全运维服务时间、服务内容、服务方式、服务期限、服务人员、服务交付物、服务质量管理、服务沟通机制、服务风险管理等方面要求。

b) 提供安全设备、业务系统的健康检查服务，并约定服务方式、检查频次和检查内容。

c)专业人员负责安全管理的接口。

E1.3 服务实施阶段

a)实施初始服务，根据合同约定服务范围完成信息系统资产识别。 b)采集信息系统重要资产的安全配置、流量信息等安全信息。

c) 对安全设备进行日常维护及监控，并记录硬件故障。

d) 收集与分析网络及安全设备、服务器、数据库、中间件、应用系统的日志。

e) 实施日常巡检服务：对用户的安全设备、网络设备、服务器提供业务操作巡检、状态巡检、安全策略配置巡检服务。

f) 实施日常安全运维服务：完成安全设备、网络设备、服务器、应用系统安全事件监控；病毒监测、查杀及网络防病毒维护；漏洞扫描、安全加固、补丁安装；并有相关记录。

g) 对信息安全事件进行统计与分析。

h) 实施健康检查服务：完成安全设备、业务系统的健康检查服务。

E1.4 服务报告阶段

a) 向客户提交服务报告，定期收集与报告安全运维实施情况。

b) 汇总整理全年服务记录，形成年终安全运维服务总结报告。

c)根据合同约定，配合组织项目验收，出具项目验收报告。

E2 二级要求

组织申报二级资质，除满足三级能力要求外，还应满足以下要求：

E2.1 服务准备阶段

E2.1.1 需求调研与分析

a)分析客户对信息系统安全服务的需求和类型。 b)收集与分析信息系统的可用性指标。

c) 分析以往服务的数据，提取出来未来可自动化的服务(监审时适用)。

E2.1.2 签订服务协议

a) 签订服务级别协议。

E2.2 服务方案设计阶段

a) 编制信息系统的可用性计划，监控可用性事件，报告可用性执行，指导可用性的改进。

b) 识别与分析信息系统运维过程的历史数据，提出系统运维的保障策略和解决方案（监审时适用）。 c)编制信息系统的安全基线。

d)建立信息系统安全的配置库。

E2.3 服务实施阶段

a)收集与建立配置管理数据库，确保配置项目的机密性、完整性、可用性（专职管理）。 b)实施安全设备、网络设备、中间件、数据库、服务器等资产的安全配置管理，定期对配置项进行更新和维护。

c)根据制定的安全配置基线，定期进行安全配置核查工作。 d)实施运维监控与分析并形成记录。

E2.4 服务报告阶段

a) 应定期收集与分析安全运维的关键指标数据，数据包括但不限于：异常报告及时率、异常漏报率、故障隐患发现率、异常主动发现率、问题解决率、漏洞扫描覆盖率、加固设备覆盖率、安全补丁安装及时率、安全事件次数。 (参照服务合同)

b) 建立客户满意度调查机制。

E3 一级要求

组织申报一级资质，除满足二级能力要求外，还应满足以下要求：

E3.1 服务准备阶段

E3.1.1 需求调研与分析

a) 内部团队之间的安全运营级别协议应和与安全运维第三方之间的服务级别设计保持一致。

b)安全组织中要设定安全领导小组。

E3.2 方案设计阶段

a) 建立信息系统应急事件响应机制和恢复保障。

b)编制安全运维项目作业指导书。

c)建立应急响应和灾难恢复机制，形成业务连续性计

划。 d)基于漏洞发现与分析进行信息系统漏洞的管理

工作。

E3.3 服务实施阶段

a) 实施安全培训服务：完成安全意识、基本安全技术的培训服务。

b) 实施安全通告及漏洞分析服务：完成业界动态的通告、收集国家安全政策及法律法规、漏洞通告、病毒通告、厂商安全通告及其他安全通告。

c) 实施应急响应服务：完成应急响应预案制定，对应急事件及时响应，并对应急预案进行演练，形成相关记录。

d) 依据运维变更管理程序，对运维实施过程中方案、资源变更进行有效控制，完整记录变更过程。

e)制定运维应急处置方案和恢复策略，对运维过程中的应急事件及时进行响应。

f) 依据风险评估方案与计划实施信息系统风险评估；依据渗透测试方案与计划实施信息系统渗透测试。

g) 依据漏洞管理方案实施信息系统漏洞管理工作。

E3.4 服务报告阶段

a) 对客户满意度进行趋势分析。

b) 对客户系统的安全态势做出分析，并给出安全建议。

附录 F（规范性附录）：信息系统灾难备份与恢复服务资质交付能力评价要求

信息系统灾难备份与恢复服务资质分 A（资源服务类）、B（技术服务类）两个类型，每个类型的服务内容不同：

A 类的服务内容有：灾备中心场地资源服务、灾备中心基础设施服务、灾备中心运维服务。

B 类的服务内容有：方案设计、系统建设与管理、预案制定与演练.

具体分级要求如下：

F1 三级要求

F1.1 灾备中心场地资源要求

a) 拥有至少 1 个可用于灾备中心的场地，位置避免处于地质沉降地带，交通便利、抗震等级按照国家规定的该地区抗震设防烈度执行，抗震设防类别为丙类及以上。

b) 机房设置 7×24 小时门禁系统，所有进入机房的外部人员均需获得授权。

c) 提供7×24 小时闭路电视监控，其中公共区域的监控数据保留 1 个月以上，机房区域的监控数据保留 2 个月以上。

d) 具备较高灵敏度的烟雾探测系统和消防系统，可实现分区灭火和定点报警。

e)灾备中心建筑耐火等级达到二级及以上。

F.1.2 灾备中心基础设施要求

a) 拥有灾备中心基础保障设施，包括但不限于供配电设施、空调暖通设施、给排水设施、监控设施、货运设施等，并定期检查。

b) 拥有灾备中心基础配套设施，包括但不限于灾难恢复指挥中心、灾难恢复坐席、办公区、新闻发布中心、会议室、培训教室、模拟演练室等。

c) 拥有灾备中心基础生活设施，包括但不限于日常运维人员生活所需宿舍、食堂、活动室等。

d) 拥有灾备中心运行所需工作环境，包括但不限于计算机机房、主操作室、通讯机房、介质机房、信息系统设备测试维修机房等。

e) 具备单路高压供电和独立 UPS 不间断电源保障。 f)

采用精密空调系统，并具备恒温恒湿要求。

F.1.3 灾备中心运维管理要求

a) 拥有灾备中心运维组织架构和运行管理团队，建立灾备中心机房运行管理和信息安全管理制度，

并有效运行。

b) 建立灾备中心信息系统运行监控平台，及时发现灾备系统运行的故障并进行故障定位、诊断和审计，保存相关记录。

c) 建立灾备中心与生产中心统一变更流程。

d) 定期开展数据验证工作，确保生产与灾备数据的一致性、完整性和可用性。

F.1.4 方案设计要求

a) 开展灾难恢复系统建设需求调研，并进行需求分析。

b) 按照灾难恢复规划和客户的投入能力，制定灾难备份与恢复系统技术方案、实施方案。

F.1.5 系统建设与管理要求

a) 依据灾难备份与恢复实施方案，实施灾难备份与恢复系统建设。

b)妥善保存灾难备份与恢复系统建设过程记录文档。

F.1.6 预案制定与演练要求

a) 制定信息系统灾难恢复预案。

b) 开展信息系统灾难恢复桌面推演，并详细记录。

c)结合项目需要，组织开展灾难恢复预案培训。

F2 二级要求

F2.1 灾备中心场地资源要求

a) 拥有至少 1 个可用于灾备中心的场地，位置避免处于地质沉降地带，交通便利、抗震等级按照国家规定的该地区抗震设防烈度执行，抗震设防类别为丙类及以上。

b) 机房设置 7×24 小时门禁系统，所有进入机房的外部人员均需获得授权。

c) 提供 7×24 小时闭路电视监控，其中公共区域的监控数据保留 1 个月以上，机房区域的监控数据保留 2 个月以上。

d) 具备较高灵敏度的烟雾探测系统和消防系统，可实现分区灭火和定点报警。

e)灾备中心建筑耐火等级达到二级及以上。

f) 拥有至少2个在不同地域的可用于灾备中心的场地资源，抗震设防烈度按照国家规定的该地区抗震设防烈度执行，抗震设防类别为乙类及以上。

g) 灾备中心建设等级满足国标A级或国际T3以上机房要求。

h) 具备气体灭火的消防系统，并具备早期报警系统/温感和烟感系统两级报警。

F.2.2 灾备中心基础设施要求

a) 拥有灾备中心基础保障设施，包括但不限于供配电设施、空调暖通设施、给排水设施、监控设施、货运设施等，并定期检查。

b) 拥有灾备中心基础配套设施，包括但不限于灾难恢复指挥中心、灾难恢复坐席、办公区、新闻发布中心、会议室、培训教室、模拟演练室等。

c) 拥有灾备中心基础生活设施，包括但不限于日常运维人员生活所需宿舍、食堂、活动室等。

d) 拥有灾备中心运行所需工作环境，包括但不限于计算机机房、主操作室、通讯机房、介质机房、信息系统设备测试维修机房等。

e) 具备单路高压供电和独立 UPS 不间断电源保障。 f)

采用精密空调系统，并具备恒温恒湿要求。

g) 建立并运行基础设施日常巡检、监控、检查、维护、性能和容量管理、系统优化、应急与故障演练制度和流程。

h) 具备双路高压供电和双路 UPS 供电，拥有后备发电机组，并能在 UPS 后备时间内提供电力供应，满足全部负荷连续运行 48 小时以上。

i) 采用精密空调系统，机房温度应达到 22 ° C ± 2 ° C，湿度应达到 45%-65%。

F.2.3 灾备中心运维管理要求

a) 拥有灾备中心运维组织架构和运行管理团队，建立灾备中心机房运行管理和信息安全管理制度，并有效运行。

b) 建立灾备中心信息系统运行监控平台，及时发现灾备系统运行的故障并进行故障定位、诊断和审计，保存相关记录。

c) 建立灾备中心与生产中心统一变更流程。

d) 定期开展数据验证工作，确保生产与灾备数据的一致性、完整性和可用性。

e)灾备中心建立与生产中心统一的运维管理流程，实现两个中心联动运维。

f)灾备中心建立完整的电子化 IT 资产管理系统，能动态跟踪灾备中心 IT 资产变更。

g)灾备中心提供统一的客户服务平台，集中受理客户服务请求。

h) 妥善保管运维记录，所有文档应满足客户监管机构要求。

i) 定期开展灾难恢复模拟切换演练工作，确保发生灾难时，灾备系统能够接替生产系统运行。

F.2.4 方案设计要求

a) 开展灾难恢复系统建设需求调研，并进行需求分析。

b) 按照灾难恢复规划和客户的投入能力，制定灾难备份与恢复系统技术方案、实施方案。

c) 按照不同灾难恢复等级对资源的要求，确定灾备中心基础设施、数据备份系统、备用数据处理系统和备用网络系统等方面的需求，形成调研报告。

d) 对业务系统中断后的损失进行分析，制定业务系统的最大可容忍业务中断时间（RTO）、最大可容忍中断时间点（RPO）。

e) 依据系统建设要求和技术方案，制定系统测试方案。

F.2.5 系统建设与管理要求

a) 依据灾难备份与恢复实施方案，实施灾难备份与恢复系统建设。

b)妥善保存灾难备份与恢复系统建设过程记录文档。

c) 依据测试方案，组织实施系统测试，并详细记录。

d) 制定灾难备份与恢复系统试运行方案，并详细记录试运行过程情况。

F.2.6 预案制定与演练要求

a) 制定信息系统灾难恢复预案。

b) 开展信息系统灾难恢复桌面推演，并详细记录。

c)结合项目需要，组织开展灾难恢复预案培训。

d)制定系统演练方案，明确演练范围、人员、场景、步骤等内容。 e)组织演练培训和动员，明确参演人员角色、职责和具体任务。 f)设计多种演练场景并组织推演，详细记录演练过程。

F3 一级要求

F3.1 灾备中心场地资源要求

a) 拥有至少 1 个可用于灾备中心的场地，位置避免处于地质沉降地带，交通便利、抗震等级按照国家规定的该地区抗震设防烈度执行，抗震设防类别为丙类及以上。

b) 机房设置 7×24 小时门禁系统，所有进入机房的外部人员均需获得授权。

c) 提供7×24 小时闭路电视监控，其中公共区域的监控数据保留 1 个月以上，机房区域的监控数据

保留2个月以上。

d) 具备较高灵敏度的烟雾探测系统和消防系统，可实现分区灭火和定点报警。

e)灾备中心建筑耐火等级达到二级及以上。

f) 拥有至少2个在不同地域的可用于灾备中心的场地资源，抗震设防烈度按照国家规定的该地区抗震设防烈度执行，抗震设防类别为乙类及以上。

g) 灾备中心建设等级满足国标A级或国际T3以上机房要求。

h) 具备气体灭火的消防系统，并具备早期报警系统/温感和烟感系统两级报警。

i) 拥有至少2个在不同地域且处于不同的风险区域的灾备中心，满足异地灾备场地要求。 j)

灾备中心应符合环保要求，采用高效新风换气系统，机房内正压，确保机房洁净度。

k) 灾备中心的所有通道、机房内均设置。摄像头和7X24小时监控，并且可以按照客户的要求提供更长的保存期限。

l) 灾备中心建筑耐火等级达到一级。

F.3.2 灾备中心基础设施要求

a) 拥有灾备中心基础保障设施，包括但不限于供配电设施、空调暖通设施、给排水设施、监控设施、货运设施等，并定期检查。

b) 拥有灾备中心基础配套设施，包括但不限于灾难恢复指挥中心、灾难恢复坐席、办公区、新闻发布中心、会议室、培训教室、模拟演练室等。

c) 拥有灾备中心基础生活设施，包括但不限于日常运维人员生活所需宿舍、食堂、活动室等。

d) 拥有灾备中心运行所需工作环境，包括但不限于计算机机房、主操作室、通讯机房、介质机房、信息系统设备测试维修机房等。

e) 具备单路高压供电和独立UPS不间断电源保障。 f)

采用精密空调系统，并具备恒温恒湿要求。

g) 建立并运行基础设施日常巡检、监控、检查、维护、性能和容量管理、系统优化、应急与故障演练制度和流程。

h) 具备双路高压供电和双路UPS供电，拥有后备发电机组，并能在UPS后备时间内提供电力供应，满足全部负荷连续运行48小时以上。

i) 采用精密空调系统，机房温度应达到 22 ° C ± 2 ° C，湿度应达到 45%-65%。

j) 高压电来自两个独立的变电站的双路设计。

k) 后备发电机组具有不停机补充燃料的能力，并且与燃料供应商签署燃料供应保障协议，保障燃料数量和质量要求，UPS 和油机可自动切换。

F.3.3 灾备中心运维管理要求

a) 拥有灾备中心运维组织架构和运行管理团队，建立灾备中心机房运行管理和信息安全管理制度，并有效运行。

b) 建立灾备中心信息系统运行监控平台，及时发现灾备系统运行的故障并进行故障定位、诊断和审计，保存相关记录。

c) 建立灾备中心与生产中心统一变更流程。

d) 定期开展数据验证工作，确保生产与灾备数据的一致性、完整性和可用性。

e)灾备中心建立与生产中心统一的运维管理流程，实现两个中心联动运维。

f) 灾备中心建立完整的电子化 IT 资产管理系统，能动态跟踪灾备中心 IT 资产变更。 g)

灾备中心提供统一的客户服务平台，集中受理客户服务请求。

h) 妥善保管运维记录，所有文档应满足客户监管机构要求。

i) 定期开展灾难恢复模拟切换演练工作，确保发生灾难时，灾备系统能够接替生产系统运行。

j)采用运维监控和流程管理工具，实现对多数据中心资源的统一监控和自动化管理。

k) 针对特定的灾难场景进行灾难恢复真实切换演练，并能接替生产完成至少 2 个小时的真实交易，并能在规定时间内进行回切。

l) 具备真实切换演练的方案设计、培训、实施管理和应急处置能力。

m)定期维护灾难恢复预案，及时更新和分发预案文档，确保预案体系持续有效。

n)建立灾备中心应急管理体系，确保灾备系统稳定运行。

F.3.4 方案设计要求

a) 开展灾难恢复系统建设需求调研，并进行需求分析。

b) 按照灾难恢复规划和客户的投入能力，制定灾难备份与恢复系统技术方案、实施方案。

c) 按照不同灾难恢复等级对资源的要求，确定灾备中心基础设施、数据备份系统、备用数据处理系统和备用网络系统等方面的需求，形成调研报告。

d) 对业务系统中断后的损失进行分析，制定业务系统的最大可容忍业务中断时间（RTO）、最大可

容忍中断时间点（RPO）。

e) 依据系统建设要求和技术方案，制定系统测试方案。

f) 识别客户的信息资产及其脆弱性和威胁，对基础设施和信息系统进行风险评估，制定本地风险控制策略和灾难恢复策略。

g) 分析业务系统与应用系统之间的关联关系，确定应用系统灾难恢复指标和恢复优先级别。

F.3.5 系统建设与管理要求

a) 依据灾难备份与恢复实施方案，实施灾难备份与恢复系统建设。

b)妥善保存灾难备份与恢复系统建设过程记录文档。

c) 依据测试方案，组织实施系统测试，并详细记录。

d) 制定灾难备份与恢复系统试运行方案，并详细记录试运行过程情况。

F.3.6 预案制定与演练要求

a) 制定信息系统灾难恢复预案。

b) 开展信息系统灾难恢复桌面推演，并详细记录。

c)结合项目需要，组织开展灾难恢复预案培训。

d)制定系统演练方案，明确演练范围、人员、场景、步骤等内容。 e)组织演练培训和动员，明确参演人员角色、职责和具体任务。 f)设计多种演练场景并组织推演，详细记录演练过程。

g) 制定信息系统灾难恢复预案体系，包括应急预案和恢复预案。

h)基于特定的演练场景，制定详细的切换演练方案。

i) 组织完成真实切换演练前的桌面推演和模拟测试工作。

j) 详细记录演练过程并进行总结，及时修订应急和恢复预案体系。

附录 G（规范性附录）：业控制系统安全服务资质交付能力评价要求

工业控制系统安全服务资质级别是衡量服务提供方的工业控制系统安全服务资格和能力的尺度。工业控制系统安全服务资质专业评价要求针对安全服务规划、服务实施、服务总结三个过程进行，项目实施过程应形成文件，具体分级要求如下：

G1 三级要求

申请三级资质认证的单位，至少有 1 个针对工业生产行业领域的系统集成或系统运维的服务项目；在技术和管理方面具备安全服务的过程管理、风险管理，以及识别跟踪信息安全漏洞的能力；具备安全问题解决的验证和证据分析、安全服务不断提升改进的能力。

G1.1 服务规划阶段

G1.1.1 调研客户需求 a) 调研业务情况，或编制工业控制系统调研表，并按照需要收集有效信息。 b) 有效掌握工业企业的组织结构、了解对工业控制系统的管理机制。 c) 采集客户对工业控制系统安全管理和技术服务的目标和需求。

G1.1.2 分析服务业务 a) 识别工业控制系统面临的潜在威胁，分析服务过程中可能生产的安全风险；

b) 识别影响工业控制系统安全服务的法律、政策、标准、外部影响和约束条件； c) 分析客户业务需求，明确客户工业控制系统安全服务的目标与需求。

G1.1.3 编制服务方案 a) 结合调研的安全需求，与客户、工业控制系统开发单位及其他相关人员充分沟通，编制安 全服务技术方案和服务预算。 b) 与客户签订服务协议，编制实施方案，明确服务范围、目标、进度、内容、金额、交付质 量、沟通和风险等方面的要求。

G1.1.4 组建服务团队 a) 应考虑服务项目的目标、内容、范围等组建团队。 b) 选择工业控制系统安全服务项目负责人应满足通用评价要求的人员能力要求，熟悉工业控 制系统业务流程,能与工业控制系统运行人员进行有效沟通。

G1.1.5 实施准备 a) 应根据服务内容准备必要的工具。 b) 对服务过程中可能会采取的操作、处理等行为，获得用户的书面授权。 c) 对团队成员进行安全教育、信息安全服务技能和工业控制系统操作规程培训。

G1.2 服务实施阶段

G1.2.1 项目实施 a) 实施初始服务，采集工业控制系统重要资产以及资产的安全配置；收集与分析网络及安全设备、服务器、数据库、中间件、应用系统的日志；收集和分析工业控制系统的硬件故障及安

全事件。 b) 依据已确认的安全服务技术方案和实施方案，按照时间和质量要求进行安全集成服务\安全 运维和风险评估服务。 c) 对工业控制系统的应用系统升级、补丁升级和病毒库升级应在线下模拟环境中进行验证，在不影响系统可用性、实时性和稳定性的前提下实施更新。 d) 在实施过程中，必须遵守工业控制系统的相关操作章程，以防止敏感信息泄漏和确保及时处理意外事件。 e) 对直接涉及在运工业控制系统的安全服务，尽可能避开安全生产的敏感时期和业务高峰期。 f) 针对工业控制系统业务特点和系统组成，分析系统脆弱性形成原因，识别跟踪工业控制系 统的漏洞，在服务过程中采取有效措施避免安全风险。 g) 项目实施人员按时提交服务记录，及时向项目经理汇报项目进度。 h) 建立安全服务项目协调机制，明确责任人，畅通信息沟通渠道，保障各相关方在项目实施过程中能够有效充分的沟通。

G1.2.2 系统运行测试 a) 实施结束后，对工业控制系统进行功能和性能检测，保障系统运行的可靠性和稳定性，并记录系统运行状况。 b) 必要时，制定系统安全性测试方案，对于系统改造或升级项目，还需进行兼容性测试，完整记录测试过程相关信息。 c) 建立系统维保服务流程，制定维保方案并形成维保记录。

G1.3 服务总结阶段

G1.3.1 服务验收 a) 根据合同约定，向客户提交完整的项目交付物，并提出终验申请。 b) 根据合同约定，配合组织项目验收，出具项目验收报告。 c) 验收报告中应描述工业控制系统在验收时的运行状况，以及客户单位的反馈意见。

G1.3.2 服务交接 a) 告知客户工业控制系统网络安全现状和可能存在的安全风险。 b) 提供针对安全风险的应对建议，必要时指导和协助客户实施。 c) 应建立报告的批准和交付程序，保留交付记录。

G1.3.3 服务总结 a) 应保存完整的安全服务工作记录，并对安全服务过程进行总结和分析，提交工业控制系统网络安全服务的工作报告，内容应包括项目概况、依据、服务过程、结论、进一步工作建议，以及工业控制系统安全服务过程中发现问题等。b) 应形成和保存工业控制系统的状态和防护情况的记录，包括工业控制系统的业务流程、系统组成、设备配置、存在漏洞，以及采取的安全措施。 c) 应指派至少一人复核与评价相关的所有信息和结果，复核应由未参与评价过程且熟悉相应生产行业业务领域的人员进行。

G2 二级要求

组织申报二级资质，除满足三级能力要求外，还应满足以下要求： 申请二级资质认证的单位，至少完成 3 个与申请工业控制领域一致的完整的安全集成或安全运维服务项目；在技术和管理方面具备安全服务的过程管理、风险管理能力；具备针对工业控制系统开 展风险评估服务的能力；具备安全问题解决的验证和证据分析、安全服务不断提升改进的能力。

G2.1 服务规划阶段

G2.1.1 调研客户需求 a) 调研客户工业控制系统的业务逻辑、工作流程，工业控制系统的设备组成、网络架构等。 b) 编制完整的客户调研报告，调研的内容包括组织架构、制度列表、业务流程、工业控制系统资产信息、工业控制系统相关的管理人员信息等。

G2.1.2 分析服务业务 a) 了解所属行业主管部门对工业控制系统安全要求。

G2.1.3 编制服务方案 a) 制定针对人员、设备、文档、系统的风险监控措施，有效保障工业控制系统的安全、稳定。 b) 对于在运工业控制系统，应搭建控制系统的模拟环境，模拟真实系统的运行情况、配置、数据、业务流程，验证方案的有效性。 c) 安全服务技术方案和实施方案应经过评审，并与客户达成一致。

G2.1.4 组建服务团队 a) 团队成员必须包括所服务业务领域的工业控制系统专业人员，熟悉工业控制系统工作原理、业务流程和操作规程。

G2.1.5 实施准备 a) 应根据服务的需求准备必要的工具，具有工具定制研发的能力。 b) 结合项目需要，编制安全服务项目施工手册和作业指导书。 c) 对团队成员进行安全服务技能培训和工业控制系统原理、组成和操作的培训。

G2.2 服务实施阶段

G2.2.1 项目实施 a) 建立服务过程质量监控机制，监督工业控制系统安全服务实施的过程，定期开展工业控制 系统安全服务质量检查。 b) 针对工业控制系统业务特点和系统组成，分析系统脆弱性形成原因，识别跟踪和验证工业控制系统的漏洞，在服务过程中采取有效措施避免安全风险。 c) 如有远程服务的需求，应建立远程访问审批流程，经批准后方能实施，实施过程应采取必要的访问控制策略并对操作过程进行安全审计。 d) 应编制服务过程中发现的工业控制系统安全风险的风险列表。

G2.2.2 风险评估 a) 识别工业控制系统的重要资产、安全威胁、脆弱性，验证已有的安全措施，构建风险分析模型进行风险计算和评价，给出风险评估报告； b) 协助用户确定风险处置原则，对组织不可

接受的风险提出风险处置措施。 c) 对客户提出完整的风险处置方案，协助客户进行风险处置，必要时，对残余风险进行再评估。

G2.2.3 系统运行测试 a) 制定系统安全性测试方案，在运行系统中或模拟环境中进行测试，完整记录测试过程相关信息，形成系统测试报告。

G2.3 服务总结阶段

G2.3.1 服务验收 a) 应建立程序，对服务验收中可能存在的重要分歧或者遗漏及时更正，并将更正后的验收报告提交给用户方。

G2.3.2 服务交接 a) 建立客户满意度调查机制。

G2.3.3 服务总结 a) 验证在服务过程中发现的工业控制系统的漏洞，建立管理机制跟踪漏洞消缺情况。 G3 一级要求

组织申报一级资质，除满足二级能力要求外，还应满足以下要求：申请一级资质认证的单位，至少完成 6 个与申请工业控制领域一致的完整的安全集成和安全运 维服务项目；在技术和管理方面具备安全服务的过程管理、风险管理能力；具备针对工业控制系统开展风险评估服务、应急处理服务的能力；具备安全问题解决的验证和证据分析、安全服务不断提 升改进的能力。

G3.1 服务规划阶段

G3.1.1 调研客户需求 a) 调研客户企业愿景，对工业控制系统安全业务的发展规划和未来几年业务发展目标。

G3.1.2 分析服务业务 a) 对客户的安全生产和网络安全现状进行评估，调研行业安全防护的水平，明确薄弱环节。

G3.1.3 编制服务方案 a) 确定实施过程的备份机制和应急处理方案，并与客户充分沟通，预测应急处理方案可能造 成的影响。

G3.1.4 组建服务团队 a) 团队成员必须配备能够对工业控制系统进行应急处理的服务人员。

G3.1.5 实施准备 a) 具有根据工业控制系统特点，自主开发专业检测工具的能力。 b) 配备有处理网

络或信息安全事件的工具包，包括常用的系统命令、工具软件等。 c) 应根据服务的需求配备必要的服务质量监测手段，具备对服务行为进行审计的能力。

G3.2 服务实施阶段

G3.2.1 项目实施 a) 有能力利用客户的备用设备或仿真环境搭建控制系统的模拟环境，模拟真实系统的结果、 配置、数据、业务流程，在仿真系统中验证服务内容和测试，以保障在运系统的安全、稳定运行。 b) 建立服务过程质量监控机制，定期开展服务质量评价工作，能够对多个团队的服务质量的一致性进行把控。

G3.2.2 风险评估及应急处置 a) 能够对工业控制系统发生的网络安全事件进行原因分析，采取措施抑制或根除潜在的安全 风险，提交应急处置方案。 b) 网络与信息安全事件处理记录应具备可追溯性。 G3.2.3 系统运行测试 a) 制定系统安全性测试方案，模拟攻击场景，在模拟环境中进行安全性测试，形成测试报告。 b) 综合分析控制系统运行状况，制定安全运维、应急响应方案。

G3.3 服务总结阶段

G3.3.1 服务验收 无

G3.3.2 服务交接 a) 建立应急保障团队，及时响应客户需求。

G3.3.3 服务总结 a) 建立服务项目知识库，积累和汇总不同行业的业务知识和系统特点。 b) 提供详实的网络与信息安全事件处理报告，完整展现应急处理服务的整个过程。

附录 H:参考文献

[1]GB/T20261-2006 信息技术系统安全工程能力成熟度模型

[2]YD/T1621-2007 网络与信息安全服务资质评价准则

[3]YD/T2252-2011 网络与信息安全风险评估服务能力评价方法 [4]RB/T201-2013 信息系统安全集成服务资质认证评价要求 [5]《计算机信息系统集成企业资质等级评定条件》

[6]《通信信息网络系统集成企业资质认定》

[7]《安防工程企业资质评定标准》中安协资[2007]2 号

[8]《建筑智能化工程专业承包企业资质等级标准》

[9]GB/T22080/ISO/IEC 27001《信息技术 安全技术 信息安全管理体系 要求》 [10]CCRC-ISV-C01《信息安全服务规范》

[11]GB/T37988《信息安全技术 数据安全能力成熟度模型》