文件编码：ISCCC-SV-001:2015

信息安全服务资质认证实施规则

（第 2 版）

2015-04-01 发布　　2015-04-01 实施

中国信息安全认证中心 发布

目 录

1. 适用范围

信息安全服务资质认证是依据国家认证认可法律法规、相关技术标准和规范，对信息安全服务提供者的资质进行评价的合格评定活动。

本规则规定了信息安全服务提供者（以下简称服务提供者）应具备的通用评价要求、专业评价要求以及认证机构开展服务资质认证的程序。

本规则可用于第三方机构对服务提供者进行资信和能力评价，可作为服务提供者开展自我评价的依据，并可为政府及有关社会组织选择服务提供者提供依据。

2. 规范性引用文件

下列文件中的条款通过本文件引用而成为本文件的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本文件，然而，鼓励根据本文件达成协议的各方研究可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本文件。

CNCA/CTS 0052-2007《信息安全服务资质认证技术规范》

YDT1799-2008《网络与信息安全应急处理服务资质评估方法》

ISCCC-SV-002:2010《信息安全风险评估服务资质认证实施规则》

ISCCC-SV-003:2014《信息系统安全集成服务资质认证实施规则》

ISCCC-SV-004:2012《信息系统灾难备份与恢复服务资质认证实施规则》

GB/T 5271.8-2001《信息技术词汇第8部分：安全》中的术语和定义适用于本标准。

3. 术语与定义

3.1. 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/IEC TR 15443-1:2005《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》）

3.2. 信息安全服务资质

信息安全服务资质是信息安全服务机构提供安全服务的一种资格，包括法律地位、资源状况、管理水平、 技术能力等方面的要求。

3.3. 信息安全风险评估

运用科学的方法和手段，系统地分析网络与信息系统所面临的威胁及其存在的脆弱性，评估安全事件一旦发生可能造成的危害程度，提出有针对性的抵御威胁的防护对策和整改措施，以求防范和化解信息安全风险，或将风险控制在可接受的水平。

3.4. 信息安全应急处理

制定应急处理计划，组织实施演练，并在出现网络与信息系统安全事故时，及时实施应急处理

计划的过程。

3.5. 信息系统安全集成

在从事网络系统、应用系统、安防系统、建筑智能化系统的集成过程中，所进行的安全需求界定、安全设计、安全实施、安全保障等活动。

3.6. 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活动，分为资源服务类（A 类）、技术服务类（B 类）两个类别。

3.7. 软件安全开发

通过对软件开发过程的控制，将开发的软件存在的风险控制在可接受的水平。

3.8. 信息系统安全运维

通过技术设施安全评估，技术设施安全加固，安全漏洞补丁通告、安全事件响应以及信息安全运维咨询，协助组织的信息系统管理人员进行信息系统的安全运维工作，以发现并修复信息系统中所存在的安全隐患，降低安全隐患被非法利用的可能性，并在安全隐患被利用后及时加以响应。

4. 通用评价要求

通用评价要求适用于风险评估、安全集成、应急处理、灾难备份与恢复、软件安全开发、安全运维等类别的信息安全服务认证评价，均分为三个级别，其中一级最高。

4.1. 三级评价要求

4.1.1. 法律地位要求

在中华人民共和国境内注册的独立法人组织，发展历程清晰，产权关系明确。

4.1.2. 财务资信要求

近 3 年经营状况良好，财务数据真实可信，应提供在中华人民共和国境内登记注册的会计师事务所出具的近 3 年财务审计报告。

4.1.3. 办公场所要求

拥有长期固定办公场所和相适应的办公条件，能够满足机构设置及其业务需要。

4.1.4. 人员素质与资质要求

a) 组织负责人拥有2年以上信息技术领域管理经历。

b) 技术负责人获得信息安全相关专业硕士及以上学位或电子信息技术类中级职称，且从事信息安全技术工作2年以上。

c） 财务负责人具有财务系列初级以上职称。

d） 从事信息安全服务人员10名以上。

e） 拥有信息安全专业认证（与申报类别一致）人员2名以上。

f） 拥有项目管理资格证书人员1名以上。

4.1.5. 业绩要求

a） 从事信息安全服务（与申报类别一致）1年以上。

b） 近3年内签订并完成至少1个信息安全服务（与申报类别一致）项目。

4.1.6. 服务管理要求

a） 遵循国家相关法律法规、标准要求，无违法违规记录，资信状况良好。

b） 建立人员管理程序和能力考核指标；制定业务和技能培训计划，定期对相关人员开展培训和考核。

c） 建立文档控制程序，明确文档管理职责，任命管理人员，确保项目文档资料妥善保管。

d） 建立项目管理制度，并按照制度执行。

e） 提供资源，确保信息安全服务项目的实施。

4.1.7. 服务合同要求

a) 了解客户及所处的行业对信息安全服务的特定要求。

b) 确定信息安全服务范围。

c) 应签订信息安全服务合同或协议。

4.1.8. 服务安全要求

a） 满足法律法规对服务安全的要求。

b） 满足与客户签订服务合同中的安全要求。

c） 制定保密管理制度，明确岗位保密责任。

d） 按照客户要求，对于接触到的客户敏感信息和知识产权信息予以保护，并确保服务方人员了解客户的相关要求。

e） 与相关人员签订保密协议，并进行保密教育。

f） 确保其供应商满足上述服务安全要求。

4.1.9. 服务技术要求

a） 建立信息安全服务（与申报类别一致）流程。

b） 制定信息安全服务（与申报类别一致）规范并按照规范实施。

4.2. 二级评价要求

4.2.1. 法律地位要求

在中华人民共和国境内注册的独立法人组织，发展历程清晰，产权关系明确。

4.2.2. 财务资信要求

近 3 年经营状况良好，财务数据真实可信，应提供在中华人民共和国境内登记注册的会计师事务所出具的近 3 年财务审计报告。

4.2.3. 办公场所要求

拥有长期固定办公场所和相适应的办公条件，能够满足机构设置及其业务需要。

4.2.4. 人员素质与资质要求

a) 组织负责人拥有3年以上信息技术领域管理经历。

b) 技术负责人应获得信息安全相关专业硕士及以上学位或电子信息技术类高级职称，且从事信息安全技术工作5年以上。

c) 财务负责人具有财务系列中级以上职称。

d) 从事信息安全服务人员30名以上。

e) 拥有信息安全专业认证（与申报类别一致）人员6名以上。

f) 拥有项目管理资格证书人员2名以上。

4.2.5. 技术工具要求

a) 具备独立的测试环境及必要的软、硬件设备，用于技术培训和模拟测试。

b) 具备承担信息安全服务（与申报类别一致）项目所需的安全工具，并对工具进行管理和版本控制。

4.2.6. 业绩要求

a) 从事信息安全服务（与申报类别一致）3年以上，或取得信息安全服务（与申报类别一致）三级资质1年以上。

b) 近三年内签订并完成至少6个信息安全服务项目（与申报类别一致）。

4.2.7. 服务管理要求

a) 遵循国家相关法律法规、标准要求，无违法违规记录，资信状况良好。

b) 建立项目管理制度，并按照制度执行。

c) 参照国际或国内标准，建立业务范围覆盖信息安全服务的质量管理体系，并有效运行。

d) 参照国际或国家标准，建立业务范围覆盖信息安全服务的信息安全管理体系或信息技术服务管理体系，并有效运行。

e) 提供资源，确保信息安全服务项目的实施。

4.2.8. 服务合同要求

a) 了解客户及所处的行业对信息安全服务的特定要求。

b) 确定信息安全服务范围。

c) 应签订信息安全服务合同或协议。

d) 合同应明确信息安全服务的行为规范。

4.2.9. 服务安全要求

a) 满足法律法规对服务安全的要求。

b) 满足与客户签订服务合同中的安全要求。

c) 制定保密管理制度，明确岗位保密责任。

d) 按照客户要求，对于接触到的客户敏感信息和知识产权信息予以保护，并确保服务方人员了解客户的相关要求。

e) 与相关人员签订保密协议，并进行保密教育。

f) 确保其供应商满足上述服务安全要求。

4.2.10. 服务技术要求

a) 建立信息安全服务（与申报类别一致）流程。

b) 制定信息安全服务（与申报类别一致）规范并按照规范实施。

4.3. 一级评价要求

4.3.1. 申请条件

取得信息安全服务（与申报类别一致）二级资质 1 年以上。（行业领头企业除外）

4.3.2. 法律地位要求

在中华人民共和国境内注册的独立法人组织，发展历程清晰，产权关系明确。

4.3.3. 财务资信要求

近 3 年经营状况良好，财务数据真实可信，应提供在中华人民共和国境内登记注册的会计师事务所出具的近 3 年财务审计报告。

4.3.4. 办公场所要求

拥有长期固定办公场所和相适应的办公条件，能够满足机构设置及其业务需要。

4.3.5. 人员素质与资质要求

a) 组织负责人拥有4年以上信息技术领域管理经历。

b) 技术负责人应获得信息安全相关专业硕士及以上学位或电子信息技术类高级职称，且从事信息安全技术工作8年以上。

c） 财务负责人拥有财务系列高级职称，或取得中级职称8年以上。

d） 从事信息安全技术服务人员50名以上。

e） 拥有信息安全专业认证人员（与申报类别一致）10名以上。

f） 拥有项目管理资格证书人员5名以上。

4.3.6. 技术工具要求

a） 具备独立的测试环境及必要的软、硬件设备，用于技术培训和模拟测试。

b） 具备承担信息安全服务（与申报类别一致）项目所需的安全工具，如漏洞扫描工具、渗透测试工具、协议分析仪等。

4.3.7. 业绩要求

a） 从事信息安全服务（与申报类别一致）5年以上。

b） 近三年内至少签订并完成10个信息安全服务项目（与申报类别一致）。

4.3.8. 服务管理要求

a） 遵循国家相关法律法规、标准要求，无违法违规记录，资信状况良好。

b） 建立项目管理制度，并按照制度执行。

c） 参照国际、国内标准，建立业务范围覆盖信息安全服务的质量管理体系，并提供有效运行的相关证明。

d） 参照国际、国家标准，建立业务范围覆盖信息安全服务的信息安全管理体系或信息技术服务管理体系，并提供有效运行的相关证明。

e） 提供足够资源，确保信息安全服务项目的实施。

4.3.9. 服务合同要求

a) 了解客户及所处的行业对信息安全服务的特定要求。

b) 确定信息安全服务范围。

c) 应签订信息安全服务合同或协议。

d) 合同应明确信息安全服务的行为规范。

e) 合同应明确信息安全服务的安全要求。

4.3.10. 服务安全要求

a） 满足法律法规对服务安全的要求。

b） 满足与客户签订服务合同中的安全要求。

c） 制定保密管理制度，明确岗位保密责任。

d) 按照客户要求，对于接触到的客户敏感信息和知识产权信息予以保护，并确保服务方人员了解客户的相关要求。

e) 与相关人员签订保密协议，并进行保密教育。

f) 确保其供应商满足上述服务安全要求。

4.3.11. 服务技术要求

a) 建立信息安全服务（与申报类别一致）流程。

b) 制定信息安全服务（与申报类别一致）规范，并按照规范实施。

5. 专业评价要求

5.1. 风险评估服务资质专业评价要求

风险评估服务资质专业评价要求参见附录A。

5.2. 安全集成服务资质专业评价要求

安全集成服务资质专业评价要求参见附录 B。

5.3. 应急处理服务资质专业评价要求

应急处理服务资质专业评价要求参见附录C。

5.4. 灾难备份与恢复服务资质专业评价要求

灾难备份与恢复服务资质专业评价要求参见附录D。

5.5. 软件安全开发服务资质专业评价要求

软件安全开发服务资质专业评价要求参见附录E。

5.6. 安全运维服务资质专业评价要求

安全运维服务资质专业评价要求参见附录F。

6. 认证程序

6.1. 自评估

组织在中国信息安全认证中心网站下载《信息安全服务自评估表》，并实施自主评估。

6.2. 认证申请

组织依据信息安全服务资质认证程序、认证实施规则中相关要求，确定申请服务资质类别，并填写《信息安全服务资质认证申请书》。

组织向中国信息安全认证中心或其指定机构提交《信息安全服务资质认证申请书》、《信息安全服务自评估表》及相关证明材料。

6.3. 申请材料评审

中心依据认证程序和相关标准要求，对申请组织提交的认证相关材料进行评审，并确定申报级别和资质类别，签订认证合同。

6.4. 现场评审

认证机构组成评审组，依据相关标准和评审要求，到申请组织现场进行评审，并出具现场评审报告。特别，对申请一级资质认证的组织，必要时选择申请组织的客户进行项目实施现场见证。

6.5. 认证决定

认证决定委员会由3名以上（含3名）奇数认证决定人员组成，做出认证决定。

6.6. 证书颁发

对于符合认证要求的申请组织，颁发认证证书，并予以公示。

6.7. 证后监督

6.7.1. 证后监督频次和方式

对获证组织实施监督，每年度（不超过12个月）进行一次监督评审。

当获证组织发生重大变更、事故或客户投诉时，可增加现场监督评审的频次。

6.7.2. 证后监督内容

监督评审除包括初次评审的内容外，还应对上一次审核中提出的观察项所采取纠正/预防措施进行验证。还应包括获证企业变更情况、对其投诉处理情况，以及认证证书及认证标识的使用情况等。

6.7.3. 证后监督结论

对于通过监督评审的获证组织，做出维持认证证书有效的决定；否则，暂停或撤销其认证证书。

6.7.4. 信息通报

为确保获证组织的安全服务能力持续有效，获证组织应建立信息通报渠道，及时报告以下信息：

a) 组织机构变更信息；

b) 安全事故、客户投诉信息；

c) 其他重要信息。

6.8. 认证证书管理

6.8.1. 证书有效期

获证组织如持续满足标准要求，且通过年度监督评审，可保持证书有效。

6.8.2. 暂停认证证书

获证组织有下列情形之一，认证机构应暂停其认证证书：

a) 未按规定接受监督评审；

b) 违规使用认证证书，且未造成不良影响；

c） 监督评审有严重不符合项；

d） 其他需要暂停证书的情况。

证书暂停时间一般为三个月。在证书暂停期间，组织可提出恢复证书的申请，并经认证机构审核、批准后方可使用证书。

6.8.3. 撤销认证证书

获证组织有下列情形之一，应撤销其认证证书：

a） 证书暂停期间，未在规定时间内完成整改并通过验证；

b） 违规使用认证证书，造成不良影响；

c） 获证组织出现严重责任事故、被投诉且经核实，影响其继续有效提供服务；

d） 其他需要撤销证书的情况。

认证证书撤销后，获证组织应交回认证证书，中心予以公示。

6.8.4. 注销认证证书

获证组织因自身原因不再维持证书，可提出注销认证证书的申请，中心应及时给予注销。

认证证书注销后，获证组织应交回认证证书，中心予以公示。

6.8.5. 证书变更

证书变更如只涉及地址、资金或法定代表人的变更，获证组织需递交变更申请，经书面审核批准后，中心可更换其证书并收回原证书。

如获证组织发生除以上外的重大调整，应向中心提出变更申请，并提供相关材料。

中心需进行现场验证，并做出认证决定。

附录 A（规范性附录）： 信息安全风险评估服务资质专业评价要求

信息安全风险评估服务资质专业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，至少有一个完成的风险评估项目，该系统的用户数在1,000以上；具备从管理或（和）技术层面对脆弱性进行识别的能力。

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。

d) 对项目采取文档化管理。

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。

A2.2.3威胁识别

a) 应参考国家或国际标准，对威胁进行分类。

b) 应识别对已识别的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。

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) 应根据分析模型确定的方法计算出风险值。

A1.3.2风险评价

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。

b) 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，除满足三级资质的所有条件外，还需满足以下要求：

申请二级资质认证的单位，针对多种类型组织，多行业组织，至少完成一个风险评估项目，该系统的用户数在10,000以上；具备从管理和技术层面对脆弱性进行识别的能力。

A2.1准备阶段

根据评估目标和范围，确定风险评估对象中包含的信息系统，以及对组织的资产进行分类。

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；

b) 建立项目管理规程，对项目按规程进行管理。

A2.2风险识别阶段

A2.2.1威胁识别

a) 依据相关标准中的威胁分类方法对威胁进行分类。

b) 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风险分析模型建立

a) 构建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) 资产价值应依据资产在保密性、完整性和可用性上的赋值等级，经过综合评定得出。

A2.3.2风险计算方法确定

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。

A2.3.3风险评价

a) 应根据风险评价准则确定风险等级。

b) 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。

A2.3.4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

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

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，除满足二级资质的所有条件外，还需满足以下要求：

申请一级资质认证的单位，能够在全国范围内，针对5个（含）以上行业开展风险评估服务；至少完成两个风险评估项目，该系统的用户数在100,000以上；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以及工具自身的安全性、适用性；

b) 建立项目管理规程，对项目按规程进行管理；必要时，采取项目群、项目组合管理。

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应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

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专业评价要求

信息系统安全集成服务资质专业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，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。

B1.1.2 签订服务协议

a) 与客户、供应商签订服务协议，明确范围、目标、时间、内容、金额、质量和输出等。

b) 与客户、供应商等相关方签订保密协议，明确保密职责和违约责任。

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，试运行周期至少一个月。

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。

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保密性、完整性、可用性、可靠性等方面的安全需求，提出系统安全保障策略和建议。

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。

d) 依据技术方案具体指标要求，制定系统测试计划。

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。

B2.3.2 监督管理

建立客户满意度调查机制，并对调查结果进行分析。

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

试运行结束后，项目组制定系统试运行报告，并提交客户。

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

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。

B3.1.2 签订服务协议

建立安全集成服务级别管理程序，签订服务级别协议。

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

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

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) 提供三个月以上的试运行记录和报告。

附录 C（规范性附录）： 信息安全应急处理服务资质专业评价要求

信息安全应急处理服务资质专业评价要求针对准备、检测、抑制、根除、恢复、总结六个过程进行，具体分级要求如下：

C1 三级要求

C1.1 准备阶段

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 2 小时应急响应服务能力。

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) 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》）

C1.2 检测阶段

a) 确定检测对象及范围，并得到客户的授权。

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) 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) 协助客户按照系统的初始化安全策略恢复系统。

d) 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) 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。

C1.6 总结阶段

a) 及时检查网络或信息安全事件处理记录是否齐全，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。

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) 向客户提供规范化应急处理服务流程。

e) 可提供本地 1 小时、外地 8 小时应急响应服务能力。

f) 配备有处理网络与信息安全事件的工具包，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。

h) 具有处理较大信息安全事件的能力。

C2.2 检测阶段

a) 检测对象及范围应得到客户的书面授权。

b) 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。

c) 协助客户确定安全事件等级。

d) 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。

e) 应急处理方案应包含实施方案失败的应变和回退措施。

C2.3 抑制阶段

a) 在采取抑制措施之前与客户充分沟通，告知可能存在的风险，制定应变和回退措施，并与其达成协议。

b) 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。

C2.4 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) 明确告知客户所采取的根除措施可能带来的风险，制定应变和回退措施，并获得客户的书面授权。

c) 找出导致网络与信息安全事件发生的原因，并予以彻底消除。

C2.5 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) 帮助客户为重建后的系统建立系统快照。

C2.6 总结阶段

a) 及时检查网络与信息安全事件处理记录是否齐全，是否具备可追溯性，并对事件处理过程进行总结和分析。

b) 提供详实的网络与信息安全事件处理报告。

c) 提供网络与信息安全方面的建议和意见，必要时指导和协助客户实施。

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 7*24 小时、外地 4 小时应急响应服务能力。

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。

e) 具有处理重大及特别重大信息安全事件的能力。

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。

e) 保留可能用于司法程序的相关证据信息。

C3.3 抑制阶段

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

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

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) 提供详实的网络与信息安全事件处理报告，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）： 信息系统灾难备份与恢复服务资质专业评价要求

信息系统灾难备份与恢复服务分为两类，即提供灾难备份与恢复资源服务为资源服务类（A类），提供灾难备份与恢复系统设计、实施为技术服务类（B类），其专业评价要求分别如下：

D1资源服务类（A类）要求

D1.1 三级要求

D1.1.1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) 用于和可用于灾备中心IT运行区的高架地板面积不少于1000平米。

c) 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。

d) 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。

e) 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。

f) 灾备中心建筑耐火等级达到二级及以上。

D1.1.2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。

D1.1.3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) 建立信息系统灾难恢复指挥系统，保障灾难恢复效率。

d) 建立灾备中心与生产中心统一变更流程。

e) 定期开展数据验证工作，确保生产与灾备的数据一致性、完整性和可用性。

D1.2 二级要求

组织申报二级资质，除满足三级要求外，还应满足以下要求：

D1.2.1灾备中心场地资源要求

a) 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。

b) 用于和可用于灾备中心IT运行区的高架地板面积不少于2000平米。

c) 灾备中心建设等级满足国标A级或国际T3以上机房要求。

d) 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。

D1.2.2灾备中心基础设施要求

a) 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。

b) 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。

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

D1.2.3灾备中心运维管理要求

a) 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。

b) 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。

c) 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。

d) 妥善保管运维记录，所有文档应满足客户监管机构要求。

e) 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。

D1.3一级要求

组织申报一级资质，除满足二级要求外，还应满足以下要求：

D1.3.1灾备中心场地资源要求

a) 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。

b) 用于灾备中心的场地应自有产权,或者签署有剩余期限不少于5年的长期租赁合同。

c) 用于和可用于灾备中心IT运行区的高架地板面积不低于5000平米。

d) 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。

e) 至少采用园区保安、机房门卫、前台三重审核的外部保安措施。

f) 灾备中心的所有通道、机房内均设置 CCTV 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。

g) 灾备中心建筑耐火等级达到一级。

D1.3.2灾备中心基础设施要求

a) 高压电来自两个独立的变电站的双路设计。

b) 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协议，保障燃料数量和质量要求，UPS和油机可自动切换。

D1.3.3灾备中心运维管理要求

a) 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。

b) 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。

c) 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。

d) 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。

e) 建立灾备中心应急管理体系，确保灾备系统稳定运行。

D2技术服务类（B类）要求

D2.1 三级要求

D2.1.1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。

D2.1.2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。

D2.1.3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。

D2.2 二级要求

组织申报二级资质，除满足三级要求外，还应满足以下要求：

D2.2.1方案设计要求

a) 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。

b) 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）。

c) 依据系统建设要求和技术方案，制定系统测试方案。

D2.2.2系统建设与管理要求

a) 依据测试方案，组织实施系统测试，并详细记录。

b) 制定灾难备份与恢复系统试运行方案，并详细试运行过程情况。

D2.2.3预案制定与演练要求

a) 制定系统演练方案，明确演练范围、人员、场景、步骤等内容。

b) 组织演练培训和动员，明确参演人员角色、职责和具体任务。

c) 设计多种演练场景并组织推演，详细记录演练过程。

D2.3一级要求

组织申报一级资质，除满足二级要求外，还应满足以下要求：

D2.3.1方案设计要求

a) 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。

b) 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。

D2.3.2系统建设与管理要求

a) 建立系统运行维护管理制度，实时监控灾难备份中心运行状况，及时响应和处理异常情况，分析异常产生的原因，并依据流程升级和上报。

b) 建立存储介质和数据管理制度，规范数据传输和复制过程，定期检查和验证存储介质和数据。

D2.3.3预案制定与演练要求

a) 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。

b) 基于特定的演练场景，制定详细的切换演练方案。

c) 组织完成真实切换演练前的桌面推演和模拟测试工作。

d) 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 E（规范性附录）： 软件安全开发服务资质专业评价要求

软件安全开发服务资质专业评价要求针对准备、需求、设计、编码、测试、验收和维保七个阶段进行，具体分级要求如下：

E1 三级要求

E1.1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。

E1.2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、性能及安全性要求。

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。

E1.3设计阶段

a) 根据软件项目需求，编制软件设计方案、设计说明书。

b) 软件设计方案明确系统/子系统的功能和非功能设计要求。

c) 软件设计方案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。

E1.4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。

E1.5测试阶段

a) 依据软件设计方案、设计说明书对软件功能、安全功能进行测试。

b) 对测试过程中发现的漏洞进行分析并有效修复。

E1.6验收阶段

E1.6.1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，试运行周期至少一个月。

b) 基于系统试运行相关记录，及时对软件进行调整、维护。

E1.6.2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。

E1.7维保阶段

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。

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。

E2.2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) 基于客户需求和投入能力，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。

E2.3设计阶段

E2.3.1概要设计

概要设计方案明确安全功能要求，还应包括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。

E2.3.2详细设计

详细设计说明书中包含对数据产生、传输、存储、使用、处理和归档安全性的详细设计。

E2.4编码阶段

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，且形成记录。

E2.5测试阶段

E2.5.1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。

E2.5.2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。

c) 对安全子系统进行兼容性和安全性测试，完整记录测试过程相关信息。

E2.5.3系统测试

a) 制定针对系统安全性测试在内的测试计划和测试设计，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) 提供系统测试报告和安全方面分析报告。

E2.6验收阶段

E2.6.1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。

E2.6.2验收交付

提交软件安全评析报告。

E2.7维保阶段

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

b) 及时应对突发事件，并向用户提供故障事件解决报告。

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。

E3.2需求阶段

a) 基于软件安全威胁，开展需求分析，编制具有软件安全需求的分析报告。

b) 基于软件项目需求分析，结合安全开发要素建立软件开发模型。

E3.3设计阶段

E3.3.1概要设计

a) 设计方案中明确基于软件安全威胁分析的安全要求。

b) 设计方案中明确安全功能要求，还应包括抗抵赖、安全标记、可信路径等。

E3.3.2详细设计

依据安全要求和设计方案，明确基于软件安全威胁分析的详细设计。

E3.4编码阶段

采用代码检查工具实施安全审查。

E3.5测试阶段

E3.5.1单元测试

对单元测试结果进行分析，形成分析报告。

E3.5.2集成测试

对集成测试结果进行分析，形成分析报告。

E3.5.3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。

E3.6验收阶段

E3.6.1系统试运行

a) 提供三个月以上的试运行记录和报告。

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。

E3.6.2验收交付

提交软件产品最终安全评析报告。

E3.7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 F（规范性附录）：安全运维服务资质专业评价要求

安全运维服务资质专业评价要求针对服务准备、服务实施、监视评审、持续改进四个阶段进行，具体分级要求如下：

F1 三级要求

F1.1准备阶段

F1.1.1需求调研与分析

a) 采集客户对信息系统运维服务时间的需求。

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。

F1.1.2运维服务设计

a) 制定安全运维服务目录，包括但不限于：初始服务、安全设备运维、日常巡检服务、健康检查、安全事件审计。

b) 对信息系统相关的IT资产进行识别。

c) 对安全设备进行日常维护及监控，并记录硬件故障。

d) 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。

e) 采集系统配置、流量信息、系统状态等安全信息。

f) 收集与分析网络及安全设备、服务器、操作系统、网络应用的日志。

F1.1.3运维服务导入

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。

b) 专业人员负责安全管理的接口。

c) 建立服务目录。

d) 建立事件响应和解决的机制，有基本的安全运维报告模式。

F1.1.4明确服务协议特殊要求

a) 明确安全事件处理与应急响应流程，包括但不限于：安全事件的分类、安全事件上报流程、安全事件处理流程、安全事件的事后处理。

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

F1.2运维服务实施阶段

a) 实施初始服务：完成资产识别，定期配置项的更新和维护，实施相关运维流程。

b) 实施安全设备运维服务：完成日常维护，状态检查，定期查杀，故障处理、保养、更新、升级、故障检测及排除，并对安全设备出现的硬件故障进行统计记录。

c) 实施日常巡检服务：完成安全设备监控；病毒监测、查杀及网络防病毒维护，并有相关记录。

d) 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。

e) 实施安全事件审计服务：完成网络及安全设备日志、服务器、操作系统、网络应用的日志、并且进行记录。

f) 组建运维服务台职能，培养服务台人员的专业能力。

g) 建立事件管理程序和信息安全服务请求管理程序。

F1.3运维监视评审阶段

a) 应定期收集与分析安全运维报告的数据，包括但不限于：异常报告及时率、异常漏报率、维护作业计划的及时完成率、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。

b) 对运维实现情况进行监视测量，未能实现的目标应采取纠正预防措施。

c) 建立与分析客户满意度调查。

F1.4运维持续改进阶段

a) 应在运维过程和监视过程中识别改进项目，制定持续改进计划，包括但不限于对改进机会的评估标准。

b) 应有文件化的程序，用以识别、记录、批准、评估、测量和报告改进措施。

c) 应采取预防措施，以消除潜在的不符合项的原因，以防止其发生。

F2 二级要求

组织申报二级资质，除满足三级资质的所有条件外，还需满足以下要求。

F2.1运维服务准备阶段

F2.1.1需求调研与分析

a) 根据评估目标和范围，对安全运维对象中包含的信息系统，组织的资产进行分类。

b) 识别与分析信息系统运维过程中的历史数据，提出系统运维的保障策略和解决方案。

c) 分析客户对信息系统安全服务的需求和类型。

d) 收集与分析信息系统的可用性指标，明确可用性指标的类型。

e) 分析以往服务的数据，提取出来未来可自动化的服务。

F2.1.2运维服务设计

a) 对信息安全事件进行统计与分析；

b) 编写安全运维服务目录，包括但不限于：运维监控与分析、终端安全监控、合规性运维。

c) 建立信息系统安全运维的问题管理程序。

d) 建立知识管理程序及初步形成知识库。

e) 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。

f) 形成信息安全管理的组织架构，组织结构的构成要素与安全运维活动角色相对应。

F2.1.3运维服务导入

采用流程化管理方法，基于安全事件处理流程、安全培训服务流程、渗透测试流程进行标准化的信息系统安全运维工作。

F2.1.4明确服务协议特殊要求

a) 建立信息系统安全主动管理机制；

b) 签订信息系统安全运维服务级别协议，承诺信息系统核心指标。

c) 建立问题管理程序。

d) 建立信息系统安全的配置库及关联关系信息。

F2.2运维服务实施阶段

a) 实施运维监控与分析并形成记录。

b) 进行合规性运维。

F2.3运维监视评审阶段

F2.3.1内审

按照计划的时间间隔执行内部审核，满足既定标准要求、安全运维服务需求和客户所提出的SMS要求，并有效实施和维护。

F2.3.2管理评审

a) 定期回顾安全运维服务，确保其持续适用和有效。

b) 管理评审输入至少包括但不限于：客户反馈、服务和流程的执行情况和符合性、当前和预测资源水平、纠正措施的进展情况、可能影响安全运维服务的变更、改进机会。

F2.4运维持续改进阶段

a) 改进机会应划分优先级，策划被批准的改进机会。

b) 改进活动应进行管理，包括但不限于：设定改进目标、确保批准的改进活动被实施、报告被实施的改进计划。

F3一级要求

组织申报一级资质，除满足二级资质的所有条件外，还需满足以下要求。

F3.1运维服务准备阶段

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；在采用外包模式的情况下，执行组还应包含安全运维服务供应商参与运维的人员。

c) 采用基于PDCA的管理模型，从策划，实施，监视与评审和持续改进进行体系化的信息系统安全运维服务。

d) 建立安全运维可视化视图。

F3.1.1需求调研与分析

a) 基于信息系统安全的生命周期，建立信息系统安全运维的整体策略。

b) 基于客户、业务的价值体现，形成安全运维的整体视图。

F3.1.2运维服务设计

a) 编制安全运维项目作业指导书。

b) 建设实施过程中应关注信息系统的功能、性能和安全性方面要求。

c) 改造过程中应制定测试计划及回退措施。

d) 编写安全运维服务目录，包括但不限于：安全通告及漏洞分析、应急响应服务。

F3.1.3运维服务导入

a) 基于渗透测试流程管理进行标准化的信息系统安全运维工作。

b) 编制信息安全产品和工具定制开发计划。

F3.1.4明确服务协议的特殊要求

a) 建立信息系统安全运维服务级别管理程序，签订服务级别协议。

b) 建立信息系统应急事件响应机制和恢复保障。

c) 对客户满意度进行趋势分析。

d) 建立应急响应和灾难恢复机制，形成业务连续性计划。

F3.2运维服务实施阶段

a) 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

b) 实施应急响应服务：制定应急响应预案，对应急事件及时响应，并对应急进行演练，形成相关记录

c) 建立运维变更管理程序，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。

d) 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。

F3.3运维监视评审阶段

a) 形成体系化的审核机制及企业文化。

b) 体系化的服务监视管理，形成审核机制。

c) 定期评审客户对安全运维服务的满意度。

F3.4运维持续改进阶段

a) 持续服务改进，形成持续服务改进文化和意识。

b) 基于运维服务的缺陷，提出改进策略和方案。

c) 分析运维服务的数据并进行服务预测。

附录 G: 参考文献

[1] GB/T 20261-2006 信息技术 系统安全工程 能力成熟度模型

[2] YD/T 1621-2007 网络与信息安全服务资质评价准则

[3] YD/T 2252-2011 网络与信息安全风险评估服务能力评价方法

[4] RB/T 201-2013 信息系统安全集成服务资质认证评价要求

[5] CNCA/CTS 0052-2007 信息安全服务资质认证技术规范

[6] 《计算机信息系统集成企业资质等级评定条件》（2012年修定版）

[7] 《通信信息网络系统集成企业资质认定》

[8] 《安防工程企业资质评定标准》中安协资[2007] 2号

[9] 《建筑智能化工程专业承包企业资质等级标准》