ICS 35.240
L 60

团　　体　　标　　准

T/BJCSA 02-2022

网络空间安全服务规范

Specification for cyberspace security services

2022-3-18 发布　　2022-3-20 实施

北京网络空间安全协会
广东省网络空间安全协会　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。

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。

本文件由网安联认证中心有限公司提出。

本文件由北京网络空间安全协会和广东省网络空间安全协会归口。

本文件起草单位：网安联认证中心有限公司、湖南省网络空间安全协会、陕西省信息网络安全协会、武汉市网络安全协会、广东关键信息基础设施保护中心、国源天顺科技产业集团有限公司、广州华南信息安全测评中心、南方电网数字电网研究院有限公司、广东省科技基础条件平台中心、联通（广东）产业互联网有限公司、北京天融信网络安全技术有限公司四川分公司、广州百蕴启辰科技有限公司、广东广信通信服务有限公司、成都深思天地计算机技术有限公司、广州市盛通建设工程质量检测有限公司、福建省网络与信息安全测评中心、广东机电职业技术学院、骏捷（广东）科技有限公司。

本文件起草人：成珍苑、黄志强、张华兵、熊璐、伍阳军、姚灏、林勇忠、刘悦恒、刘纯纯、高松涛、利传杰、李美芹、林小博、王辉、王巧巧、周世刚、曹强、钟承峰、朱灿阳、陈宁、王卫亚、唐锦奎、吴隶妍、吴星火、钟英南、张东、常磊、刘智强、王福、郑明亮、谢光骥。

本文件首次修订。

引　言

伴随信息革命的飞速发展，互联网、通信网、计算机系统、自动化控制系统、数字设备及其承载的应用、服务和数据等组成的网络空间，正在全面改变人们的生产生活方式，深刻影响人类社会历史发展进程，网络空间已经成为与陆地、海洋、天空、太空同等重要的人类活动新领域，国家主权拓展延伸到网络空间，网络空间主权成为国家主权的重要组成部分。网络在给我们带来发展和生活便利的同时，网络安全问题也日益凸显，网络违法犯罪、网络治安乱象、网络安全隐患等严重威胁网络空间安全，国家政治、经济、文化、社会、国防安全及公民在网络空间的合法权益面临严峻风险与挑战。网络空间安全已经上升到国家战略高度。如何确保信息网络的设施安全、运行安全和数据安全，备受社会各方关注。《中华人民共和国网络安全法》、《数据安全法》、《个人信息保护法》正式实施，对如何强化网络安全管理、提高网络产品和服务的安全可控水平等提出了明确的要求。在此环境下，众多为网络安全建设、安全运维、数据安全可用提供技术性服务的机构应运而生、发展迅猛，已经形成规模庞大的网络安全服务产业。这些服务机构的技术能力、工作规范及管理水平，直接影响着我国信息网络的安全。

制定本规范，按照标准要求实施网络安全服务机构等级认证，客观公正地评价服务机构的服务能力，有利于规范市场秩序、杜绝不良企业涉足网络安全行业，促进网络安全服务行业的健康发展，切实保护我国的网络安全。

网络空间安全服务规范

1 范围

本文件规定了网络空间安全服务机构（以下简称“服务机构”）应具备的基本资格、基本能力和专业能力要求。

本文件适用于服务机构开展服务能力评价，可作为第三方认证机构对服务机构进行基本资格、基本能力和专业能力评价的依据，为用户在维护网络安全工作中选择服务机构提供参考。

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 30279-2020 信息安全技术 网络安全漏洞分类分级指南

3 术语和定义

下列术语和定义适用于本文件。

3.1

网络空间安全服务 cyberspace security service

在网络空间开展的安全咨询、安全集成、软件安全开发、安全运维、监测预警、应急响应、渗透测试、风险评估、安全审计、数据安全、工业控制系统安全、云计算安全等安全服务。

3.2

网络空间安全服务机构 cyberspace security service institution

按照合同或协议的约定提供网络空间安全服务的组织，通常称为网络安全服务提供商。

3.3

网络空间安全服务机构等级 cyberspace security service institution grade

按照从业时间、机构资信、财务资信、制度及流程、人员状况、技术能力、专业能力等要求对网络空间安全服务机构进行水平评价和服务等级划分。

4 网络空间安全服务类型

4.1 安全咨询

服务机构通过知识传递、工作辅导和系统规划等提供的咨询服务，主要包括安全规划、安全设计、信息安全管理体系、业务连续性管理、数据安全管理、个人信息保护管理等咨询服务。

4.2 安全集成

服务机构在网络空间信息系统集成过程中，提供的安全需求界定、设计、实施、保障等网络安全服务。

4.3 软件安全开发

服务机构在网络空间信息系统软件开发过程中，提供的安全需求分析、安全设计、安全编码、安全测试等提高软件安全质量的服务。

4.4 安全运维

服务机构在网络空间信息系统运维过程中，提供的安全巡检、安全加固、病毒查杀、备份和恢复、安全优化等安全服务，协助服务对象提高信息系统保障防护能力。

4.5 监测预警

服务机构在网络空间信息系统保障工作中，提供的恶意代码和攻击监测、安全态势感知和安全通报等安全服务，协助服务对象及时发现网络安全风险并进行持续跟踪、分析、预警和上报。

4.6 应急响应

服务机构在网络空间信息系统保障工作中，提供的应急响应预案编制、演练测试、应急处置、系统恢复等安全服务，最大程度减少事件造成的影响和损失，协助服务对象提高应对各类突发事件的能力。

4.7 渗透测试

服务机构在网络空间信息系统保障工作中，通过模拟网络安全攻击，进行非破坏性测试，发现安全漏洞、隐患及攻击路径，将入侵过程和漏洞细节报告服务对象，提出详细、合理的修复建议，指导其进行整改、清除安全隐患、降低安全风险，为服务对象信息系统的平稳运行提供安全保障。

4.8 风险评估

服务机构在网络空间信息系统保障工作中，对信息系统的资产价值、潜在威胁、薄弱环节、已采取的防护措施等进行分析，判断安全事件发生的概率以及可能造成的损失，提出风险管理措施的服务，协助服务对象增强网络安全风险管控。

4.9 安全审计

服务机构在网络空间信息系统保障工作中，通过收集和分析审计证据，检查和促进服务对象信息系统及其内部控制的真实性、正确性、完整性、安全性和可靠性等要素，协助服务对象符合国家法律法规要求，确保系统稳定、可靠、安全运行。

4.10 数据安全

服务机构在网络空间信息系统保障工作中，通过采取必要措施，提供数据收集、存储、使用、加工、传输、提供、公开等数据处理全过程安全服务，协助服务对象确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

4.11 工业控制系统安全

服务机构在网络空间工业控制系统保障工作中，提供系统调研、安全评估、安全设计、安全加固、体系建设等服务，协助服务对象保障工业控制系统连续正常运行。

4.12 云计算安全

服务机构在网络空间云计算保障工作中，提供基础设施安全保障、虚拟化和容器安全、应用安全、数据保护等服务，协助服务对象符合法律法规规定，确保云计算系统可靠稳定运行。

5 服务机构等级划分

网络空间安全服务规范包含通用评价要求和专业能力评价要求。通用评价要求包含基本资格、基本能力，如机构资信、财务资信、人员状况、办公场所、从业时间、经营业绩、管理制度、合同管理、保密管理、专业工具等，具体要求见第6章。不同方向的专业能力要求各不相同，各方向具体要求见附录A-L。依据服务机构的基本资格、基本能力和专业能力分为一级、二级、三级、四级，其中四级最高，一级最低。

6 通用评价要求

6.1 一级要求

6.1.1 机构资信

具有中华人民共和国境内注册的独立法人资格，产权关系明确，具有相应的经营范围。

6.1.2 财务资信

有健全的财务管理制度，财务数据真实可信。

6.1.3 办公场所

具有固定的办公场所和相应的办公条件，能够满足机构设置及其业务需要。

6.1.4 人员能力

一级服务机构人员能力要求如下：

a) 机构负责人应拥有1年以上信息技术领域管理经历；
b) 技术负责人应从事网络空间安全技术工作1年以上；
c) 有网络空间安全技术服务人员5名以上，其中应有与申报类别一致的网络空间安全专业人员认证证书2名以上。

6.1.5 从业时间

首次申请不做要求。

6.1.6 经营业绩

首次申请不做要求，维持资格最少完成一个1个与申报类别一致的网络空间安全服务项目。

6.1.7 管理要求

一级服务机构管理要求如下：

a) 建立人力资源管理制度，明确安全服务人员的岗位职责、技术能力要求，并通过评价证明其能够胜任其承担的职责；
b) 建立服务人员培训管理制度，包括网络空间安全相关的技术、管理、意识等内容，并有效落实，确保服务人员持续胜任其承担的职责；

c) 建立文档管理制度，明确文档管理职责，并能有效控制文档产生、发布、保存、传输、使用、废弃等；
d) 建立项目管理制度，明确服务项目的组织、计划、实施、交付等环节的操作规程；
e) 建立供应商管理制度，确保其供应商满足服务安全要求（仅适用于安全集成、安全运维）。

6.1.8 保密管理

建立保密管理制度，明确岗位保密责任，签订保密协议，并能够适时对相关人员进行保密教育。

6.1.9 合同管理

一级服务机构合同管理要求如下：
a) 建立合同管理制度；
b) 合同内容应具有明确的服务范围，服务内容和方法，符合网络安全法律法规要求，应具有保护客户的敏感信息和知识产权条款。

6.2 二级要求

6.2.1 机构资信

具有中华人民共和国境内注册的独立法人资格，产权关系明确，具有相应的经营范围。

6.2.2 财务资信

有健全的财务管理制度，财务数据真实可信，近1年经营状况良好。

6.2.3 办公场所

具有固定的办公场所和相应的办公条件，能够满足机构设置及其业务需要。

6.2.4 人员能力

二级服务机构人员能力要求如下：
a) 机构负责人应拥有2年以上信息技术领域管理经历；
b) 技术负责人应从事网络空间安全技术工作2年以上；
c) 有网络空间安全技术服务人员8名以上，其中应有与申报类别一致的网络空间安全专业人员认证证书3名以上。

6.2.5 从业时间

从事与申报类别一致的网络空间安全服务1年以上。

6.2.6 经营业绩

近三年内应签订并完成至少2个与申报类别一致的网络空间安全服务项目。维持资格最少完成一个1个与申报类别一致的网络空间安全服务项目。

6.2.7 管理要求

二级服务机构管理要求如下：
a) 建立人力资源管理制度，明确安全服务人员的岗位职责、技术能力要求，并通过评价证明其能够胜任其承担的职责；
b) 建立服务人员培训管理制度，包括网络空间安全相关的技术、管理、意识等内容，并有效落

实，确保服务人员持续胜任其承担的职责；

c） 建立文档管理制度，明确文档管理职责，并能有效控制文档产生、发布、保存、传输、使用、废弃等；

d） 建立项目管理制度，明确服务项目的组织、计划、实施、交付等环节的操作规程；

e） 建立供应商管理制度，确保其供应商满足服务安全要求（仅适用于安全集成、安全运维）。

6.2.8 保密管理

建立保密管理制度，明确岗位保密责任，签订保密协议，并能够适时对相关人员进行保密教育。

6.2.9 合同管理

二级服务机构合同管理要求如下：

a） 建立合同管理制度；

b） 合同内容应具有明确的服务范围，服务内容和方法，符合网络安全法律法规要求，应具有保护客户的敏感信息和知识产权条款；

c） 具有健全的合同评审程序。

6.3 三级要求

6.3.1 机构资信

具有中华人民共和国境内注册的独立法人资格，产权关系明确，具有相应的经营范围。

6.3.2 财务资信

有健全的财务管理制度，财务数据真实可信，近3年经营状况良好。

6.3.3 办公场所

具有固定的办公场所和相应的办公条件，能够满足机构设置及其业务需要。

6.3.4 人员能力

三级服务机构人员能力要求如下：

a） 机构负责人应拥有3年以上信息技术领域管理经历；

b） 技术负责人应从事网络空间安全技术工作3年以上；

c） 有网络空间安全技术服务人员20名以上，其中应有与申报类别一致的网络空间安全专业人员认证证书8名以上。

6.3.5 从业时间

从事与申报类别一致的网络空间安全服务3年以上，或取得网络空间安全服务资质2级满1年以上。

6.3.6 经营业绩

近三年内应签订并完成至少6个与申报类别一致的网络空间安全服务项目。维持资格最少完成一个1个与申报类别一致的网络空间安全服务项目。

6.3.7 管理要求

三级服务机构管理要求如下：

a） 建立人力资源管理制度，明确安全服务人员的岗位职责、技术能力要求，并通过评价证明其

能够胜任其承担的职责；

b) 建立服务人员培训管理制度，包括网络空间安全相关的技术、管理、意识等内容，并有效落实，确保服务人员持续胜任其承担的职责；

c) 建立文档管理制度，明确文档管理职责，并能有效控制文档产生、发布、保存、传输、使用、废弃等，应配备专门的档案室及高安全性的文件服务器；

d) 建立项目管理制度，明确服务项目的组织、计划、实施、风险控制、交付等环节的操作规程，能有效跟踪和控制项目风险；

e) 建立供应商管理制度，明确供应商或外包过程中的风险，对供应商或承包方的服务基本资格、服务过程控制、服务质量、服务交付等进行识别，确保其供应商或承包方满足服务安全要求（仅适用于安全集成、安全运维）。

6.3.8 保密管理

建立保密管理制度，明确岗位保密责任，签订保密协议，并能够适时对相关人员进行保密教育。

6.3.9 合同管理

三级服务机构合同管理要求如下：

a) 建立合同管理制度；

b) 合同内容应具有明确的服务范围，服务内容和方法，符合网络安全法律法规要求，应具有保护客户的敏感信息和知识产权条款；

c) 具有健全的合同评审程序。

6.3.10 专业工具

三级服务机构专业工具要求如下：

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) 具备承担与申报类别一致的网络安全服务项目所需的安全工具，并对工具进行管理和版本控制。

6.4 四级要求

6.4.1 机构资信

具有中华人民共和国境内注册的独立法人资格，产权关系明确，具有相应的经营范围。

6.4.2 财务资信

有健全的财务管理制度，财务数据真实可信，近3年经营状况良好。

6.4.3 办公场所

具有固定的办公场所和相应的办公条件，能够满足机构设置及其业务需要。

6.4.4 人员能力

四级服务机构人员能力要求如下：

a) 机构负责人应拥有5年以上（含5年）信息网络技术领域管理经历；

b) 技术负责人应从事网络空间安全技术工作5年以上；

c) 有网络空间安全技术服务人员30名以上，其中拥有与申报类别一致的网络空间安全专业人员

认证证书12名以上。

6.4.5 从业时间

从事与申报类别一致的网络空间安全服务5年以上，或取得网络空间安全服务资质3级满1年以上。

6.4.6 经营业绩

近三年内应签订并完成至少10个与申报类别一致的网络空间安全服务项目。维持资格最少完成一个1个与申报类别一致的网络空间安全服务项目。

6.4.7 管理要求

四级服务机构管理要求如下：

a) 建立人力资源管理制度，明确安全服务人员的岗位职责、技术能力要求，并通过评价证明其能够胜任其承担的职责；
b) 应建立服务人员培训管理制度，包括网络空间安全相关的技术、管理、意识等内容，并有效落实，确保服务人员持续胜任其承担的职责；
c) 建立文档管理制度，明确文档管理职责，并能有效控制文档产生、发布、保存、传输、使用、废弃等，应配备专门的档案室及高安全性的文件服务器；
d) 建立项目管理制度，明确服务项目的组织、计划、实施、风险控制、交付等环节的操作规程，能有效跟踪和控制项目风险；
e) 建立供应商管理制度，明确供应商或外包过程中的风险，对供应商或承包方的服务基本资格、服务过程控制、服务质量、服务交付等进行识别，确保其供应商或承包方满足服务安全要求（仅适用于安全集成、安全运维）；
f) 参照国际或国内标准，建立覆盖信息网络安全服务的质量管理体系并有效运行一年以上；
g) 参照国际或国内标准，建立信息安全管理体系并有效运行一年以上。

6.4.8 保密管理

建立保密管理制度，明确岗位保密责任，签订保密协议，并能够适时对相关人员进行保密教育。

6.4.9 合同管理

四级服务机构合同管理要求如下：

a) 建立合同管理制度；
b) 合同内容应具有明确的服务范围，服务内容和方法，符合网络安全法律法规要求，应具有保护客户的敏感信息和知识产权条款；
c) 具有健全的合同评审程序。

6.4.10 专业工具

四级服务机构专业工具要求如下：

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) 具备承担与申报类别一致的网络安全服务项目所需的安全工具，并对工具进行管理和版本控制。

附 录 A
（规范性）
安全咨询服务专业能力评价要求

A.1 一级要求

A.1.1 基本要求

A.1.1.1 业绩要求

首次申请不做要求，维持资格最少完成1个安全咨询服务项目。

A.1.2 准备阶段

A.1.2.1 需求调研和分析

a) 开展项目前期调研，了解服务对象安全现状，确定客户需求；
b) 根据客户需求、项目目标和前期调研结果，分析与有关标准要求的差距，形成需求分析报告；
c) 与服务对象相关方充分沟通，就需求情况达成共识并形成记录。

A.1.2.2 人员和工具准备

a) 组建项目团队，包括技术咨询人员和管理咨询人员，指定项目负责人；
b) 根据项目需求准备必要的工具；
c) 对项目团队实施安全咨询服务前的培训。

A.1.3 方案设计阶段

a) 编制安全咨询服务方案和安全咨询服务模板，并在项目实施过程中按照模板实施；
b) 为安全咨询服务实施活动提供工作计划，方案应包含安全咨询服务准则。

A.1.4 实施阶段

A.1.4.1 安全咨询记录

a) 面向组织操作层，了解组织业务流程、技术应用和数据开发利用情况；
b) 形成安全咨询服务的解决方案；
c) 按照服务能力要求实施管理活动并记录，确保服务能力管理和服务过程实施可追溯，服务结果可度量或可评估。

A.1.4.2 安全咨询结果

a) 提交满足安全咨询服务方案的结果；
b) 根据调查及分析结果，为解决问题制定改善方案，并对其可行性和实效性进行评价，必要时对安全服务方案进行修改。

A.1.5 改进阶段

A.1.5.1 安全咨询管理

a) 建立客户满意度调查机制，对服务能力实施的结果进行评价，支持服务改进；
b) 识别改进项目，制定持续改进计划。

A.2 二级要求

A.2.1 基本要求

A.2.1.1 业绩要求

近三年内签订并完成至少2个安全咨询服务项目，维持资格最少完成1个安全咨询服务项目。

A.2.2 准备阶段

A.2.2.1 需求调研和分析

a) 开展项目前期调研，了解服务对象安全现状，确定客户需求；
b) 根据客户需求、项目目标和前期调研结果，分析与有关标准要求的差距，形成需求分析报告；
c) 与服务对象相关方充分沟通，就需求情况达成共识并形成记录。

A.2.2.2 人员和工具准备

a) 组建项目团队，包括技术咨询人员和管理咨询人员，指定项目负责人；
b) 根据项目需求准备必要的工具；
c) 对项目团队实施安全咨询服务前的培训。

A.2.3 方案设计阶段

a) 编制安全咨询服务方案和安全咨询服务模板，并在项目实施过程中按照模板实施；
b) 为安全咨询服务实施活动提供工作计划，方案应包含安全咨询服务准则。

A.2.4 实施阶段

A.2.4.1 安全咨询记录

a) 面向组织操作层和执行层，了解组织业务流程、技术应用和数据开发利用情况；
b) 形成安全咨询服务的解决方案；
c) 按照服务能力要求实施管理活动并记录，确保服务能力管理和服务过程实施可追溯，服务结果可度量或可评估。

A.2.4.2 安全咨询结果

a) 提交满足安全咨询服务方案的结果；
b) 根据调查及分析结果，为解决问题制定改善方案，并对其可行性和实效性进行评价，必要时对安全服务方案进行修改；
c) 实施成果在交付之前，应进行项目内部评审。

A.2.5 改进阶段

A.2.5.1 安全咨询管理

a) 建立客户满意度调查机制，对服务能力实施的结果进行评价，支持服务改进；

b） 识别改进项目，制定持续改进计划。

A.2.5.2 安全咨询要素

a） 对不符合要求的行为进行总结分析，对未达成的指标进行调查分析，根据分析结果确定改进措施，制定服务能力改进计划并实施；
b） 在整个组织中开展各种改进与创新，包括人员、过程、技术和资源等要素。

A.3 三级要求

A.3.1 基本要求

A.3.1.1 业绩要求

a） 近三年内签订并完成至少6个安全咨询服务项目，维持资格最少完成1个安全咨询服务项目；
b） 安全咨询服务近三年完成的服务业绩累积达30万元以上，其中至少有一个单个服务项目合同金额10万元及以上。

A.3.2 准备阶段

A.3.2.1 需求调研和分析

a） 开展项目前期调研，了解服务对象安全现状，确定客户需求；
b） 根据客户需求、项目目标和前期调研结果，分析与有关标准要求的差距，形成需求分析报告；
c） 与服务对象相关方充分沟通，就需求情况达成共识并形成记录。

A.3.2.2 人员和工具准备

a） 组建项目团队，包括技术咨询人员和管理咨询人员，指定项目负责人；
b） 根据项目需求准备必要的工具；
c） 对项目团队实施安全咨询服务前的培训。

A.3.3 方案设计阶段

a） 编制安全咨询服务方案和安全咨询服务模板，并在项目实施过程中按照模板实施；
b） 为安全咨询服务实施活动提供工作计划，方案应包含安全咨询服务准则。

A.3.4 实施阶段

A.3.4.1 安全咨询记录

a） 面向组织操作层、执行层和管理层，了解组织业务流程、技术应用和数据开发利用情况；
b） 形成安全咨询服务的解决方案；
c） 按照服务能力要求实施管理活动并记录，确保服务能力管理和服务过程实施可追溯，服务结果可度量或可评估。

A.3.4.2 安全咨询结果

a） 提交满足安全咨询服务方案的结果；
b） 根据调查及分析结果，为解决问题制定改善方案，并对其可行性和实效性进行评价，必要

时对安全服务方案进行修改；

c） 实施成果在交付之前，应进行项目内部评审；

d） 对用户开展安全咨询服务成果培训。

A.3.5 改进阶段

A.3.5.1 安全咨询管理

a） 建立客户满意度调查机制，对服务能力实施的结果进行评价，支持服务改进；

b） 识别改进项目，制定持续改进计划。

A.3.5.2 安全咨询要素

a） 对不符合要求的行为进行总结分析，对未达成的指标进行调查分析，根据分析结果确定改进措施，制定服务能力改进计划并实施；

b） 用多种方法在整个组织中开展各种改进与创新，包括人员、过程、技术和资源等要素；

c） 安全咨询服务的培训应区分对象和层次针对性开展，要有培训计划、培训课件、培训效果统计和考核。

A.4 四级要求

A.4.1 基本要求

A.4.1.1 业绩要求

a） 近三年内至少签订并完成10个安全咨询服务项目，维持资格最少完成1个安全咨询服务项目；

b） 安全咨询服务近三年完成的服务业绩累积达50万元及以上，其中至少有一个单个服务项目合同金额20万元及以上。

A.4.1.2 专业能力要求

近三年内，专业能力应具备下列其中一个：

a） 完成1项省（部）级及以上政府部门正式立项的本专业工程技术项目，对防范、控制网络空间安全事故有显著效果，并通过鉴定或验收；

b） 独立或合作解决技术问题，撰写技术或工程报告1篇及以上，并通过省（部）级以上科技或网络安全行政主管部门认定；

c） 主导或参与安全咨询相关的国际、国家、行业、地方、团体标准编制。

A.4.1.3 安全咨询资源

a） 建立安全咨询服务知识库，具备知识收集、检索和维护的手段和功能；

b） 建立安全咨询服务标准库，具备时效性、完善性、系统性和适用性；

c） 建立安全咨询服务专家库，能够满足项目需要。

A.4.2 准备阶段

A.4.2.1 需求调研和分析

a） 开展项目前期调研，了解服务对象安全现状，确定客户需求；

b） 根据客户需求、项目目标和前期调研结果，分析与有关标准要求的差距，形成需求分析报告；
c） 与服务对象相关方充分沟通，就需求情况达成共识并形成记录。

A.4.2.2 人员和工具准备

a） 组建项目团队，包括技术咨询人员和管理咨询人员，指定项目负责人；
b） 根据项目需求准备必要的工具；
c） 对项目团队实施安全咨询服务前的培训。

A.4.3 方案设计阶段

a） 编制安全咨询服务方案和安全咨询服务模板，并在项目实施过程中按照模板实施；
b） 为安全咨询服务实施活动提供工作计划，方案应包含安全咨询服务准则；
c） 提供项目风险识别、分析和控制措施，确定影响风险作用的程度和范围。

A.4.4 实施阶段

A．4.4.1 安全咨询记录

a） 面向组织操作层、执行层、管理层和决策层，了解组织业务流程、技术应用和数据开发利用情况；
b） 形成安全咨询服务的解决方案；
c） 按照服务能力要求实施管理活动并记录，确保服务能力管理和服务过程实施可追溯，服务结果可度量或可评估。

A．4.4.2 安全咨询结果

a） 提交满足安全咨询服务方案的结果；
b） 根据调查及分析结果，为解决问题制定改善方案，并对其可行性和实效性进行评价，必要时对安全服务方案进行修改；
c） 实施成果在交付之前，应进行项目内部评审；
d） 对用户开展安全咨询服务成果培训。

A．4.4.3 安全咨询方法

a） 采用多种咨询方法进行服务实施；
b） 针对项目成果应组织召开专家评审会。

A.4.5 改进阶段

A.4.5.1 安全咨询管理

a） 建立客户满意度调查机制，对服务能力实施的结果进行评价，支持服务改进；
b） 识别改进项目，制定持续改进计划。

A.4.5.2 安全咨询要素

a） 对不符合要求的行为进行总结分析，对未达成的指标进行调查分析，根据分析结果确定改进措施，制定服务能力改进计划并实施；

b) 用多种方法在整个组织中开展各种改进与创新，包括人员、过程、技术和资源等要素；
c) 安全咨询服务的培训应区分对象和层次针对性开展，要有培训计划、培训课件、培训效果统计和考核。

附 录 B
（规范性）
安全集成服务专业能力评价要求

B.1 一级要求

B.1.1 基本要求

首次申请不做要求，维持资格最少完成1个安全集成服务项目。

B.1.2 准备阶段

a) 调研客户信息，明确客户需求，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) 组建项目团队，团队应由管理层、相关业务骨干、IT技术人员等组成。

B.1.3 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。

B.1.4 实施阶段

B.1.4.1 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、服务对象汇报项目进度。

B.1.5 保障阶段

B.1.5.1 合规要求

无。

B.1.5.2 系统试运行

a) 系统部署完成后安排试运行，记录系统运行状况；
b) 基于系统运行情况，对系统进行调整和优化，以满足系统安全集成建设需求。

B.1.5.3 验收阶段

根据合同约定，提出验收申请并向服务对象提交完整的项目资料及交付物。

B.2 二级要求

B.2.1 基本要求

近三年内至少签订并完成2个安全集成服务项目，且安全集成服务业绩累积达总额150万元以上，工程按合同要求质量合格，已通过验收并投入实际应用。维持资格最少完成1个安全集成服务项目。

B.2.2 准备阶段

a) 调研客户信息，明确客户需求，采集系统建设安全需求和建设目标,明确系统功能、性能及安全性要求；
b) 组建项目团队，团队应由管理层、相关业务骨干、IT技术人员等组成，项目负责人应当具备同类项目的实施经验；
c) 根据调研信息并结合相应的安全建设标准、规范开展需求分析，编制需求分析报告。

B.2.3 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。

B.2.4 实施阶段

B.2.4.1 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、服务对象汇报项目进度；
c) 建立项目协调机制，与服务对象明确项目集成过程中的分工界面、双方的责任，保障各相关方在项目实施过程中能够充分有效的沟通；
d) 对项目实施过程中需要变更的地方应及时和服务对象进行沟通，并做好变更记录，同时与服务对象签字确认。

B.2.5 保障阶段

B.2.5.1 合规要求

a) 编写系统安全评估方案，并依据系统评估方案，对系统进行联调和系统测评，完整记录测评过程相关信息，形成评估报告，经双方责任人签字确认；
b) 针对系统测评的不符合项进行整改并记录。

B.2.5.2 系统试运行

a) 系统部署完成后安排试运行，记录系统运行状况；
b) 基于系统运行情况，对系统进行调整和优化，以满足系统安全集成建设需求；
c) 提供至少一个月的试运行记录，并及时整改系统运行中存在的问题。

B.2.5.3 验收阶段

依据合同约定，提出验收申请并向服务对象提交完整的项目资料及交付物。

B.3 三级要求

B.3.1 基本要求

近三年内至少签订并完成6个安全集成服务项目，且安全集成服务业绩累积总额达3000万元以上，并承担过至少1项不少于250万元或至少3项不少于150万元的项目；工程按合同要求质量合格，已通过验收并投入实际应用。维持资格最少完成1个安全集成服务项目。

B.3.2 准备阶段

a) 调研客户信息，明确客户需求，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) 组建项目团队，团队应由管理层、相关业务骨干、IT技术人员、应急人员等组成，项目负责人应当具备同类项目实施经验，应急人员应具有网络安全相关认证资质；
c) 根据调研信息并结合相应的安全建设标准、规范开展需求分析，编制需求分析报告。

B.3.3 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) 组织服务对象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，并结合方案评审意见，对方案进行调整、修改；
d) 结合技术、实施方案，对项目组及第三方配合人员进行业务和技能培训。

B.3.4 实施阶段

B.3.4.1 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、服务对象汇报项目进度；
c) 建立项目协调机制，与服务对象明确项目集成过程中的分工界面、双方的责任，保障各相关方在项目实施过程中能够充分有效的沟通；
d) 对项目实施过程中需要变更的地方应及时和服务对象进行沟通，并做好变更记录，同时与服务对象签字确认；
e) 项目建设施工完成后，提交完工报告；
f) 项目实施完成后，相关过程记录及时归档，并统一保管。

B.3.4.2 监督管理

服务机构应建立服务对象满意度调查机制，对项目实施过程中的所有变更、产品质量等需由服务对象责任人进行监督管理，所有设备入库、变更应由服务对象责任人签字确认。

B.3.5 保障阶段

B.3.5.1 合规要求

a) 编写系统安全评估方案，并依据系统评估方案，对系统进行联调和系统测评，完整记录测评过程相关信息，形成评估报告，经双方责任人签字确认；
b) 针对系统测评的不符合项进行整改并记录；
c) 依据技术方案具体指标要求，编写系统安全测评计划，对系统进行新上线前安全测评或安全符合性测评，形成测评报告，经双方责任人签字确认。

B.3.5.2 系统试运行

a) 系统部署完成后安排试运行，记录系统运行状况；
b) 基于系统运行情况，对系统进行调整和优化，以满足系统安全集成建设需求；
c) 提供至少两个月的试运行记录，并及时整改系统运行中存在的问题；

d) 试运行结束后，项目组编写系统试运行报告，提交给服务对象。

B.3.5.3 验收阶段

a) 根据合同约定，提出验收申请并向服务对象提交完整的项目资料及交付物；
b) 根据合同约定，配合组织项目验收，出具项目验收报告。

B.4 四级要求

B.4.1 基本要求

近三年内至少签订并完成10个安全集成服务项目，且安全集成服务业绩总额累积达5000万元以上，并承担过至少1项不少于500万元或至少4项不少于200万元的项目；工程按合同要求质量合格，已通过验收并投入实际应用。维持资格最少完成1个安全集成服务项目。

B.4.2 准备阶段

a) 调研客户信息，明确客户需求，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) 组建项目团队，团队应由管理层、相关业务骨干、IT技术人员、应急人员等组成，项目负责人应当具备同类项目实施经验，应急人员应具有网络安全相关认证资质；
c) 根据调研信息并结合相应的安全建设标准、规范开展需求分析，编制需求分析报告；
d) 建立安全集成服务制度或管理程序。

B.4.3 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) 组织服务对象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，并结合方案评审意见，对方案进行调整、修改；
d) 结合技术、实施方案，对项目组及第三方配合人员进行业务和技能培训；
e) 结合项目需要，编制安全集成项目施工手册和作业指导书，并由服务对象责任人确认；
f) 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；
g) 对于系统改造，应考虑改造前技术测试验证及在实施失败后的回退措施，制定应急处置计划书；
h) 基于安全集成项目需求和进度计划，编制网络安全产品或工具定制开发计划。

B.4.4 实施阶段

B.4.4.1 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、服务对象汇报项目进度；
c) 建立项目协调机制，与服务对象明确项目集成过程中的分工界面、双方的责任，保障各相关方在项目实施过程中能够充分有效的沟通；
d) 对项目实施过程中需要变更的地方应及时和服务对象进行沟通，并做好变更记录，同时与服务对象签字确认；

e) 项目建设施工完成后，提交完工报告；
f) 项目实施完成后，相关过程记录及时归档，并统一保管；
g) 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；
h) 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。并且对事件响应的过程有详细的文档记录和相关截图，记录包括：起因、现象、影响、处理过程、处理结果等。

B.4.4.2 监督管理

a) 服务机构应建立服务对象满意度调查机制，对项目实施过程中的所有变更、产品质量等需由服务对象责任人进行监督管理，所有设备入库、变更应由服务对象责任人签字确认；
b) 服务机构要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。

B.4.5 保障阶段

B.4.5.1 合规要求

a) 编写系统安全评估方案，并依据系统评估方案，对系统进行联调和系统测评，完整记录测评过程相关信息，形成评估报告，经双方责任人签字确认；
b) 针对系统测评的不符合项进行整改并记录；
c) 依据技术方案具体指标要求，编写系统安全测评计划，对系统进行新上线前安全测评或安全符合性测评，形成测评报告，经双方责任人签字确认；
d) 基于建设系统的安全要求，制定系统安全性测评方案，有专门的网络攻击工具，能模拟网络攻击场景，对系统安全性进行测评；
e) 基于系统的稳定性、承载能力要求，制定系统稳定性测评方案，有专门的系统压力测评工具，对系统的稳定性进行测评。

B.4.5.2 系统试运行

a) 系统部署完成后安排试运行，记录系统运行状况；
b) 基于系统运行情况，对系统进行调整和优化，以满足系统安全集成建设需求；
c) 提供至少三个月的试运行记录，并对系统试运行中存在的问题及时整改；
d) 试运行结束后，项目组编写系统试运行报告，提交给服务对象；
e) 对进行回归测试，合格后进行项目最终验收；
f) 制定系统试运行计划，建立应急响应服务保障团队和应急响应计划，及时应对突发事件；
g) 综合分析系统运行状态，建立系统运行管理手册和安全管理指南，并对相关产品和设备设施进行配置管理。

B.4.5.3 验收阶段

a) 根据合同约定，提出验收申请并向服务对象提交完整的项目资料及交付物；
b) 根据合同约定，配合组织项目验收，出具项目验收报告。

附 录 C
（规范性）
软件安全开发服务专业能力评价要求

C.1 一级要求

C.1.1 基本要求

首次申请不做要求，维持资格最少完成1个软件安全开发服务项目。

C.1.2 准备阶段

a) 拥有软件项目安全开发团队不少于3人，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。

C.1.3 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。

C.1.4 设计阶段

a) 根据软件项目需求，编制软件设计说明书；
b) 软件设计说明书应明确系统/子系统的功能和非功能设计要求；
c) 软件设计说明书应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。

C.1.5 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，应对软件进行安全编码；
c) 软件代码应经过安全检查、评审，对于发现的漏洞能有效修复，并形成记录。

C.1.6 测试阶段

a) 依据软件设计说明书应对软件功能、安全功能进行测试；
b) 应对测试发现的漏洞进行分析并有效修复。

C.1.7 验收交付

C.1.7.1 系统试运行

a) 测试系统运行的可靠性、稳定性和安全性，应进行试运行，并记录系统运行状况，试运行周期至少半个月；
b) 基于系统试运行相关记录，应及时对软件进行调整、维护。

C.1.7.2 验收项目

a) 根据合同约定，应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，应进行项目验收，形成项目验收报告。

C.1.7.3 维保阶段

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

C.2 二级要求

C.2.1 基本要求

近三年内签订并完成至少2个软件安全开发服务项目，维持资格最少完成1个软件安全开发服务项目。

C.2.2 准备阶段

a) 拥有软件项目安全开发团队不少于5人，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。

C.2.3 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。

C.2.4 设计阶段

a) 根据软件项目需求，编制软件设计说明书；
b) 软件设计说明书应明确系统/子系统的功能和非功能设计要求；
c) 软件设计说明书应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。

C.2.5 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，应对软件进行安全编码；
c) 软件代码应经过安全检查、评审，对于发现的漏洞能有效修复，并形成记录。

C.2.6 测试阶段

a) 依据软件设计说明书应对软件功能、安全功能进行测试；
b) 应对测试发现的漏洞进行分析并有效修复。

C.2.7 验收交付

C.2.7.1 系统试运行

a) 测试系统运行的可靠性、稳定性和安全性，并记录系统运行状况，试运行周期至少半个

月；

b） 基于系统试运行相关记录，应及时对软件进行调整、维护。

C.2.7.2 验收项目

a） 根据合同约定，应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，应进行项目验收，形成项目验收报告。

C.2.7.3 维保阶段

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

C.3 三级要求

C.3.1 基本要求

近三年内签订并完成至少6个软件安全开发服务项目，维持资格最少完成1个软件安全开发服务项目。

C.3.2 准备阶段

a） 拥有软件项目安全开发团队不少于8人，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） 制定软件项目培训计划，对相关人员进行安全培训；

f） 建立独立的测试环境，确保测试环境与开发环境隔离；

g） 配备专职测试人员。

C.3.3 需求阶段

a） 调研项目背景信息，收集项目需求，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,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；

c） 基于软件安全、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，报告中应明确项目开发过程中使用的安全技术标准、规范；

d） 对于数据采集、产生、使用，应明确识别安全保护要求。

C.3.4 设计阶段

a） 根据软件项目需求，编制软件设计说明书；

b） 软件设计说明书应明确系统/子系统的功能和非功能设计要求；

c） 软件设计说明书应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；

d） 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；

e） 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；

f） 基于软件项目需求分析建立软件安全开发模型。

C.3.5 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，应对软件进行安全编码；
c） 软件代码应经过安全检查、评审，对于发现的漏洞能有效修复，并形成记录。

C.3.6 测试阶段

C.3.6.1 单元测试

a） 应明确单元测试策略，制定单元测试计划；
b） 应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。

C.3.6.2 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.3.6.3 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。

C.3.7 验收交付

C.3.7.1 系统试运行

a） 测试系统运行的可靠性、稳定性和安全性，记录系统运行状况，提供至少一个月以上的试运行记录和报告；
b） 基于系统试运行相关记录，应及时对软件进行调整、维护。

C.3.7.2 验收项目

a） 根据合同约定，应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，应进行项目验收，形成项目验收报告；
c） 提交软件产品安全测评报告或安全认证证书。

C.3.7.3 维保阶段

a） 对于影响软件系统安全、稳定运行的缺陷，应及时有效采取打补丁、版本升级等方式给予消除并提供远程技术支持服务；
b） 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；
c） 根据健康检查报告进行分析，持续优化系统。

C.4 四级要求

C.4.1 基本要求

近三年内签订并完成至少10个软件安全开发服务项目，维持资格最少完成1个软件安全开发服务项目。

C.4.2 准备阶段

a) 拥有软件项目安全开发团队不少于12人，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) 制定软件项目培训计划，对相关人员进行安全培训；
f) 建立独立的测试环境，确保测试环境与开发环境隔离；
g) 配备专职测试人员；
h) 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。

C.4.3 需求阶段

a) 调研项目背景信息，收集项目需求，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,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；
c) 基于软件安全、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，报告中应明确项目开发过程中使用的安全技术标准、规范；
d) 对于数据采集、产生、使用，应明确识别安全保护要求；
e) 基于软件的业务流程开展安全威胁和安全隐私调研并进行登记管理。

C.4.4 设计阶段

a) 根据软件项目需求，编制软件设计说明书；
b) 软件设计说明书应明确系统/子系统的功能和非功能设计要求；
c) 软件设计说明书应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；
d) 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；
e) 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；
f) 基于软件项目需求分析建立软件安全开发模型；
g) 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；
h) 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。

C.4.5 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，应对软件进行安全编码；
c) 软件代码应经过安全检查、评审，对于发现的漏洞能有效修复，并形成记录；
d) 采用自动化工具结合人工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。

C.4.6 测试阶段

C.4.6.1 单元测试

a) 应明确单元测试策略，制定单元测试计划；
b) 应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。

C.4.6.2 集成测试

a) 明确集成测试策略，制定集成测试计划；
b) 应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.4.6.3 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；
d) 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；
e) 进行额外的模糊测试，增加模糊测试范围和持续时间。

C.4.7 验收交付

C.4.7.1 系统试运行

a) 测试系统运行的可靠性、稳定性和安全性，记录系统运行状况，提供三个月以上的试运行记录和报告；
b) 基于系统试运行相关记录，应及时对软件进行调整、维护；
c) 对可能发生的软件功能方面及安全方面提供可靠性指导说明书。

C.4.7.2 验收项目

a) 根据合同约定，应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，应进行项目验收，形成项目验收报告；
c) 提交软件产品安全测评报告或安全认证证书。

C.4.7.3 维保阶段

a) 对于影响软件系统安全、稳定运行的缺陷，应及时有效采取打补丁、版本升级等方式给予消除并提供远程技术支持服务；
b) 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；
c) 根据健康检查报告进行分析，持续优化系统；
d) 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；
e) 及时应对突发安全事件，并向用户提供安全事件解决报告；
f) 持续跟踪，若发生软件进行升级、权限变更、数据对接等问题，应进行再次测试及安全加

固服务；

g） 完成加固整改，应进行再次核查，检查加固效果是否符合安全需求。

附 录 D
（规范性）
安全运维服务专业能力评价要求

D.1 一级要求

D.1.1 基本要求

首次申请不做要求，维持资格最少完成1个安全运维服务项目。

D.1.2 准备阶段

a) 调研客户信息系统安全现状，收集客户运维服务需求，分析客户对信息系统安全运维服务的需求和类型；
b) 与服务对象充分沟通，并签订服务协议，对服务范围、内容、运维方式、时间、质量、管理要求等达成共识并形成记录。

D.1.3 方案设计阶段

a) 分析服务对象对信息网络系统安全服务的需求和类型，编写安全运维服务方案，明确日常巡检服务、运维监控与分析、安全运维服务时间、内容、运维方式、服务期限、服务人员、务交付物、质量管理、沟通机制、风险管理等方面要求；
b) 识别与分析信息系统运维过程中的历史数据和当前安全状态，提出系统运维的保障策略和解决方案。

D.1.4 实施阶段

a) 初始服务，主要包括资产识别、调研安全配置项、采集设备运行信息；
b) 对系统设备进行日常维护及监控，并记录硬件故障；
c) 日常巡检服务，对用户的网络设备、安全设备、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；
d) 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；
e) 健康检查服务，完成安全设备、业务系统的健康检查服务；
f) 对安全设备、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。

D.1.5 评审阶段

a) 向服务对象提交服务报告，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。

D.1.6 改进阶段

a) 建立客户满意度调查机制；
b) 运维过程中识别改进项目，制定持续改进计划。

D.2 二级要求

D.2.1 基本要求

近三年内签订并完成至少2个安全运维服务项目，维持资格最少完成1个安全运维服务项目。

D.2.2 准备阶段

a) 调研客户信息系统安全现状，收集客户运维服务需求，分析客户对信息系统安全运维服务的需求和类型；
b) 与服务对象充分沟通，并签订服务协议，对服务范围、内容、运维方式、时间、质量、管理要求等达成共识并形成记录。

D.2.3 方案设计阶段

a) 分析服务对象对信息网络系统安全服务的需求和类型，编写安全运维服务方案，明确日常巡检服务、运维监控与分析、安全运维服务时间、内容、运维方式、服务期限、服务人员、服务交付物、质量管理、沟通机制、风险管理等方面要求；
b) 识别与分析信息系统运维过程中的历史数据和当前安全状态，提出系统运维的保障策略和解决方案。

D.2.4 实施阶段

a) 初始服务，主要包括资产识别、调研安全配置项、采集设备运行信息；
b) 对系统设备进行日常维护及监控，并记录硬件故障；
c) 日常巡检服务，对用户的网络设备、安全设备、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；
d) 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；
e) 健康检查服务，完成安全设备、业务系统的健康检查服务；
f) 对安全设备、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。

D.2.5 评审阶段

a) 向服务对象提交服务报告，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。

D.2.6 改进阶段

a) 建立客户满意度调查机制；
b) 运维过程中识别改进项目，制定持续改进计划。

D.3 三级要求

D.3.1 基本要求

近三年内签订并完成至少6个安全运维服务项目，维持资格最少完成1个安全运维服务项目。

D.3.2 准备阶段

a) 调研客户信息系统安全现状，收集客户运维服务需求，分析客户对信息系统安全运维服务的需求和类型；
b) 与服务对象充分沟通，并签订服务协议，对服务范围、内容、运维方式、时间、质量、管理要求等达成共识并形成记录；
c) 根据客户的需求和收集的相关信息，编写需求分析报告。

D.3.3 方案设计阶段

a) 分析服务对象对信息网络系统安全服务的需求和类型，编写安全运维服务方案，明确日常巡检服务、运维监控与分析、安全运维服务时间、内容、运维方式、服务期限、服务人员、服务交付物、质量管理、沟通机制、风险管理等方面要求；
b) 识别与分析信息系统运维过程中的历史数据和当前安全状态，提出系统运维的保障策略和解决方案；
c) 建立信息网络系统安全运维的问题管理程序；
d) 建立安全事件处理流程、安全培训服务流程、渗透测试流程；
e) 建立知识管理程序形成知识库。

D.3.4 实施阶段

a) 初始服务，主要包括资产识别、调研安全配置项、采集设备运行信息；
b) 对系统设备进行日常维护及监控，并记录硬件故障；
c) 日常巡检服务，对用户的网络设备、安全设备、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；
d) 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；
e) 健康检查服务，完成安全设备、业务系统的健康检查服务；
f) 对安全设备、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；
g) 安全事件审计，收集与分析网络及安全设备、服务器、操作系统、应用系统日志，并进行记录；
h) 安全通告及漏洞分析，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；
i) 利用正版授权的工具或者自主研发的安全工具完成信息安全渗透测试，及时了解系统的安全现状；
j) 组建运维服务台职能，培养服务台人员的专业能力。

D.3.5 评审阶段

a) 向服务对象提交服务报告，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。

D.3.6 改进阶段

a) 建立客户满意度调查机制；

b) 运维过程中识别改进项目，制定持续改进计划；
c) 对客户系统的安全态势做出分析，并给出安全建议。

D.4 四级要求

D.4.1 基本要求

近三年内签订并完成至少10个安全运维服务项目，维持资格最少完成1个安全运维服务项目。

D.4.2 准备阶段

a) 调研客户信息系统安全现状，收集客户运维服务需求，分析客户对信息系统安全运维服务的需求和类型；
b) 与服务对象充分沟通，并签订服务协议，对服务范围、内容、运维方式、时间、质量、管理要求等达成共识并形成记录；
c) 根据客户的需求和收集的相关信息，编写需求分析报告。

D.4.3 方案设计阶段

a) 分析服务对象对信息网络系统安全服务的需求和类型，编写安全运维服务方案，明确日常巡检服务、运维监控与分析、安全运维服务时间、内容、运维方式、服务期限、服务人员、服务交付物、质量管理、沟通机制、风险管理等方面要求；
b) 识别与分析信息系统运维过程中的历史数据和当前安全状态，提出系统运维的保障策略和解决方案；
c) 建立信息网络系统安全运维的问题管理程序；
d) 建立安全事件处理流程、安全培训服务流程、渗透测试流程；
e) 建立知识管理程序形成知识库；
f) 建立系统应急事件响应机制和恢复保障机制；
g) 建立应急响应和灾难恢复机制，形成业务连续性计划。

D.4.4 实施阶段

a) 初始服务，主要包括资产识别、调研安全配置项、采集设备运行信息；
b) 对系统设备进行日常维护及监控，并记录硬件故障；
c) 日常巡检服务，对用户的网络设备、安全设备、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；
d) 日常安全运维，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；
e) 健康检查服务，完成安全设备、业务系统的健康检查服务；
f) 对安全设备、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；
g) 安全事件审计，收集与分析网络及安全设备、服务器、操作系统、应用系统日志，并进行记录；
h) 安全通告及漏洞分析，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；
i) 利用正版授权的工具或者自主研发的安全工具完成信息安全渗透测试，及时了解系统的安

全现状；

j） 组建运维服务台职能，培养服务台人员的专业能力；

k） 应急响应，制定应急响应预案，对应急事件及时响应，并对应急事件的处置开展演练，形成相关记录；

l） 变更控制，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；

m） 对已发现的信息网络系统安全漏洞及风险，进行系统安全加固与优化。

D.4.5 评审阶段

a） 向服务对象提交服务报告，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。

D.4.6 改进阶段

a） 建立客户满意度调查机制；

b） 运维过程中识别改进项目，制定持续改进计划；

c） 对客户系统的安全态势做出分析，并给出安全建议。

附 录 E
（规范性）
监测预警服务专业能力评价要求

E.1 一级要求

E.1.1 基本要求

a) 首次申请不做要求，维持资格最少完成1个监测预警服务项目；
b) 配备必要的监测环境、网络环境；
c) 具备专用监测工具或仪器设备；
d) 具有专业团队或专人负责开展网络安全监测预警服务工作。

E.1.2 准备阶段

a) 制定监测预警服务规范、流程；
b) 调研服务对象安全监测与预警的需求，签订相关服务合同或协议；
c) 取得服务对象的监测委托书或授权书；
d) 梳理完成服务对象的防护资产清单。

E.1.3 方案设计阶段

a) 组织项目成员对服务对象的网络环境、监测目标资产详情等进行现场或远程调研，根据服务对象需求制定监测预警技术方案；
b) 编制监测预警服务方案，明确项目组人员、项目负责人、进度、质量、沟通、风险等方面的要求。

E.1.4 实施阶段

a) 建立监测预警平台或将监测目标加入监测预警平台，对监测目标进行安全监测；
b) 定期对服务内容进行整理分析，定位系统脆弱性问题，形成阶段性安全服务报告；
c) 按服务对象要求，服务现场保存信息系统安全监测预警阶段性报告、网络安全信息通报报告、网络安全监测预警值班日志、网络安全监测预警值班表、网络安全监测采集规范、IT资产台账清单等文档。

E.1.5 总结阶段

a) 保存监测与预警工作日志；
b) 及时向服务对象提供安全通报或预警通报。

E.2 二级要求

E.2.1 基本要求

a) 近三年最少完成2个监测预警服务项目，维持资格最少完成1个监测预警服务项目；
b) 配备必要的监测环境、网络环境；
c) 具备专用监测工具或仪器设备；
d) 具有专业团队或专人负责开展网络安全监测预警服务工作。

E.2.2 准备阶段

a) 制定监测预警服务规范、流程；
b) 调研服务对象安全监测与预警的需求，签订相关服务合同或协议；
c) 取得服务对象的监测委托书或授权书；
d) 梳理完成服务对象的防护资产清单；
e) 制定监测流量和日志采集规范。

E.2.3 方案设计阶段

a) 组织项目成员对服务对象的网络环境、监测目标资产详情等进行现场或远程调研，根据服务对象需求制定监测预警技术方案；
b) 编制监测预警服务方案，明确项目组人员、项目负责人、进度、质量、沟通、风险等方面的要求。

E.2.4 实施阶段

a) 建立监测预警平台或将监测目标加入监测预警平台，对监测目标进行安全监测；
b) 定期对服务内容进行整理分析，定位系统脆弱性问题，形成阶段性安全服务报告；
c) 按服务对象要求，服务现场保存信息系统安全监测预警阶段性报告、网络安全信息通报报告、网络安全监测预警值班日志、网络安全监测预警值班表、网络安全监测采集规范、IT资产台账清单等文档；
d) 对监测目标进行周期性监测，有专人负责监测结果分析，对安全事件开展预警及事件跟踪，提交监测或预警分析报告；
e) 实施成果在交付之前，进行项目内部评审。

E.2.5 总结阶段

a) 保存监测与预警工作日志；
b) 及时向服务对象提供安全通报或预警通报；
c) 定期为服务对象提供安全监测预警的总结和分析报告。

E.3 三级要求

E.3.1 基本要求

a) 近三年最少完成6个监测预警服务项目，维持资格最少完成1个监测预警服务项目；
b) 配备必要的监测环境、网络环境；
c) 具备专用监测工具或仪器设备；
d) 具有专业团队或专人负责开展网络安全监测预警服务工作。

E.3.2 准备阶段

a) 制定监测预警服务规范、流程；
b) 调研服务对象安全监测与预警的需求，签订相关服务合同或协议；
c) 取得服务对象的监测委托书或授权书；
d) 梳理完成服务对象的防护资产清单；
e) 制定监测流量和日志采集规范。

E.3.3 方案设计阶段

a) 组织项目成员对服务对象的网络环境、监测目标资产详情等进行现场或远程调研，根据服务对象需求制定监测预警技术方案；
b) 编制监测预警服务方案，明确项目组人员、项目负责人、进度、质量、沟通、风险等方面的要求。

E.3.4 实施阶段

a) 建立监测预警平台或将监测目标加入监测预警平台，对监测目标进行安全监测；
b) 定期对服务内容进行整理分析，定位系统脆弱性问题，形成阶段性安全服务报告；
c) 按服务对象要求，服务现场保存信息系统安全监测预警阶段性报告、网络安全威胁情报分析报告、网络安全信息通报报告、网络安全监测预警值班日志、网络安全监测预警值班表、网络安全风险隐患分析报告、网络安全应急处置预案、网络安全应急演练报告、网络安全监测采集规范、IT资产台账清单等文档；
d) 对监测目标进行周期性监测，有专人负责监测结果分析，对安全事件开展预警及事件跟踪，提交监测或预警分析报告；
e) 实施成果在交付之前，应进行项目内部评审；
f) 项目实施人员按时提交监测记录及监控日志，及时汇报系统监控情况；
g) 在服务期间，应提供不间断的实时监测与预警服务；
h) 对网络安全事件实时跟踪，做好影响面评估，制定并定期修订网络安全事件应急预案。

E.3.5 总结阶段

a) 保存监测与预警工作日志；
b) 及时向服务对象提供安全通报、预警通报或安全威胁情报；
c) 定期为服务对象提供安全监测预警的总结和分析报告；
d) 向服务对象提供安全应急处置预案；
e) 为服务对象提供重大保障任务期间的安全分析报告；
f) 制定客户满意度调查机制，对服务实施的结果进行评价，支持服务改进。

E.4 四级要求

E.4.1 基本要求

a) 近三年最少完成10个监测预警服务项目，维持资格最少完成1个监测预警服务项目；
b) 配备必要的监测环境、网络环境；
c) 具备专用监测工具或仪器设备；
d) 具有专业团队或专人负责开展网络安全监测预警服务工作；
e) 至少有一项自主研发的网络安全检测分析工具或仪器设备；
f) 有独立的监测预警中心。

E.4.2 准备阶段

a) 制定监测预警服务规范、流程；
b) 调研服务对象安全监测与预警的需求，签订相关服务合同或协议；
c) 取得服务对象的监测委托书或授权书；

d) 梳理完成服务对象的防护资产清单；
e) 制定监测流量和日志的采集规范。

E.4.3 方案设计阶段

a) 组织项目成员对服务对象的网络环境、监测目标资产详情等进行现场或远程调研，根据服务对象需求制定监测预警技术方案；
b) 编制监测预警服务方案，明确项目组人员、项目负责人、进度、质量、沟通、风险等方面的要求。

E.4.4 实施阶段

a) 建立监测预警平台或将监测目标加入监测预警平台，对监测目标进行安全监测；
b) 定期对服务内容进行整理分析，定位系统脆弱性问题，形成阶段性安全服务报告；
c) 按服务对象要求，服务现场保存信息系统安全监测预警阶段性报告、网络安全攻击溯源取证报告、网络安全威胁情报分析报告、网络安全信息通报报告、网络安全监测预警值班日志、网络安全监测预警值班表、网络安全风险隐患分析报告、网络安全应急处置预案、网络安全应急演练报告、网络安全监测采集规范、IT资产台账清单等文档；
d) 对监测目标进行周期性监测，有专人负责监测结果分析，对安全事件开展预警及事件跟踪，提交监测或预警分析报告；
e) 实施成果在交付之前，应进行项目内部评审；
f) 项目实施人员按时提交监测记录及监控日志，及时汇报系统监控情况；
g) 在服务期间，应提供不间断的实时监测与预警服务；
h) 对网络安全事件实时跟踪，做好影响面评估，制定并定期修订网络安全事件应急预案；
i) 对网络安全攻击开展溯源分析，结合威胁情报，提供溯源报告；
j) 实现安全监测预警指令全流程线上闭环管理。

E.4.5 总结阶段

a) 保存监测与预警工作日志；
b) 及时向服务对象提供安全通报、预警通报或安全威胁情报；
c) 定期为服务对象提供安全监测预警的总结和分析报告；
d) 向服务对象提供安全应急处置预案；
e) 为服务对象提供重大保障任务期间的安全分析报告；
f) 制定客户满意度调查机制，对服务实施的结果进行评价，支持服务改进。

附 录 F
（规范性）
应急响应服务专业能力评价要求

F.1 一级要求

F.1.1 基本要求

a) 首次申请不做要求，维持资格最少完成1个应急响应服务项目；
b) 具备本地6小时、外地8小时以内，应急响应服务能力；
c) 配备应急处理服务人员至少2人，能处理一般网络安全事件能力；
d) 配备处理网络安全事件的工具包，定期更新工具包并记录。

F.1.2 准备阶段

a) 明确服务对象应急需求内容；
b) 制定应急处理服务流程。

F.1.3 检测阶段

a) 确定检测对象及范围，并得到用户的授权，机密性数据信息未经授权不应访问；
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、安全事件的响应等级，与服务对象共同确定应急处理方案；
c) 检测工作应在客户的监督与配合下完成。

F.1.4 抑制阶段

a) 应与服务对象充分沟通，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，必要时，需断开网络的对外连接，把损失控制在最小范围内；
c) 严格执行应急预案中抑制阶段规定的内容，如果有必要更改，应获得客户的授权同意；
d) 抑制措施应能够限制受攻击的范围，能抑制潜在的或进一步的攻击和破坏行为。

F.1.5 根除阶段

a) 协助服务对象检查所有受影响的系统，提出根除的方案建议；
b) 协助服务对象进行具体实施，明确告知所采取的根除措施可能带来的风险；
c) 找出导致安全事件发生的原因，并予以根除或控制；
d) 告知服务对象所采取的根除措施可能带来的风险，制定应变和回退措施，并获得书面授权。

F.1.6 恢复阶段

a) 与服务对象共同制定系统恢复方案，协助选择合理的恢复方法；
b) 告知服务对象系统的恢复方法及可能存在的风险；
c) 对于不能肯定系统经过根除处理后是否可恢复正常时，应选择通过原有的备份数据进行系统恢复；

d） 系统恢复后，应定期对系统数据进行备份，并验证备份数据有效性。

F.1.7 总结阶段

对事件处理过程进行总结和分析。

F.2 二级要求

F.2.1 基本要求

a） 近三年最少完成2个应急响应服务项目，维持资格最少完成1个应急响应服务项目；
b） 具备本地4小时、外地8小时以内，应急响应服务能力；
c） 配备应急处理服务人员至少3人，能处理一般网络安全事件能力；
d） 配备处理网络安全事件的工具包，定期更新工具包并记录。

F.2.2 准备阶段

a） 明确服务对象应急需求内容；
b） 制定应急处理服务流程。

F.2.3 检测阶段

a） 确定检测对象及范围，并得到用户的授权，机密性数据信息未经授权不应访问；
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、安全事件的响应等级，与服务对象共同确定应急处理方案；
c） 检测工作应在客户的监督与配合下完成；
d） 与服务对象充分沟通，评估应急处理方案可能造成的影响。

F.2.4 抑制阶段

a） 应与服务对象充分沟通，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，必要时，需断开网络的对外连接，把损失控制在最小范围内；
c） 严格执行应急预案中抑制阶段规定的内容，如果有必要更改，应获得客户的授权同意；
d） 抑制措施应能够限制受攻击的范围，能抑制潜在的或进一步的攻击和破坏行为。

F.2.5 根除阶段

a） 协助服务对象检查所有受影响的系统，提出根除的方案建议；
b） 协助服务对象进行具体实施，明确告知所采取的根除措施可能带来的风险；
c） 找出导致安全事件发生的原因，并予以根除或控制；
d） 告知服务对象所采取的根除措施可能带来的风险，制定应变和回退措施，并获得书面授权。

F.2.6 恢复阶段

a） 与服务对象共同制定系统恢复方案，协助选择合理的恢复方法；
b） 告知服务对象系统的恢复方法及可能存在的风险；
c） 对于不能肯定系统经过根除处理后是否可恢复正常时，应选择通过原有的备份数据进行系统恢复；

d） 系统恢复后，应定期对系统数据进行备份，并验证备份数据有效性。

F.2.7 总结阶段

a） 对事件处理过程进行总结和分析；
b） 提供详实的事件处理报告；
c） 提供建议和意见，协助服务对象完善系统安全建设。

F.3 三级要求

F.3.1 基本要求

a） 近三年最少完成6个应急响应服务项目，维持资格最少完成1个应急响应服务项目；
b） 具备本地2小时、外地8小时以内，应急响应服务能力；
c） 配备应急处理服务人员至少6人，具有处理较大网络安全事件的能力；

注：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。

d） 配备处理网络安全事件的工具包，定期更新工具包并记录；
e） 网络与信息安全事件工具包中应配备专业技术检测设备。

F.3.2 准备阶段

a） 明确服务对象应急需求内容；
b） 制定应急处理服务流程；
c） 按照服务对象需求制定应急服务方案，方案应涉及客户应急预案的启动与执行，若服务对象未建立应急预案，应协助服务对象建立和完善应急预案；
d） 建立常规应用系统、安全设备、常见网络安全事件的检测技术规范。

F.3.3 检测阶段

a） 确定检测对象及范围，并得到用户的授权，机密性数据信息未经授权不应访问；
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、安全事件的响应等级，与服务对象共同确定应急处理方案；
c） 检测工作应在客户的监督与配合下完成；
d） 与服务对象充分沟通，评估应急处理方案可能造成的影响；
e） 协助服务对象确定安全事件等级；
f） 根据应急预案制定本次应急处理方案，内容应包含实施方案失败的应变和回退措施。

F.3.4 抑制阶段

a） 应与服务对象充分沟通，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，必要时，需断开网络的对外连接，把损失控制在最小范围内；
c） 严格执行应急预案中抑制阶段规定的内容，如果有必要更改，应获得客户的授权同意；
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；
e） 在采取抑制措施之前，应告知客户可能存在的风险，制定应变和回退措施，并签订协议。

F.3.5 根除阶段

a) 协助服务对象检查所有受影响的系统，提出根除的方案建议；
b) 协助服务对象进行具体实施，明确告知所采取的根除措施可能带来的风险；
c) 找出导致安全事件发生的原因，并予以根除或控制；
d) 告知服务对象所采取的根除措施可能带来的风险，制定应变和回退措施，并获得书面授权。

F.3.6 恢复阶段

a) 与服务对象共同制定系统恢复方案，协助选择合理的恢复方法；
b) 告知服务对象系统的恢复方法及可能存在的风险；
c) 对于不能肯定系统经过根除处理后是否可恢复正常时，应选择通过原有的备份数据进行系统恢复；
d) 系统恢复后，应定期对系统数据进行备份，并验证备份数据有效性；
e) 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；
f) 若需重建系统，协助服务对象对重建后的系统进行备份；
g) 协助服务对象重建系统前应进行全面的数据备份，确保备份数据没有受到过攻击者的修改。

F.3.7 总结阶段

a) 对事件处理过程进行总结和分析；
b) 提供详实的事件处理报告；
c) 提供建议和意见，协助服务对象完善系统安全建设；
d) 及时检查事件处理记录，确保具备可追溯性。

F.4 四级要求

F.4.1 基本要求

a) 近三年最少完成10个应急响应服务项目，维持资格最少完成1个应急响应服务项目；
b) 具备本地1小时、外地8小时以内，应急响应服务能力；
c) 配备应急处理服务人员至少10人，具有重大网络安全事件处理能力；

注：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。

d) 配备处理网络安全事件的工具包，定期更新工具包并记录；
e) 网络与信息安全事件工具包中应配备专业技术检测设备。

F.4.2 准备阶段

a) 明确服务对象应急需求内容；
b) 制定应急处理服务流程；
c) 按照服务对象需求制定应急服务方案，方案应涉及客户应急预案的启动与执行，若服务对象未建立应急预案，应协助服务对象建立和完善应急预案；
d) 建立常规应用系统、安全设备、常见网络安全事件的检测技术规范，并具有应对高技术入侵的检测能力。

F.4.3 检测阶段

a) 确定检测对象及范围，并得到用户的授权,机密性数据信息未经授权不应访问；
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、安全事件的响应等级，与服务对象共同确定应急处理方案；
c) 检测工作应在客户的监督与配合下完成；
d) 与服务对象充分沟通，评估应急处理方案可能造成的影响；
e) 协助服务对象确定安全事件等级；
f) 根据应急预案制定本次应急处理方案，内容包含实施方案失败的应变和回退措施；
g) 保留完整的安全事件的检测步骤和文档，作为司法程序的相关证据。

F.4.4 抑制阶段

a) 应与服务对象充分沟通，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，必要时，需断开网络的对外连接，把损失控制在最小范围内；
c) 严格执行应急预案中抑制阶段规定的内容，如果有必要更改，应获得客户的授权同意；
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；
e) 在采取抑制措施之前，应告知客户可能存在的风险，制定应变和回退措施，并签订协议；
f) 应使用可信工具或自主开发的工具进行安全事件的抑制处理；
g) 应具备可靠的网络防御和攻击追踪溯源能力；
h) 应具备1小时内现场网络功能恢复能力，并使用可信工具构建防御体系。

F.4.5 根除阶段

a) 协助服务对象检查所有受影响的系统，提出根除的方案建议；
b) 协助服务对象进行具体实施，明确告知所采取的根除措施可能带来的风险；
c) 找出导致安全事件发生的原因，并予以根除或控制；
d) 告知服务对象所采取的根除措施可能带来的风险，制定应变和回退措施，并获得书面授权；
e) 应使用可信工具或自主开发的工具进行安全事件的根除处理。

F.4.6 恢复阶段

a) 与服务对象共同制定系统恢复方案，协助选择合理的恢复方法；
b) 告知服务对象系统的恢复方法及可能存在的风险；
c) 对于不能肯定系统经过根除处理后是否可恢复正常时，应选择通过原有的备份数据进行系统恢复；
d) 系统恢复后，应定期对系统数据进行备份，并验证备份数据有效性；
e) 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；
f) 若需重建系统，协助服务对象对重建后的系统进行备份；
g) 协助服务对象重建系统前应进行全面的数据备份，确保备份数据没有受到过攻击者的修改；
h) 若需重建系统，应协助客户对重建后的系统进行全面的安全加固，并利用工具对系统的安全性进行验证。

F.4.7 总结阶段

a) 对事件处理过程进行总结和分析；
b) 提供详实的事件处理报告；
c) 提供建议和意见，协助服务对象完善系统安全建设；
d) 及时检查事件处理记录，确保具备可追溯性；
e) 对事件进行总结和分析，针对典型案例建立事件知识库；
f) 告知服务对象所发生的事件可能涉及法律诉讼方面的要求或影响。

附 录 G
（规范性）
渗透测试服务专业能力评价要求

G.1 一级要求

G.1.1 基本要求

a) 首次申请不做要求，维持资格最少完成1个渗透测试服务项目；
b) 有必要的渗透测试工具，并对工具进行管理和版本控制。

G.1.2 准备阶段

G.1.2.1 需求分析

a) 调研客户背景信息，明确服务对象需求和渗透测试范围；
b) 签订服务合同或协议。

G.1.2.2 服务方案制定

a) 根据服务对象需求制定渗透测试方案，明确渗透测试目标、范围和边界、测试时间、测试深度和限制规则、项目组人员、项目负责人、进度、质量、沟通、风险等方面的要求；
b) 方案测试内容最少包括自动化测试方案，应有最新主流市面国产漏洞扫描工具使用要求，拟定扫描接入点方案，能对网络设备、应用系统、数据库等进行漏洞扫描能发现常规漏洞；手动渗透测试方案，应制定渗透测试能够发现未列入常用列表（例如， OWASP Top 10）的漏洞和弱点，并制定测试自动测试可能忽略的业务逻辑（例如，数据验证、完整性检查）进行验证方案；
c) 结合渗透测试方案，与客户进行沟通，获得客户认可。

G.1.2.3 人员和工具准备

a) 组建测试团队，测试团队应由管理层、相关业务骨干、测试人员等组成；
b) 准备渗透测试工具，包括但不限于主流漏洞扫描系统（能扫描主机、网络设备、安全设备、应用、数据库）、端口扫描工具、抓包分析工具、溢出工具、破解工具，工具都应有合法正规的来源，对漏洞扫描工具进行漏洞库与规则库更新，确保达到最新状态，并向用户报备；
c) 与用户方签署保密协议，与项目组成员签署保密承诺书，开展保密教育，落实保密措施；
d) 对测试团队实施渗透测试前的安全教育和技术培训。

G.1.2.4 其他准备工作

a) 取得服务对象书面渗透测试授权书；
b) 制定渗透测试风险告知书，告知用户方测试可能存在的风险，获得用户签字确认，并制定风险规避措施，确认用户已进行必要的数据备份；
c) 制定渗透测试行为规范，明确渗透测试人员测试过程中应遵守的行为准则，包括但不限于使用工具、禁用的渗透测试方式、不准许获得用户的生产数据、数据篡改、测试过程中禁

用的操作和命令、数据清除等；

d) 应向用户报备渗透测试过程中可能使用的IP地址。

G.1.3 实施阶段

a) 收集渗透对象的相关信息，包括但不限于IP、网段、域名、端口等基本信息、操作系统、数据库等系统信息等；

b) 使用漏洞扫描系统，应对渗透测试目标进行全面漏洞扫描，并记录漏洞扫描结果；

c) 编制渗透测试测试表单，表单上应列出所有需测试的内容，开展渗透测试，保存渗透测试结果，渗透人员签字确认；

d) 测试完成后，应对测试过程中产生的冗余数据和文件进行清除；

e) 渗透结束后应明确告知客户。

G.1.4 报告阶段

a) 对已验证存在的安全漏洞进行汇总分析，根据GB/T 30279-2020开展漏洞等级判定；

b) 对漏洞成因、验证过程、可能造成的危害进行分析，对所发现的问题提出合理高效安全的解决方案，形成渗透测试报告。

G.1.5 复测阶段

a) 对服务对象已整改的漏洞进行复测，保留复测记录，并签字确认；

b) 向服务对象提交渗透测试复测报告。

G.1.6 总结阶段

建立客户满意度调查机制。

G.2 二级要求

G.2.1 基本要求

a) 近3年最少完成2个渗透测试服务项目，维持资格最少完成1个渗透测试服务项目；

b) 有必要的渗透测试工具，并对工具进行管理和版本控制。

G.2.2 准备阶段

G.2.2.1 需求分析

a) 调研客户背景信息，明确服务对象需求和渗透测试范围；

b) 签订服务合同或协议。

G.2.2.2 服务方案制定

a) 根据服务对象需求制定渗透测试方案，明确渗透测试目标、范围和边界、测试时间、测试深度和限制规则、项目组人员、项目负责人、进度、质量、沟通、风险等方面的要求；

b) 方案测试内容最少包括自动化测试方案，应有最新主流市面国产漏洞扫描工具使用要求，拟定扫描接入点方案，能对网络设备、应用系统、数据库等进行漏洞扫描能发现常规漏洞；手动渗透测试方案，应制定渗透测试能够发现未列入常用列表（例如， OWASP Top

10）的漏洞和弱点，并制定测试自动测试可能忽略的业务逻辑（例如，数据验证、完整性检查）进行验证方案；

c) 结合渗透测试方案，与客户进行沟通，获得客户认可。

G.2.2.3 人员和工具准备

a) 组建测试团队，测试团队应由管理层、相关业务骨干、测试人员等组成；

b) 准备渗透测试工具，包括但不限于主流漏洞扫描系统（能扫描主机、网络设备、安全设备、应用、数据库）、端口扫描工具、抓包分析工具、溢出工具、破解工具，工具都应有合法正规的来源，对漏洞扫描工具进行漏洞库与规则库更新，确保达到最新状态，并向用户报备；

c) 与用户方签署保密协议，与项目组成员签署保密承诺书，开展保密教育，落实保密措施；

d) 对测试团队实施渗透测试前的安全教育和技术培训；

G.2.2.4 其他准备工作

a) 取得服务对象书面渗透测试授权书；

b) 制定渗透测试风险告知书，告知用户方测试可能存在的风险，获得用户签字确认，并制定风险规避措施，确认用户已进行必要的数据备份；

c) 制定渗透测试行为规范，明确渗透测试人员测试过程中应遵守的行为准则，包括但不限于使用工具、禁用的渗透测试方式、不准许获得用户的生产数据、数据篡改、测试过程中禁用的操作和命令、数据清除等；

d) 应向用户报备渗透测试过程中可能使用的IP地址；

e) 针对渗透测试过程中可能存在的风险制定应急处置预案。

G.2.3 实施阶段

a) 收集渗透对象的相关信息，包括但不限于IP、网段、域名、端口等基本信息、操作系统、数据库等系统信息等；

b) 使用漏洞扫描系统，对渗透测试目标进行全面漏洞扫描，并记录漏洞扫描结果；

c) 编制渗透测试测试表单，表单上应列出所有需测试的内容，开展渗透测试，保存渗透测试结果，渗透人员签字确认；

d) 测试完成后，应对测试过程中产生的冗余数据和文件进行清除；

e) 渗透结束后应明确告知客户。

G.2.4 报告阶段

a) 对已验证存在的安全漏洞进行汇总分析，根据GB/T 30279-2020开展漏洞等级判定；

b) 对漏洞成因、验证过程、可能造成的危害进行分析，对所发现的问题提出合理高效安全的解决方案，形成渗透测试报告。

G.2.5 复测阶段

a) 对服务对象已整改的漏洞进行复测，保留复测记录，并签字确认；

b) 向服务对象提交渗透测试复测报告；

G.2.6 总结阶段

a) 建立客户满意度调查机制；
b) 测试过程中识别改进项目，制定持续改进计划。

G.3 三级要求

G.3.1 基本要求

a) 近3年最少完成6个渗透测试服务项目，维持资格最少完成1个渗透测试服务项目；
b) 有必要的渗透测试工具，并对工具进行管理和版本控制；
c) 制定渗透测试服务规范，明确渗透测试内容、渗透测试方法、渗透测试流程等。

G.3.2 准备阶段

G.3.2.1 需求分析

a) 调研客户背景信息，明确服务对象需求和渗透测试范围；
b) 签订服务合同或协议。

G.3.2.2 服务方案制定

a) 根据服务对象需求制定渗透测试方案，明确渗透测试目标、范围和边界、测试时间、测试深度和限制规则、项目组人员、项目负责人、进度、质量、沟通、风险等方面的要求；
b) 方案测试内容最少包括自动化测试方案，应有最新主流市面国产漏洞扫描工具使用要求，拟定扫描接入点方案，能对网络设备、应用系统、数据库等进行漏洞扫描能发现常规漏洞；手动渗透测试方案，应制定渗透测试能够发现未列入常用列表（例如， OWASP Top 10）的漏洞和弱点，并制定测试自动测试可能忽略的业务逻辑（例如，数据验证、完整性检查）进行验证方案；
c) 结合渗透测试方案，与客户进行沟通，获得客户认可。

G.3.2.3 人员和工具准备

a) 组建测试团队，测试团队应由管理层、相关业务骨干、测试人员等组成；
b) 准备渗透测试工具，包括但不限于主流漏洞扫描系统（能扫描主机、网络设备、安全设备、应用、数据库）、端口扫描工具、抓包分析工具、溢出工具、破解工具，工具都应有合法正规的来源，对漏洞扫描工具进行漏洞库与规则库更新，确保达到最新状态，并向用户报备；
c) 与用户方签署保密协议，与项目组成员签署保密承诺书，开展保密教育，落实保密措施；
d) 对测试团队实施渗透测试前的安全教育和技术培训。

G.3.2.4 其他准备工作

a) 取得服务对象书面渗透测试授权书；
b) 制定渗透测试风险告知书，告知用户方测试可能存在的风险，获得用户签字确认，并制定风险规避措施，确认用户已进行必要的数据备份；
c) 制定渗透测试行为规范，明确渗透测试人员测试过程中应遵守的行为准则，包括但不限于使用工具、禁用的渗透测试方式、不准许获得用户的生产数据、数据篡改、测试过程中禁用的操作和命令、数据清除等；
d) 应向用户报备渗透测试过程中可能使用的IP地址；

e) 针对渗透测试过程中可能存在的风险制定应急处置预案；
f) 召开项目启动会议，与用户方、项目组成员，明确渗透测试目标、渗透测试范围和边界、测试时间、测试深度和限制规则，并有用户方确认签字。

G.3.3 实施阶段

a) 收集渗透对象的相关信息，包括但不限于IP、网段、域名、端口等基本信息、操作系统、数据库等系统信息等；
b) 使用漏洞扫描系统，应对渗透测试目标进行全面漏洞扫描，并记录漏洞扫描结果；
c) 编制渗透测试测试表单，表单上应列出所有需测试的内容，开展渗透测试，保存渗透测试结果，渗透人员签字确认；
d) 测试完成后，应对测试过程中产生的冗余数据和文件进行清除；
e) 渗透结束后应明确告知客户；
f) 对渗透测试发现的漏洞，有专人负责漏洞的复核；
g) 对渗透过程中全部流量进行审计记录留存，必要时提供录屏，确保渗透过程可追溯。

G.3.4 报告阶段

a) 对已验证存在的安全漏洞进行汇总分析，根据GB/T 30279-2020开展漏洞等级判定；
b) 对漏洞成因、验证过程、可能造成的危害进行分析，对所发现的问题提出合理高效安全的解决方案，形成渗透测试报告；
c) 对服务对象的安全漏洞进行闭环管理，给用户进行漏洞演示和讲解，指导用户开展漏洞整改。

G.3.5 复测阶段

a) 对服务对象已整改的漏洞进行复测，保留复测记录，并签字确认；
b) 向服务对象提交渗透测试复测报告；
c) 复测完成后，应再次对测试过程中产生的冗余数据和文件进行清除；
d) 安排人员对复测结果进行复核；
e) 对复测过程中全部流量进行审计记录留存，必要时可提供录屏，确保渗透过程可追溯。

G.3.6 总结阶段

a) 建立客户满意度调查机制；
b) 测试过程中识别改进项目，制定持续改进计划；
c) 定期向服务对象提供最新安全漏洞预警。

G.4 四级要求

G.4.1 基本要求

a) 近3年最少完成10个渗透测试服务项目，维持资格最少完成1个渗透测试服务项目；
b) 有必要的渗透测试工具，并对工具进行管理和版本控制；
c) 制定渗透测试服务规范，明确渗透测试内容、渗透测试方法、渗透测试流程等；
d) 至少有一项自主研发的用于网络安全领域漏洞检测验证分析工具或仪器设备；
e) 具有原创漏洞的挖掘能力，在CNVD或CNNVD国家漏洞库获得原创漏洞证明，且具备逆向分

析、0day漏洞的挖掘能力；

f) 具有自建的漏洞库和渗透测试知识库，包括但不限于各类安全漏洞的测试代码和工具、各类安全设备的防御和检测规则绕过机制及绕过工具。

G.4.2 准备阶段

G.4.2.1 需求分析

a) 调研客户背景信息，明确服务对象需求和渗透测试范围；
b) 签订服务合同或协议。

G.4.2.2 服务方案制定

a) 根据服务对象需求制定渗透测试方案，明确渗透测试目标、范围和边界、测试时间、测试深度和限制规则、项目组人员、项目负责人、进度、质量、沟通、风险等方面的要求；
b) 方案测试内容最少包括自动化测试方案，应有最新主流市面国产漏洞扫描工具使用要求，拟定扫描接入点方案，能对网络设备、应用系统、数据库等进行漏洞扫描能发现常规漏洞；手动渗透测试方案，应制定渗透测试能够发现未列入常用列表（例如， OWASP Top 10）的漏洞和弱点，并制定测试自动测试可能忽略的业务逻辑（例如，数据验证、完整性检查）进行验证方案；
c) 结合渗透测试方案，与客户进行沟通，获得客户认可。

G.4.2.3 人员和工具准备

a) 组建测试团队，测试团队应由管理层、相关业务骨干、测试人员等组成；
b) 准备渗透测试工具，包括但不限于主流漏洞扫描系统（能扫描主机、网络设备、安全设备、应用、数据库）、端口扫描工具、抓包分析工具、溢出工具、破解工具，工具都应有合法正规的来源，对漏洞扫描工具进行漏洞库与规则库更新，确保达到最新状态，并向用户报备；
c) 与用户方签署保密协议，与项目组成员签署保密承诺书，开展保密教育，落实保密措施；
d) 对测试团队实施渗透测试前的安全教育和技术培训。

G.4.2.4 其他准备工作

a) 取得服务对象书面渗透测试授权书；
b) 制定渗透测试风险告知书，告知用户方测试可能存在的风险，获得用户签字确认，并制定风险规避措施，确认用户已进行必要的数据备份；
c) 制定渗透测试行为规范，明确渗透测试人员测试过程中应遵守的行为准则，包括但不限于使用工具、禁用的渗透测试方式、不准许获得用户的生产数据、数据篡改、测试过程中禁用的操作和命令、数据清除等；
d) 应向用户报备渗透测试过程中可能使用的IP地址；
e) 针对渗透测试过程中可能存在的风险制定应急处置预案；
f) 召开项目启动会议，与用户方、项目组成员，明确渗透测试目标、渗透测试范围和边界、测试时间、测试深度和限制规则，并有用户方确认签字。

G.4.3 实施阶段

a) 收集渗透对象的相关信息，包括但不限于IP、网段、域名、端口等基本信息、操作系统、数据库等系统信息等；
b) 使用漏洞扫描系统，应对渗透测试目标进行全面漏洞扫描，并记录漏洞扫描结果；
c) 编制渗透测试测试表单，表单上应列出所有需测试的内容，开展渗透测试，保存渗透测试结果，渗透人员签字确认；
d) 测试完成后，应对测试过程中产生的冗余数据和文件进行清除；
e) 渗透结束后应明确告知客户；
f) 对渗透测试发现的漏洞，有专人负责漏洞的复核；
g) 对渗透过程中全部流量进行审计记录留存，必要时提供录屏，确保渗透过程可追溯；
h) 漏洞应进一步深入验证，获得用户方的再次确认和授权。

G.4.4 报告阶段

a) 对已验证存在的安全漏洞进行汇总分析，根据GB/T 30279-2020开展漏洞等级判定；
b) 对漏洞成因、验证过程、可能造成的危害进行分析，对所发现的问题提出合理高效安全的解决方案，形成渗透测试报告；
c) 对服务对象的安全漏洞进行闭环管理，给用户进行漏洞演示和讲解，指导用户开展漏洞整改；
d) 评估安全漏洞的影响范围，给出漏洞处置预案，并形成处置分析报告。

G.4.5 复测阶段

a) 对服务对象已整改的漏洞进行复测，保留复测记录，并签字确认；
b) 向服务对象提交渗透测试复测报告；
c) 复测完成后，应再次对测试过程中产生的冗余数据和文件进行清除；
d) 安排人员对复测结果进行复核；
e) 对复测过程中全部流量进行审计记录留存，必要时可提供录屏，确保渗透过程可追溯。

G.4.6 总结阶段

a) 建立客户满意度调查机制；
b) 测试过程中识别改进项目，制定持续改进计划；
c) 定期向服务对象提供最新安全漏洞预警；
d) 与客户召开漏洞分析会，分析复盘开发、业务、运营各个环节产生漏洞的原因，针对性的制定预防方案。

附 录 H
（规范性）
风险评估服务专业能力评价要求

H.1 一级要求

H.1.1 基本资格

H.1.1.1 经验业绩

首次申请不做要求，维持资格最少完成1个网络安全风险评估服务项目。

H.1.2 准备阶段

H.1.2.1 服务需求界定

a) 应确定评估目标，充分了解评估对象，获取各项业务及各项业务功能之间的相关性，确定支持各项业务功能的相应信息系统资源及其他资源，以及系统执行的关键功能，包括执行这些功能所需的特定系统资源；
b) 应明确评估目标之后，进一步明确评估范围，并合理定义评估对象和评估范围边界，可以参考以下评估范围边界划分原则：
   1）业务系统的业务逻辑边界；
   2）网络及设备载体边界；
   3）组织管理权限边界；
   4）其他。

H.1.2.2 服务方案制定

a) 应编制风险评估方案、风险评估测试用例，并在项目实施过程中按照测试用例实施；
b) 应为风险评估实施活动提供总体计划或方案。方案至少包括评估目标、评估范围、评估依据、评估方法、评估团队组织、工作计划、评估工作中的风险规避、时间进度安排及项目验收方法等。

H.1.2.3 人员和工具准备

a) 应组建评估团队，风险评估团队应由管理层、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工具。

H.1.3 风险识别阶段

H.1.3.1 资产识别

a) 应参考国家或国际标准，对资产进行分类；
b) 应识别重要信息资产，形成资产清单；
c) 对已识别的重要资产，应分析资产的保密性、完整性和可用性等安全属性的等级要求；
d) 对资产应根据其在保密性、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。

H.1.3.2 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。

H.1.3.3 威胁识别

a) 应该参考国家或国标标准，对威胁进行分类；
b) 应识别所评估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。

H.1.3.4 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。

H.1.4 风险分析阶段

H.1.4.1 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。

H.1.4.2 风险计算方法确定

应根据分析模型确定的方法计算出风险值。

H.1.4.3 风险评价

应根据风险评价准则确定风险等级。

H.1.4.4 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。

H.1.5 风险处置阶段

H.1.5.1 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。

H.1.5.2 安全整改建议

对组织不可接受的风险应提出风险处置措施。

H.2 二级要求

H.2.1 基本资格

H.2.1.1 经验业绩

近三年内签订并完成至少2个网络安全风险评估服务项目，维持资格最少完成1个网络安全风险评估服务项目。

H.2.2 准备阶段

H.2.2.1 服务需求界定

a) 应确定评估目标，充分了解评估对象，获取各项业务及各项业务功能之间的相关性，确定支持各项业务功能的相应信息系统资源及其他资源，以及系统执行的关键功能，包括执行这些功能所需的特定系统资源；
b) 应明确评估目标之后，进一步明确评估范围，并合理定义评估对象和评估范围边界，可以参考以下评估范围边界划分原则：
   1）业务系统的业务逻辑边界；
   2）网络及设备载体边界；
   3）组织管理权限边界；
   4）其他。

H.2.2.2 服务方案制定

a) 应编制风险评估方案、风险评估测试用例，并在项目实施过程中按照测试用例实施；
b) 应为风险评估实施活动提供总体计划或方案。方案至少包括评估目标、评估范围、评估依据、评估方法、评估团队组织、工作计划、评估工作中的风险规避、时间进度安排及项目验收方法等。

H.2.2.3 人员和工具准备

a) 应组建评估团队，风险评估团队应由管理层、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工具；
c) 应对评估团队实施风险评估前安全教育、保密教育和技术培训，制定风险评估过程管理的相关规定。可根据被评估要求，双方签署保密合同，适情签署个人保密协议；
d) 为确保风险评估工作顺利有效进行，应采用合理的项目管理机制，明确主要相关人员的角色与职责。

H.2.3 风险识别阶段

H.2.3.1 资产识别

a) 应参考国家或国际标准，对资产进行分类；
b) 应识别重要信息资产，形成资产清单；
c) 对已识别的重要资产，应分析资产的保密性、完整性和可用性等安全属性的等级要求；
d) 对资产应根据其在保密性、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。

H.2.3.2 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。

H.2.3.3 威胁识别

a) 应该参考国家或国标标准，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；
e） 应识别出组织和信息系统中潜在的对组织和信息造成影响的威胁。

H.2.3.4 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。

H.2.4 风险分析阶段

H.2.4.1 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。

H.2.4.2 风险计算方法确定

应根据分析模型确定的方法计算出风险值。

H.2.4.3 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。

H.2.4.4 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；
c） 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。

H.2.5 风险处置阶段

H.2.5.1 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。

H.2.5.2 安全整改建议

对组织不可接受的风险应提出风险处置措施。

H.3 三级要求

H.3.1 基本资格

H.3.1.1 经验业绩

近三年内签订并完成至少6个网络安全风险评估服务项目，维持资格最少完成1个网络安全风险评估服务项目。

H.3.2 准备阶段

H.3.2.1 服务需求界定

a） 应确定评估目标，充分了解评估对象，获取各项业务及各项业务功能之间的相关性，确定支

持各项业务功能的相应信息系统资源及其他资源，以及系统执行的关键功能，包括执行这些功能所需的特定系统资源；

b) 应明确评估目标之后，进一步明确评估范围，并合理定义评估对象和评估范围边界，可以参考以下评估范围边界划分原则：

1）业务系统的业务逻辑边界；

2）网络及设备载体边界；

3）组织管理权限边界；

4）其他。

H.3.2.2 服务方案制定

a) 应编制风险评估方案、风险评估测试用例，并在项目实施过程中按照测试用例实施；

b) 应为风险评估实施活动提供总体计划或方案。方案至少包括评估目标、评估范围、评估依据、评估方法、评估团队组织、工作计划、评估工作中的风险规避、时间进度安排及项目验收方法等。

H.3.2.3 人员和工具准备

a) 应组建评估团队，风险评估团队应由管理层、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工具；

c) 应对评估团队实施风险评估前安全教育、保密教育和技术培训，制定风险评估过程管理的相关规定，可根据被评估要求，双方签署保密协议，适情签署个人保密协议；

d) 为确保风险评估工作顺利有效进行，应采用合理的项目管理机制，明确主要相关人员的角色与职责；

e) 应采取相关措施，保障工具管理的规范性。

H.3.3 风险识别阶段

H.3.3.1 资产识别

a) 应参考国家或国际标准，对资产进行分类；

b) 应识别重要信息资产，形成资产清单；

c) 对已识别的重要资产，应分析资产的保密性、完整性和可用性等安全属性的等级要求；

d) 对资产应根据其在保密性、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。

H.3.3.2 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；

c) 应对脆弱性严重程度进行等级化处理，并形成脆弱性分析报告。

H.3.3.3 威胁识别

a) 应该参考国家或国标标准，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；
e） 应识别出组织和信息系统中潜在的对组织和信息造成影响的威胁；
f） 应采用多种方法进行威胁调查，并在威胁调查和威胁分析的基础上，形成威胁分析报告。

H.3.3.4 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。

H.3.4 风险分析阶段

H.3.4.1 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） 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。

H.3.4.2 风险计算方法确定

a） 应根据分析模型确定的方法计算出风险值；
b） 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；
c） 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。

H.3.4.3 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。

H.3.4.4 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；
c） 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。

H.3.5 风险处置阶段

H.3.5.1 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。

H.3.5.2 安全整改建议

对组织不可接受的风险应提出风险处置措施。

H.3.5.3 组织评审会

a） 应协助被评估组织召开评审会；
b） 应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。

H.4 四级要求

H.4.1 基本资格

H.4.1.1 经验业绩

近三年内至少签订并完成10个网络安全风险评估服务项目，维持资格最少完成1个网络安全风险评估服务项目。

H.4.1.2 专业研发能力

专业研发能力应具备下列其中一个：

a) 独立开发具有自主知识产权的测试工具；

b) 主导或参与网络安全风险评估相关的国际、国家、行业、地方、团体标准编制。

H.4.2 准备阶段

H.4.2.1 服务需求界定

a) 应确定评估目标，充分了解评估对象，获取各项业务及各项业务功能之间的相关性，确定支持各项业务功能的相应信息系统资源及其他资源，以及系统执行的关键功能，包括执行这些功能所需的特定系统资源；

b) 应明确评估目标之后，进一步明确评估范围，并合理定义评估对象和评估范围边界，可以参考以下评估范围边界划分原则：

1）业务系统的业务逻辑边界；

2）网络及设备载体边界；

3）组织管理权限边界；

4）其他。

H.4.2.2 服务方案制定

a) 应编制风险评估方案、风险评估测试用例，并在项目实施过程中按照测试用例实施；

b) 应为风险评估实施活动提供总体计划或方案。方案至少包括评估目标、评估范围、评估依据、评估方法、评估团队组织、工作计划、评估工作中的风险规避、时间进度安排及项目验收方法等。

H.4.2.3 人员和工具准备

a) 应组建评估团队，风险评估团队应由管理层、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工具；

c) 应对评估团队实施风险评估前安全教育、保密教育和技术培训，制定风险评估过程管理的相关规定。可根据被评估要求，双方签署保密合同，适情签署个人保密协议；

d) 为确保风险评估工作顺利有效进行，应采用合理的项目管理机制，明确主要相关人员的角色与职责；

e) 应采取相关措施，保障工具管理的规范性。

H.4.3 风险识别阶段

H.4.3.1 资产识别

a) 应参考国家或国际标准，对资产进行分类；

b） 应识别重要信息资产，形成资产清单；
c） 对已识别的重要资产，应分析资产的保密性、完整性和可用性等安全属性的等级要求；
d） 对资产应根据其在保密性、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；
e） 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；
f） 根据业务特点和业务流程识别出关键数据和关键服务；
g） 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。

H.4.3.2 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；
c） 应对脆弱性严重程度进行等级化处理，并形成脆弱性分析报告。

H.4.3.3 威胁识别

a） 应该参考国家或国标标准，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；
e） 应识别出组织和信息系统中潜在的对组织和信息造成影响的威胁；
f） 应采用多种方法进行威胁调查，并在威胁调查和威胁分析的基础上，形成威胁分析报告。

H.4.3.4 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。

H.4.4 风险分析阶段

H.4.4.1 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） 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。

H.4.4.2 风险计算方法确定

a） 应根据分析模型确定的方法计算出风险值；
b） 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；
c） 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。

H.4.4.3 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。

H.4.4.4 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；
c) 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。

H.4.5 风险处置阶段

H.4.5.1 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。

H.4.5.2 安全整改建议

对组织不可接受的风险应提出风险处置措施。

H.4.5.3 组织评审会

a) 应协助被评估组织召开评审会；
b) 应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。

H.4.5.4 残余风险处置

a) 应对组织提出完整的风险处置方案；
b) 必要时，应对残余风险进行再评估。

附 录 I
（规范性）
安全审计服务专业能力评价要求

I.1 一级要求

I.1.1 基本要求

I.1.1.1 业绩要求

首次申请不做要求，维持资格最少完成1个信息系统安全审计服务项目。

I.1.1.2 专业能力要求

a) 应建立信息系统审计服务流程；
b) 应制定信息系统审计服务规范；
c) 应具备脆弱性测试、渗透测试、漏洞测试、账号管理审查、数据备份验证等能力。

I.1.1.3 人员和专用工具要求

a) 应至少具有2名获得信息系统审计师专业认证的技术人员；
b) 应根据服务内容的需求准备必要的工具。

I.1.2 计划阶段要求

a) 应组建审计小组，明确相关职责，并对小组人员进行技术培训；
b) 应根据被审计方需求，确定审计对象、审计目的、审计范围；
c) 应编制业务情况调研表，并按照调研表收集有效信息；
d) 应编制信息系统资产情况调研表，并按照调研表收集信息；
e) 应制定信息系统审计方案及计划，明确信息系统审计依据。

I.1.3 审计取证与评价阶段要求

a) 应建立审计取证方法，不限于访谈、文件和记录调阅、审计项检查表、系统操作验证、审计工具、函证中的一种或多种；
b) 应分析被审计方的组织结构、岗位职责；
c) 应分析被审计方IT管理情况、IT支撑业务的对应关系；
d) 应审查被审计方的信息技术一般控制情况，如机房管理情况、网络管理情况、运维管理情况、网络安全等级保护落实情况、软件正版化情况、重要信息系统情况等，并形成审计工作底稿。

I.1.4 审计报告阶段要求

a) 提供网络安全审计报告，应完整、准确地反应审计结果，内容应包括审计概况、审计依据、审计发现、审计结论、审计意见等；
b) 应建立审计报告的批准和交付程序，保留交付记录；
c) 应审计工作底稿应经被审计方签字确认。

I.2 二级要求

I.2.1 基本要求

I.2.1.1 业绩要求

近三年内签订并完成至少3个信息系统安全审计服务项目，维持资格最少完成1个信息系统安全审计服务项目。

I.2.1.2 专业能力要求

a) 应建立信息系统审计服务流程；
b) 应制定信息系统审计服务规范；
c) 应具备脆弱性测试、渗透测试、漏洞测试、日志审查、代码审计、账号管理审查、数据备份验证等能力。

I.2.1.3 人员和专用工具要求

a) 应至少具有4名获得信息系统审计师专业认证的技术人员，以及5名及以上安全服务技术人员；
b) 应根据服务内容的需求准备必要的工具，具有工具定制研发的能力。

I.2.2 计划阶段要求

a) 应组建审计小组，明确相关职责，并对小组人员进行技术培训；
b) 应根据被审计方需求，确定审计对象、审计目的、审计范围；
c) 应编制业务情况调研表，并按照调研表收集有效信息；
d) 应编制信息系统资产情况调研表，并按照调研表收集信息；
e) 应制定信息系统审计方案及计划，明确信息系统审计依据；
f) 审计范围应包括组织机构范围、业务范围、IT基础设施和应用系统范围等；
g) 审计内容应划分到具体审计事项，明确每一个审计事项的审计要点和审计方法及所需资源；
h) 审计方法及所需资源应包括审计人员、计划时间安排、审计工具，以及可操作的审计方法和流程。

I.2.3 审计取证与评价阶段要求

a) 应建立审计取证方法，不限于访谈、文件和记录调阅、审计项检查表、系统操作验证、审计工具、函证中的一种或多种；
b) 应分析被审计方的组织结构、岗位职责；
c) 应分析被审计方IT管理情况、IT支撑业务的对应关系；
d) 应审查被审计方的信息技术一般控制情况，如机房管理情况、网络管理情况、运维管理情况、网络安全等级保护落实情况、软件正版化情况、重要信息系统情况等，并形成审计工作底稿；
e) 应审查被审计方的系统建设合规（需求论证、预算制定、项目立项、项目采购、项目招标、商务谈判、供应商管理、合同管理、项目验收、钱款支付等）、系统应用绩效（系统建设、经效益、用户满意度），并形成审计工作底稿。

I.2.4 审计报告阶段要求

a) 提供网络安全审计报告，应完整、准确地反应审计结果，内容应包括审计概况、审计依据、审计发现、审计结论、审计意见等；
b) 应建立审计报告的批准和交付程序，保留交付记录；
c) 应审计工作底稿应经被审计方签字确认；
d) 应在审计取证完成后，编制审计工作底稿或审计取证单，审计工作底稿应内容完整、记录清晰、结论明确，客观地反映项目审计方案的编制及实施情况，以及与形成审计结论、意见和建议有关的所有重要事项；
e) 应要素齐全、格式规范，完整反映审计中发现的重要问题；
f) 应提出可行的改进建议，以促进被审计方信息系统有效支撑其业务的目标。

I.3 三级要求

I.3.1 基本要求

I.3.1.1 业绩要求

近三年内签订并完成至少6个信息系统安全审计服务项目，维持资格最少完成1个信息系统安全审计服务项目。

I.3.1.2 专业能力要求

a) 应建立信息系统审计服务流程；
b) 应制定信息系统审计服务规范；
c) 应具备脆弱性测试、渗透测试、漏洞测试、日志审查、代码审计、滥用案例测试、接口测试、账号管理审查、数据备份验证、安全培训、灾难恢复等能力；
d) 应符合国内或国际质量管理体系标准要求。

I.3.1.3 人员和专用工具要求

a) 应至少具有6名获得信息系统审计师专业认证的技术人员，以及10名及以上安全服务技术人员；
b) 应根据服务内容的需求准备必要的工具，自主开发专业检测工具的能力。

I.3.2 计划阶段要求

a) 应组建审计小组，明确相关职责，并对小组人员进行技术培训；
b) 应根据被审计方需求，确定审计对象、审计目的、审计范围；
c) 应编制业务情况调研表，并按照调研表收集有效信息；
d) 应编制信息系统资产情况调研表，并按照调研表收集信息；
e) 应制定信息系统审计方案及计划，明确信息系统审计依据；
f) 审计范围应包括组织机构范围、业务范围、IT基础设施和应用系统范围等；
g) 审计内容应划分到具体审计事项，明确每一个审计事项的审计要点和审计方法及所需资源；
h) 审计方法及所需资源应包括审计人员、计划时间安排、审计工具，以及可操作的审计方法和流程；
i) 应搜集并确定检查的部门政策、标准和指南；
j) 应编制审计对象列表，包括审计对象的数量、容量、功用、版本等属性；

k） 应梳理被审计方业务逻辑、应用系统处理逻辑和IT基础设施架构；
l） 应利用应用系统工具来建立和管理审计对象库；
m） 应对信息系统审计的风险进行初步评价；
n） 应梳理被审计方规章制度文件，形成审计项并编制对应检查表；
o） 应编制完整审计调研报告，并说明审计重点审计项。

I.3.3 审计取证与评价阶段要求

a） 应建立审计取证方法，不限于访谈、文件和记录调阅、审计项检查表、系统操作验证、审计工具、函证中的一种或多种；
b） 应分析被审计方的组织结构、岗位职责；
c） 应分析被审计方IT管理情况、IT支撑业务的对应关系；
d） 应审查被审计方的信息技术一般控制情况，如机房管理情况、网络管理情况、运维管理情况、网络安全等级保护落实情况、软件正版化情况、重要信息系统情况等，并形成审计工作底稿；
e） 应审查被审计方的系统建设合规（需求论证、预算制定、项目立项、项目采购、项目招标、商务谈判、供应商管理、合同管理、项目验收、钱款支付等）、系统应用绩效（系统建设、经效益、用户满意度），并形成审计工作底稿；
f） 应安排对审计发现问题的整改措施和整改措施的效果进行跟踪审计；
g） 应与被审计方约定在规定的时间内容实施跟踪审计，一般自审计报告交付起不超过6个月；
h） 应当根据跟踪审计的实施过程和结果编制跟踪审计报告；
i） 应建立审计质量控制程序，包含审计质量责任、职业道德、职业胜任能力、业务执行和质量监控等在内的质量控制制度，对被审计单位作出准确的审计结论。

I.3.4 审计报告阶段要求

a） 提供网络安全审计报告，应完整、准确地反应审计结果，内容应包括审计概况、审计依据、审计发现、审计结论、审计意见等；
b） 应建立审计报告的批准和交付程序，保留交付记录；
c） 应审计工作底稿应经被审计方签字确认；
d） 应在审计取证完成后，编制审计工作底稿或审计取证单，审计工作底稿应内容完整、记录清晰、结论明确，客观地反映项目审计方案的编制及实施情况，以及与形成审计结论、意见和建议有关的所有重要事项；
e） 应要素齐全、格式规范，完整反映审计中发现的重要问题；
f） 应提出可行的改进建议，以促进被审计方信息系统有效支撑其业务的目标；
g） 应对审计证据与审计依据的符合性进行评价，以形成审计发现；
h） 信息系统审计评价应客观、公正地反映被审计单位信息系统的真实情况。

I.4 四级要求

I.4.1 基本要求

I.4.1.1 业绩要求

近三年内签订并完成至少10个信息系统安全审计服务项目，维持资格最少完成1个信息系统安全审计服务项目。

I.4.1.2 专业能力要求

a) 应建立信息系统审计服务流程；
b) 应制定信息系统审计服务规范；
c) 应具备脆弱性测试、渗透测试、漏洞测试、日志审查、代码审计、滥用案例测试、接口测试、合成交易、账号管理审查、数据备份验证、安全培训、灾难恢复、业务连续性测试、关键绩效和风险指标测试等能力；
d) 应符合国内或国际质量管理体系标准要求；
e) 应符合国内或国际信息安全管理体系标准要求。

I.4.1.3 人员和专用工具要求

a) 应至少具有6名获得信息系统审计师专业认证的技术人员，以及10名及以上安全服务技术人员；
b) 应根据服务内容的需求准备必要的工具，自主开发专业检测工具的能力。

I.4.2 计划阶段要求

a) 应组建审计小组，明确相关职责，并对小组人员进行技术培训；
b) 应根据被审计方需求，确定审计对象、审计目的、审计范围；
c) 应编制业务情况调研表，并按照调研表收集有效信息；
d) 应编制信息系统资产情况调研表，并按照调研表收集信息；
e) 应制定信息系统审计方案及计划，明确信息系统审计依据；
f) 审计范围应包括组织机构范围、业务范围、IT基础设施和应用系统范围等；
g) 审计内容应划分到具体审计事项，明确每一个审计事项的审计要点和审计方法及所需资源；
h) 审计方法及所需资源应包括审计人员、计划时间安排、审计工具，以及可操作的审计方法和流程；
i) 应搜集并确定检查的部门政策、标准和指南；
j) 应编制审计对象列表，包括审计对象的数量、容量、功用、版本等属性；
k) 应梳理被审计方业务逻辑、应用系统处理逻辑和IT基础设施架构；
l) 应利用应用系统工具来建立和管理审计对象库；
m) 应对信息系统审计的风险进行初步评价；
n) 应梳理被审计方规章制度文件，形成审计项并编制对应检查表；
o) 应编制完整审计调研报告，并说明审计重点审计项；
p) 应制定审计风险评价准则，评价审计风险，为确定重点审计项和明确审计内容提供依据；
q) 应建立审计调研报告分级复核程序，明确规定各级复核人员的要求和责任；
r) 应具备为被审计方提供审计对象管理工具的能力。

I.4.3 审计取证与评价阶段要求

a) 应建立审计取证方法，不限于访谈、文件和记录调阅、审计项检查表、系统操作验证、审

计工具、函证中的一种或多种；

b) 应分析被审计方的组织结构、岗位职责；

c) 应分析被审计方IT管理情况、IT支撑业务的对应关系；

d) 应审查被审计方的信息技术一般控制情况，如机房管理情况、网络管理情况、运维管理情况、网络安全等级保护落实情况、软件正版化情况、重要信息系统情况等，并形成审计工作底稿；

e) 应审查被审计方的系统建设合规（需求论证、预算制定、项目立项、项目采购、项目招标、商务谈判、供应商管理、合同管理、项目验收、钱款支付等）、系统应用绩效（系统建设、经效益、用户满意度），并形成审计工作底稿；

f) 应安排对审计发现问题的整改措施和整改措施的效果进行跟踪审计；

g) 应与被审计方约定在规定的时间内容实施跟踪审计，一般自审计报告交付起不超过6个月；

h) 应当根据跟踪审计的实施过程和结果编制跟踪审计报告；

i) 应建立审计质量控制程序，包含审计质量责任、职业道德、职业胜任能力、业务执行和质量监控等在内的质量控制制度，对被审计单位作出准确的审计结论；

j) 应具备至少利用二种以上审计工具（如流量分析、漏洞和缺陷扫描类、系统配置和运行日志检查等类型）执行审计取证的能力；

k) 对电子形式存在的审计证据，应做好取证记录，并经被审计方相关人员确认；

l) 应采取必要的措施，保护取证过程中所采集的电子数据的安全性；

m) 应具备统计分析、关联分析、辅助审计等审计工具的能力；

n) 应建立网络安全审计工作手册，规范网络安全审计全生命周期内的所有活动；

o) 应确保审计质量控制程序与网络安全审计工作手册相适应；

p) 应监督信息系统审计实施的全过程；

q) 应定期开展网络安全审计质量检查；

r) 应初步建立审计依据合规库，并形成合规清单；

s) 应基本建立审计控制质量规范，如审计方案考虑因素、审计基本流程等；

t) 应建立各类审计使用的模板表单，包括方案、报告、审计底稿、审计通知书等；

u) 应建立详细的审计控制测试程序，如抽样执行方法、实质性测试具体方案、审计工具接入等。

I.4.4 审计报告阶段要求

a) 提供网络安全审计报告，应完整、准确地反应审计结果，内容应包括审计概况、审计依据、审计发现、审计结论、审计意见等；

b) 应建立审计报告的批准和交付程序，保留交付记录；

c) 应审计工作底稿应经被审计方签字确认；

d) 应在审计取证完成后，编制审计工作底稿或审计取证单，审计工作底稿应内容完整、记录清晰、结论明确，客观地反映项目审计方案的编制及实施情况，以及与形成审计结论、意见和建议有关的所有重要事项；

e) 应要素齐全、格式规范，完整反映审计中发现的重要问题；

f) 应提出可行的改进建议，以促进被审计方信息系统有效支撑其业务的目标；

g) 应对审计证据与审计依据的符合性进行评价，以形成审计发现；

h) 信息系统审计评价应客观、公正地反映被审计单位信息系统的真实情况；
i) 应建立审计工作底稿的分级复核程序，明确规定各级复核人员的要求和责任；
j) 审计工作底稿的内容应包括但不限于被审计部门的名称，审计事项及其期间或者截止日期，审计程序的执行过程及结果记录，审计结论、意见及建议，审计人员姓名和审计日期，复核人员姓名、复核日期和复核意见，编号及页次，被审计方意见、附件等；
k) 应利用应用系统工具来归档和保管审计工作底稿；
l) 应具备为被审计方提供审计工作底稿管理工具的能力；
m) 应编制审计发现列表，并利用应用系统工具来管理审计发现列表；
n) 应建立审计报告分级复核程序，明确规定各级复核人员的要求和责任；
o) 应建立程序，对已经出具的审计报告可能存在的重要错误或者遗漏及时更正，并将更正后的审计报告提交给原审计报告接收者；
p) 在审计的任何阶段，如果遇到或发现与审计目标和内容有关的重大问题，如违法违规问题、重大安全风险等，应出具审计专报；
q) 应建立审计报告归档和保管程序，任何组织或者个人查阅和使用归档后的审计报告，应经审计机构负责人批准，但国家有关部门依法进行查阅的除外；
r) 审计报告归被审计方所有，被审计方对审计报告的使用、保管等有明确要求的，应遵守其要求；
s) 应当根据跟踪审计的实施过程和结果编制跟踪审计报告。

附 录 J
（规范性）
数据安全服务专业能力评价要求

J.1 一级要求

J.1.1 基本要求

J.1.1.1 业绩要求

首次申请不做要求，维持资格最少完成1个数据安全服务项目。

J.1.1.2 专业工具

a) 具有必要的专业检测工具；
b) 应对技术工具进行管理，定期进行跟踪、检查技术工具的状态，并建立对技术工具的测量历史记录。

J.1.2 准备阶段

a) 了解数据所有者的组织架构、数据安全的管理机制；
b) 识别客户对数据安全管理和技术服务的目标和需求；
c) 调研客户信息系统业务情况、数据库类型、数据库部署环境、数据库最大并发量、单个数据库表的数量、数据条数、数据库事务数、数据库访问量、数据库访问方式等；
d) 识别影响数据安全服务的法律、政策、标准、外部影响和约束条件；
e) 识别客户实际环境中，数据面临的潜在安全威胁，分析服务过程中可能产生的安全风险；
f) 编制完整的数据生命周期各阶段安全防护现状的调研报告，调研的内容包括但不限于组织架构、制度列表、业务流程、数据库类　型数据库架构、数据访问方式、数据现有防护措施、管理人员信息等；
g) 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；
h) 服务人员签订保密协议；
i) 制定数据安全服务流程。

J.1.3 方案设计阶段

a) 根据服务对象的数据安全目标及业务现状，编制《数据安全服务方案》，方案内容包含但不限于项目目标、服务对象、服务内容、实施方法、实施流程、服务工具、服务人员安排、实施计划、项目管理、交付物等；
b) 结合《数据安全服务方案》，与客户进行沟通，获得客户认可。

J.1.4 实施阶段

a) 根据国家或行业数据资产分类分级标准识别数据资产，对数据资产进行分类和分级管理；
b) 应对生成/采集的数据进行数据分类分级的标识，内容包含但不限于数据分布管理、数据分类管理、敏感数据管理、敏感数据访问管理、数据账号权限管理等；
c) 应识别数据资产的脆弱性和威胁，以及现有防护措施；
d) 根据相关法规、标准要求，提供数据安全管理制度检查、数据库安全配置核查、数据库漏洞扫描等服务；

e） 编制配置核查及漏洞问题清单，提出加固整改建议；
f） 对数据库进行加固，如修正数据库配置、修复数据库漏洞补丁、建立配置清单、提供漏洞情况信息等；
g） 协助服务对象编写数据安全管理制度，包含但不限于数据安全方针、数据安全岗位职责规范、数据安全管理办法、数据安全系列技术规范；
h） 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；
i） 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，提交数据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，以及数据安全服务过程中发现和问题等。

J.1.5 验收阶段

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） 验收报告中应描述数据在验收时的运行状况，以及客户单位的反馈意见。

J.2 二级要求

J.2.1 基本要求

J.2.1.1 业绩要求

近三年内签订并完成至少2个数据安全服务项目，维持资格最少完成1个数据安全服务项目。

J.2.1.2 专业工具

a） 具有必要的专业检测工具；
b） 应对技术工具进行管理，定期进行跟踪、检查技术工具的状态，并建立对技术工具的测量历史记录。

J.2.2 准备阶段

a） 了解数据所有者的组织架构、数据安全的管理机制；
b） 识别客户对数据安全管理和技术服务的目标和需求；
c） 调研客户信息系统业务情况、数据库类型、数据库部署环境、数据库最大并发量、单个数据库表的数量、数据条数、数据库事务数、数据库访问量、数据库访问方式等；
d） 识别影响数据安全服务的法律、政策、标准、外部影响和约束条件；
e） 识别客户实际环境中，数据面临的潜在安全威胁，分析服务过程中可能产生的安全风险；
f） 编制完整的数据生命周期各阶段安全防护现状的调研报告，调研的内容包括但不限于组织架构、制度列表、业务流程、数据库类型、数据库架构、数据访问方式、数据现有防护措施、管理人员信息等；
g） 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；
h） 服务人员签订保密协议；
i） 制定数据安全服务流程；
j） 调研客户数据采集、传输、存储、处理、交换、销毁等阶段的安全防护现状。

J.2.3 方案设计阶段

a) 根据服务对象的数据安全目标及业务现状，编制《数据安全服务方案》，方案内容包含但不限于项目目标、服务对象、服务内容、实施方法、实施流程、服务工具、服务人员安排、实施计划、项目管理、交付物、项目质量管控、风险规避措施；
b) 结合《数据安全服务方案》，与客户进行沟通，获得客户认可；
c) 结合项目需要，编制安全服务项目施工手册和作业指导书；
d) 应制定《风险分析报告》模版，内容包含但不限于威胁库、脆弱点库、风险级别、风险处理、重要数据资产、资产值、威胁值、弱点值、风险值等；
e) 应制定《数据安全风险评估报告》，内容应当包括处理的重要数据的种类、数量，开展数据处理活动的情况，面临的数据安全风险及其应对措施等。

J.2.4 实施阶段

a) 根据国家或行业数据资产分类分级标准识别数据资产，对数据资产进行分类和分级管理；
b) 应对生成/采集的数据进行数据分类分级的标识，内容包含但不限于数据分布管理、数据分类管理、敏感数据管理、敏感数据访问管理、数据账号权限管理等；
c) 应识别数据采集、数据传输、数据存储、数据处理、数据交换、数据销毁等数据全生命周期的脆弱性和威胁，以及现有防护措施；
d) 根据相关法规、标准要求，检查数据安全管理制度、数据库安全配置核查、数据库漏洞扫描等；
e) 编制配置核查及漏洞问题清单，提出加固建议；
f) 对数据库进行加固，如修正数据库配置、修复数据库漏洞补丁、建立配置清单、提供漏洞情况信息等；
g) 协助服务对象编写数据安全管理制度，包含但不限于数据安全方针、数据安全岗位职责规范、数据安全管理办法、数据安全系列技术规范；
h) 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；
i) 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，提交数据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，以及数据安全服务过程中发现和问题等；
j) 应识别数据采集安全风险，包括采集终端接入安全风险、数据采集范围安全风险、采集数据真实性风险、敏感数据采集风险、采集数据安全传输风险、采集数据缓存安全风险、异常采集行为告警等，并形成风险分析报告；
k) 应识别数据传输安全风险，并形成风险分析报告；
l) 应识别数据存储安全风险，包括数据加密存储安全风险、存储空间隔离安全风险、数据残留与销毁安全风险、数据存储访问控制安全风险、数据封装、数据备份与恢复安全风险、数据完整性保护机制风险等，并形成风险分析报告；
m) 应识别数据处理安全风险，包括数据批处理环境安全性、数据交互式处理环境安全性、数据流处理环境安全性、敏感数据标记、敏感数据处理安全性、数据使用访问控制等，并形成风险分析报告；
n) 应识别数据交换安全风险，包括数据共享安全、数据发布安全、数据交换监控等，并形成风险分析报告；
o) 应识别数据销毁安全风险，包括介质使用管理、数据销毁处理、介质销毁处理等，并形成风险分析报告；

p) 应识别数据供应链管理风险，包括数据供应链管理机制、数据服务接口管理机制等，并形成风险分析报告；
q) 结合上述数据安全管理、数据资产、脆弱性和威胁等问题列表，采取定性或定量的方式分析数据安全风险，形成数据安全风险评估报告，风险评估报告应当包括处理的重要数据的种类、数量，开展数据处理活动的情况，面临的数据安全风险及其应对措施等。

J.2.5 验收阶段

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) 验收报告中应描述数据在验收时的运行状况，以及客户单位的反馈意见。

J.3 三级要求

J.3.1 基本要求

J.3.1.1 业绩要求

近三年内签订并完成至少6个数据安全相关项目，维持资格最少完成1个数据安全服务项目。

J.3.1.2 专业工具

a) 具有必要的专业检测工具；
b) 应对技术工具进行管理， 定期进行跟踪、检查技术工具的状态，并建立对技术工具的测量历史记录。

J.3.2 准备阶段

a) 了解数据所有者的组织架构、数据安全的管理机制；
b) 识别客户对数据安全管理和技术服务的目标和需求；
c) 调研客户信息系统业务情况、数据库类型、数据库部署环境、数据库最大并发量、单个数据库表的数量、数据条数、数据库事务数、数据库访问量、数据库访问方式等；
d) 识别影响数据安全服务的法律、政策、标准、外部影响和约束条件；
e) 识别客户实际环境中，数据面临的潜在安全威胁，分析服务过程中可能产生的安全风险；
f) 编制完整的数据生命周期各阶段安全防护现状的调研报告，调研的内容包括但不限于组织架构、制度列表、业务流程、数据库类型、数据库架构、数据访问方式、数据现有防护措施、管理人员信息等；
g) 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；
h) 服务人员签订保密协议；
i) 制定数据安全服务流程；
j) 调研客户数据采集、传输、存储、处理、交换、销毁等阶段的安全防护现状；
k) 制定数据安全服务规范。

J.3.3 方案设计阶段

a) 根据服务对象的数据安全目标及业务现状，编制《数据安全服务方案》，方案内容包含但不限于项目目标、服务对象、服务内容、实施方法、实施流程、服务工具、服务人员安排、实施计划、项目管理、交付物、项目质量管控、风险规避措施；

b) 结合《数据安全服务方案》，与客户进行沟通，获得客户认可；
c) 结合项目需要，编制安全服务项目施工手册和作业指导书；
d) 应制定《风险分析报告》模版，内容包含但不限于威胁库、脆弱点库、风险级别、风险处理、重要数据资产、资产值、威胁值、弱点值、风险值等；
e) 应制定《数据安全风险评估报告》，内容应当包括处理的重要数据的种类、数量，开展数据处理活动的情况，面临的数据安全风险及其应对措施等；
f) 制定针对人员、设备、文档、系统的风险监控措施，有效保障数据的安全、稳定；
g) 应围绕着数据生命周期从组织建设、制度流程、技术工具和人员能力四个纬度进行数据安全规划设计，形成《数据安全治理方案》，且应经过评审，并与客户达成一；
h) 应制定《数据业务规划与管理方案》，包括战略规划、需求分析、元数据安全等；
i) 应制定《合规性管理方案》，包括个人信息保护、重要数据保护、数据跨境传输、密码支持等；
j) 为服务对象定义标准化的过程文档，并按照标准化文档建立数据安全相关制度。

J.3.4 实施阶段

a) 根据国家或行业数据资产分类分级标准识别数据资产，对数据资产进行分类和分级管理；
b) 应对生成/采集的数据进行数据分类分级的标识，内容包含但不限于数据分布管理、数据分类管理、敏感数据管理、敏感数据访问管理、数据账号权限管理等；
c) 应识别数据采集、数据传输、数据存储、数据处理、数据交换、数据销毁等数据全生命周期的脆弱性和威胁，以及现有防护措施；
d) 根据相关法规、标准要求，提供检查数据安全管理制度、数据库安全配置核查、数据库漏洞扫描等；
e) 编制配置核查及漏洞问题清单，提出加固建议；
f) 对数据库进行加固，如修正数据库配置、修复数据库漏洞补丁、建立配置清单、提供漏洞情况信息等；
g) 协助服务对象编写数据安全管理制度，包含但不限于数据安全方针、数据安全岗位职责规范、数据安全管理办法、数据安全系列技术规范；
h) 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；
i) 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，提交数据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，以及数据安全服务过程中发现和问题等；
j) 应识别数据采集安全风险，包括采集终端接入安全风险、数据采集范围安全风险、采集数据真实性风险、敏感数据采集风险、采集数据安全传输风险、采集数据缓存安全风险、异常采集行为告警等，并形成风险分析报告；
k) 应识别数据传输安全风险，并形成风险分析报告；
l) 应识别数据存储安全风险，包括数据加密存储安全风险、存储空间隔离安全风险、数据残留与销毁安全风险、数据存储访问控制安全风险、数据封装、数据备份与恢复安全风险、数据完整性保护机制风险等，并形成风险分析报告；
m) 应识别数据处理安全风险，包括数据批处理环境安全性、数据交互式处理环境安全性、数据流处理环境安全性、敏感数据标记、敏感数据处理安全性、数据使用访问控制等，并形成风险分析报告；

n) 应识别数据交换安全风险，包括数据共享安全、数据发布安全、数据交换监控等，并形成风险分析报告；
o) 应识别数据销毁安全风险，包括介质使用管理、数据销毁处理、介质销毁处理等，并形成风险分析报告；
p) 应识别数据供应链管理风险，包括数据供应链管理机制、数据服务接口管理机制等，并形成风险分析报告；
q) 结合上述数据安全管理、数据资产、脆弱性和威胁等问题列表，采取定性或定量的方式分析数据安全风险，形成数据安全风险评估报告，风险评估报告应当包括处理的重要数据的种类、数量，开展数据处理活动的情况，面临的数据安全风险及其应对措施等；
r) 协助客户进行风险处置，必要时，对残余风险进行再评估，形成残余风险评估报告，内容不限于残余风险类别、关联关系、风险级别、处置措施等；
s) 应对数据安全风险进行管控及分析，内容不限于数据采集风险监测、数据传输风险监测、数据存储风险监测、数据交换风险监测、数据销毁风险监测、特权账号风险分析、异常行为风险分析、数据流程风险分析、数据资产威胁分析等，形成对应的分析报告；
t) 应定期开展数据安全应急响应及演练工作，形成数据安全应急预案、演练方案、演练报告与记录、处理应急安全事件等；
u) 能够对发生的数据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，形成事件分析报告；
v) 对数据安全事件管理，包括数据安全事件定级，数据安全事件处置，处置事件展示与管理，以及原始事件的日志检索等，安全事件处理记录应具备可追溯性；
w) 按《数据安全治理方案》实施部署相关技术产品。包含但不限于数据安全审计、数据安全访问控制、数据脱敏、数据库安全运维管控、数据存储加密、数据传输加密、数据防泄漏等。形成对应的实施方案、实施计划、实施规范、实施流程、通电测试报告、策略清单、设备列表；（可参考“安全集成服务专业能力评价”的交付要求）；
x) 对国内外主流数据库及数据安全防护设备的安全配置和漏洞补丁进行加固修复，并形成配置清单、提供漏洞情况信息等；
y) 识别数据处理过程的动态数据资产，包含但不限于数据库实例、数据库、数据表、视图、表结构、字段、存储过程、触发器、数据库账号在内的数据资产；
z) 对国内外主流的数据安全审计、数据库防火墙、数据脱敏、数据库运维管控、数据加密等数据安全防护系统进行安全策略的优化；
aa) 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，提交数据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，以及数据安全服务过程中发现问题等；
bb) 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。

J.3.5 验收阶段

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) 验收报告中应描述数据在验收时的运行状况，以及客户单位的反馈意见。

J.4 四级要求

J.4.1 基本要求

J.4.1.1 业绩要求

近三年内签订并完成至少10个数据安全相关项目，维持资格最少完成1个数据安全服务项目。

J.4.1.2 专业工具

a) 具有必要的专业检测工具；
b) 应对技术工具进行管理，定期进行跟踪、检查技术工具的状态，并建立对技术工具的测量历史记录；
c) 具有自主开发的检查工具。

J.4.2 准备阶段

a) 了解数据所有者的组织架构、数据安全的管理机制；
b) 识别客户对数据安全管理和技术服务的目标和需求；
c) 调研客户信息系统业务情况、数据库类型、数据库部署环境、数据库最大并发量、单个数据库表的数量、数据条数、数据库事务数、数据库访问量、数据库访问方式等；
d) 识别影响数据安全服务的法律、政策、标准、外部影响和约束条件；
e) 识别客户实际环境中，数据面临的潜在安全威胁，分析服务过程中可能产生的安全风险；
f) 编制完整的数据生命周期各阶段安全防护现状的调研报告，调研的内容包括但不限于组织架构、制度列表、业务流程、数据库类型、数据库架构、数据访问方式、数据现有防护措施、管理人员信息等；
g) 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；
h) 服务人员签订保密协议；
i) 制定数据安全服务流程；
j) 调研客户数据收集、存储、使用、加工、传输、提供、公开等阶段的安全防护现状；
k) 制定数据安全服务规范。

J.4.3 方案设计阶段

a) 根据服务对象的数据安全目标及业务现状，编制《数据安全服务方案》，方案内容包含但不限于项目目标、服务对象、服务内容、实施方法、实施流程、服务工具、服务人员安排、实施计划、项目管理、交付物、项目质量管控、风险规避措施；
b) 结合《数据安全服务方案》，与客户进行沟通，获得客户认可；
c) 结合项目需要，编制安全服务项目施工手册和作业指导书；
d) 制定《风险分析报告》模版，内容包含但不限于威胁库、脆弱点库、风险级别、风险处理、重要数据资产、资产值、威胁值、弱点值、风险值等；
e) 制定《数据安全风险评估报告》，内容应当包括处理的重要数据的种类、数量，开展数据处理活动的情况，面临的数据安全风险及其应对措施等；
f) 制定针对人员、设备、文档、系统的风险监控措施，有效保障数据的安全、稳定；
g) 应围绕着数据生命周期从组织建设、制度流程、技术工具和人员能力四个纬度进行数据安全规划设计，形成《数据安全治理方案》，且应经过评审，并与客户达成一；

h) 应制定《数据业务规划与管理方案》，包括战略规划、需求分析、元数据安全等；
i) 应制定《合规性管理方案》，包括个人信息保护、重要数据保护、数据跨境传输、密码支持等；
j) 为服务对象定义标准化的过程文档，并按照标准化文档建立数据安全相关制度；
k) 应编制数据采集安全方案，包括数据收集和获取、数据清洗/转换与加载、数据质量监控、数据传输安全；
l) 应编制数据传输安全方案，利用加密、签名、鉴别和认证等机制对数据传输进行安全管理，防止数据遭泄漏和篡改；
m) 应编制数据存储安全方案，包括存储架构、逻辑存储、访问控制、数据副本、数据归档、数据时效性；
n) 应编制数据销毁安全方案，包括介质使用管理、数据销毁处置、介质销毁处置；
o) 应编制数据处理安全方案，包括分布式处理安全、数据分析安全、数据正当使用、密文数据处理、数据脱敏处理、数据溯源；
p) 应编制数据交换安全方案，包括数据导入导出安全、数据共享安全、数据发布安全、数据交换监控；
q) 应编制数据供应链管理方案，包括数据供应链、数据服务接口；
r) 应制定实施过程的《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。

J.4.4 实施阶段

a) 根据国家或行业数据资产分类分级标准识别数据资产，对数据资产进行分类和分级管理；
b) 应对生成/采集的数据进行数据分类分级的标识，内容包含但不限于数据分布管理、数据分类管理、敏感数据管理、敏感数据访问管理、数据账号权限管理等；
c) 应识别数据采集、数据传输、数据存储、数据处理、数据交换、数据销毁等数据全生命周期的脆弱性和威胁，以及现有防护措施；
d) 根据相关法规、标准要求，检查数据安全管理制度、数据库安全配置核查、数据库漏洞扫描等；
e) 编制配置核查及漏洞问题清单，提出加固建议；
f) 对数据库进行加固，如修正数据库配置、修复数据库漏洞补丁、建立配置清单、提供漏洞情况信息等；
g) 协助服务对象编写数据安全管理制度，包含但不限于数据安全方针、数据安全岗位职责规范、数据安全管理办法、数据安全系列技术规范；
h) 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；
i) 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，提交数据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，以及数据安全服务过程中发现和问题等；
j) 应识别数据采集安全风险，包括采集终端接入安全风险、数据采集范围安全风险、采集数据真实性风险、敏感数据采集风险、采集数据安全传输风险、采集数据缓存安全风险、异常采集行为告警等，并形成风险分析报告；
k) 应识别数据传输安全风险，并形成风险分析报告；
l) 应识别数据存储安全风险，包括数据加密存储安全风险、存储空间隔离安全风险、数据残留

与销毁安全风险、数据存储访问控制安全风险、数据封装、数据备份与恢复安全风险、数据完整性保护机制风险等，并形成风险分析报告；

m) 应识别数据处理安全风险，包括数据批处理环境安全性、数据交互式处理环境安全性、数据流处理环境安全性、敏感数据标记、敏感数据处理安全性、数据使用访问控制等，并形成风险分析报告；

n) 应识别数据交换安全风险，包括数据共享安全、数据发布安全、数据交换监控等，并形成风险分析报告；

o) 应识别数据销毁安全风险，包括介质使用管理、数据销毁处理、介质销毁处理等，并形成风险分析报告；

p) 应识别数据供应链管理风险，包括数据供应链管理机制、数据服务接口管理机制等，并形成风险分析报告；

q) 结合上述数据安全管理、数据资产、脆弱性和威胁等问题列表，采取定性或定量的方式分析数据安全风险，形成数据安全风险评估报告，风险评估报告应当包括处理的重要数据的种类、数量，开展数据处理活动的情况，面临的数据安全风险及其应对措施等；

r) 协助客户进行风险处置，必要时，对残余风险进行再评估，形成残余风险评估报告，内容不限于残余风险类别、关联关系、风险级别、处置措施等；

s) 应对数据安全风险进行管控及分析，内容不限于数据采集风险监测、数据传输风险监测、数据存储风险监测、数据交换风险监测、数据销毁风险监测、特权账号风险分析、异常行为风险分析、数据流程风险分析、数据资产威胁分析等，形成对应的分析报告；

t) 应定期开展数据安全应急响应及演练工作，形成数据安全应急预案、演练方案、演练报告与记录、处理应急安全事件等；

u) 能够对发生的数据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，形成事件分析报告；

v) 对数据安全事件管理，包括数据安全事件定级，数据安全事件处置，处置事件展示与管理，以及原始事件的日志检索等，安全事件处理记录应具备可追溯性；

w) 按《数据安全治理方案》实施部署相关技术产品。包含但不限于数据安全审计、数据安全访问控制、数据脱敏、数据库安全运维管控、数据存储加密、数据传输加密、数据防泄漏等。形成对应的实施方案、实施计划、实施规范、实施流程、通电测试报告、策略清单、设备列表。（可参考“安全集成服务专业能力评价”的交付要求）；

x) 对国内外主流数据库及数据安全防护设备的安全配置和漏洞补丁进行加固修复，并形成配置清单、提供漏洞情况信息等；

y) 识别数据处理过程的动态数据资产，包含但不限于数据库实例、数据库、数据表、视图、表结构、字段、存储过程、触发器、数据库账号在内的数据资；

z) 对国内外主流的数据安全审计、数据库防火墙、数据脱敏、数据库运维管控、数据加密等数据安全防护系统进行安全策略的优化；

aa) 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，提交数据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，以及数据安全服务过程中发现问题等；

bb) 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；

cc) 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；
dd) 应具备根据数据资产的敏感性变化，优化调整数据收集、数据存储、数据使用、数据加工、数据传输、数据提供、数据公开等阶段数据安全策略的能力；
ee) 应能够对数据安全未知威胁进行态势感知，不限于通过基于数据库日志、业务日志、访问日志、流量等信息进行大数据分析，为服务对象获取数据安全风险和态势；
ff) 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；
gg) 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；
hh) 建立服务过程质量监控机制，监督数据安全服务实施的过程，定期开展数据安全服务质量检查。

J.4.5 验收阶段

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) 验收报告中应描述数据在验收时的运行状况，以及客户单位的反馈意；
d) 应建立变更程序，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。

附 录 K
（规范性）
工业控制系统安全服务专业能力评价要求

K.1 一级要求

K.1.1 基本要求

K.1.1.1 业绩要求

首次申请不做要求，维持资格最少完成1个工业控制系统安全服务项目。

K.1.1.2 专业能力要求

a） 制定工业控制系统安全服务流程；
b） 制定工业控制系统安全服务规范标准。

K.1.1.3 人员和专用工具要求

a） 根据服务项目的目标、内容、范围等组建项目团队；
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，即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；
c） 根据服务内容的需求准备必要的工具。

K.1.2 准备阶段

a） 编制业务情况和工业控制系统调研表，并按照调研表收集有效信息；
b） 调研工业企业的组织结构、了解对工业控制系统的管理机制；
c） 识别客户对工业控制系统安全管理和技术服务的目标和需求、工业控制系统面临的潜在威胁；
d） 调研客户工业控制系统的业务逻辑、工作流程、设备组成、网络架构；
e） 识别影响工业控制系统服务的法律、政策、标准、外部影响和约束条件，了解所属行业主管部门对工业控制系统安全要求；
f） 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；
g） 编制完整的调研报告，调研的内容包括但不限于目标、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；
h） 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；
i） 对团队成员进行安全教育、信息安全服务技能、工业控制系统业务知识和工业控制系统操作章程培训。

K.1.3 方案设计阶段

a） 结合调研情况，编制安全服务技术方案，方案内容包含安全需求、工作内容、服务方式等；
b） 结合技术方案，编制实施方案，方案内容包含服务范围、目标、人员安排、进度、内容、质量管理、沟通和风险等。

K.1.4 实施阶段

a) 识别工业控制系统重要资产以及资产的安全配置；
b) 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；
c) 收集和分析工业控制系统的硬件故障及安全事件；
d) 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；
e) 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，并采取有效措施避免安全风险，形成对应问题清单；
f) 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。

K.1.5 运行测试阶段

a) 制定系统测试方案，对工业控制系统进行功能和性能检测，确认系统运行的可靠性和稳定性，并记录系统运行状况；
b) 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) 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；
d) 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；
e) 应形成和保存工业控制系统的状态和防护情况记录，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；
f) 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。

K.1.6 验收阶段

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。

K.2 二级要求

K.2.1 基本要求

K.2.1.1 业绩要求

近三年内签订并完成至少3个工业控制系统安全服务项目，维持资格最少完成1个工业控制系统安全服务项目。

K.2.1.2 专业能力要求

a) 制定工业控制系统安全服务流程；
b) 制定工业控制系统安全服务规范标准。

K.2.1.3 人员和专用工具要求

a) 应根据服务项目的目标、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，即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；

c） 根据服务内容的需求准备必要的工具。

K.2.2 准备阶段

a） 编制业务情况和工业控制系统调研表，并按照调研表收集有效信息；
b） 调研工业企业的组织结构、了解对工业控制系统的管理机制；
c） 识别客户对工业控制系统安全管理和技术服务的目标和需求、工业控制系统面临的潜在威胁；
d） 调研客户工业控制系统的业务逻辑、工作流程、设备组成、网络架构等；
e） 识别影响工业控制系统服务的法律、政策、标准、外部影响和约束条件，了解所属行业主管部门对工业控制系统安全要求；
f） 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；
g） 编制完整的调研报告，调研的内容包括但不限于目标、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；
h） 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；
i） 对团队成员进行安全教育、信息安全服务技能、工业控制系统业务知识和工业控制系统操作章程培训；
j） 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。

K.2.3 方案设计阶段

a） 结合调研情况，编制安全服务技术方案，方案内容包含安全需求、工作内容、服务方式等；
b） 结合技术方案，编制实施方案，方案内容包含服务范围、目标、人员安排、进度、内容、质量管理、沟通和风险等；
c） 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。

K.2.4 实施阶段

a） 识别工业控制系统重要资产以及资产的安全配置；
b） 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；
c） 收集和分析工业控制系统的硬件故障及安全事件；
d） 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；
e） 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，并采取有效措施避免安全风险，形成对应问题清单；
f） 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；
g） 编制服务过程中发现的工业控制系统安全风险列表；
h） 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；
i） 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。

K.2.5 运行测试阶段

a) 制定系统测试方案，对工业控制系统进行功能和性能检测，确认系统运行的可靠性和稳定性， 并记录系统运行状况；
b) 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) 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；
d) 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；
e) 应形成和保存工业控制系统的状态和防护情况记录，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；
f) 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；
g) 建立报告的批准和交付程序，保留交付记录。

K.2.6 验收阶段

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。

K.3 三级要求

K.3.1 基本要求

K.3.1.1 业绩要求

近三年内签订并完成至少6个工业控制系统安全服务项目，维持资格最少完成1个工业控制系统安全服务项目。

K.3.1.2 专业能力要求

a) 制定工业控制系统安全服务流程；
b) 制定工业控制系统安全服务规范标准；
c) 具备工业控制系统漏洞挖掘能力，并向CNVD或CNNVD提交过1个以上的漏洞。

K.3.1.3 人员和专用工具要求

a) 根据服务项目的目标、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，即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；
c) 根据服务内容的需求准备必要的工具；
d) 搭建临时模拟环境，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。

K.3.2 准备阶段

a) 编制业务情况和工业控制系统调研表，并按照调研表收集有效信息；
b) 调研工业企业的组织结构、了解对工业控制系统的管理机制；
c) 识别客户对工业控制系统安全管理和技术服务的目标和需求、工业控制系统面临的潜在威

胁；

d) 调研客户工业控制系统的业务逻辑、工作流程，设备组成、网络架构等；

e) 识别影响工业控制系统服务的法律、政策、标准、外部影响和约束条件，了解所属行业主管部门对工业控制系统安全要求；

f) 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；

g) 编制完整的调研报告，调研的内容包括但不限于目标、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；

h) 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；

i) 对团队成员进行安全教育、信息安全服务技能、工业控制系统业务知识和工业控制系统操作章程培训；

j) 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；

k) 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。

K.3.3 方案设计阶段

a) 结合调研情况，编制安全服务技术方案，方案内容包含安全需求、工作内容、服务方式等；

b) 结合技术方案，编制实施方案，方案内容包含服务范围、目标、人员安排、进度、内容、质量管理、沟通和风险等；

c) 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；

d) 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。

K.3.4 实施阶段

a) 识别工业控制系统重要资产以及资产的安全配置；

b) 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；

c) 收集和分析工业控制系统的硬件故障及安全事件；

d) 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；

e) 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，并采取有效措施避免安全风险，形成对应问题清单；

f) 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；

g) 编制服务过程中发现的工业控制系统安全风险列表；

h) 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；

i) 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；

j) 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；

k) 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的消缺情况。

K.3.5 运行测试阶段

a) 制定系统测试方案，对工业控制系统进行功能和性能检测，确认系统运行的可靠性和稳定性，并记录系统运行状况；
b) 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) 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；
d) 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；
e) 应形成和保存工业控制系统的状态和防护情况记录，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；
f) 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；
g) 建立报告的批准和交付程序，保留交付记录；
h) 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；
i) 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。

K.3.6 验收阶段

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；
d) 建立变更程序，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；
e) 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。

K.4 四级要求

K.4.1 基本要求

K.4.1.1 业绩要求

近三年内签订并完成至少10个工业控制系统安全服务项目，维持资格最少完成1个工业控制系统安全服务项目。

K.4.1.2 专业能力要求

a) 制定工业控制系统安全服务流程；
b) 制定工业控制系统安全服务规范标准；
c) 具备工业控制系统漏洞挖掘能力，并向CNVD或CNNVD提交过3个以上的漏洞；
d) 建立应急保障团队，及时响应客户需求；
e) 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。

K.4.1.3 人员和专用工具要求

a) 根据服务项目的目标、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，即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；
c） 根据服务内容的需求准备必要的工具；
d） 搭建临时模拟环境，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；
e） 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；
f） 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。

K.4.2 准备阶段

a） 编制业务情况和工业控制系统调研表，并按照调研表收集有效信息；
b） 调研工业企业的组织结构、了解对工业控制系统的管理机制；
c） 识别客户对工业控制系统安全管理和技术服务的目标和需求、工业控制系统面临的潜在威胁；
d） 调研客户工业控制系统的业务逻辑、工作流程，设备组成、网络架构等；
e） 识别影响工业控制系统服务的法律、政策、标准、外部影响和约束条件，了解所属行业主管部门对工业控制系统安全要求；
f） 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；
g） 编制完整的调研报告，调研的内容包括但不限于目标、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；
h） 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；
i） 对团队成员进行安全教育、信息安全服务技能、工业控制系统业务知识和工业控制系统操作章程培训；
j） 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；
k） 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。

K.4.3 方案设计阶段

a） 结合调研情况，编制安全服务技术方案，方案内容包含安全需求、工作内容、服务方式等；
b） 结合技术方案，编制实施方案，方案内容包含服务范围、目标、人员安排、进度、内容、质量管理、沟通和风险等；
c） 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；
d） 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；
e） 结合项目需要，编制安全服务项目施工手册和作业指导书；
f） 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。

K.4.4 实施阶段

a） 识别工业控制系统重要资产以及资产的安全配置；
b） 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；

c) 收集和分析工业控制系统的硬件故障及安全事件；
d) 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；
e) 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，并采取有效措施避免安全风险，形成对应问题清单；
f) 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；
g) 编制服务过程中发现的工业控制系统安全风险列表；
h) 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；
i) 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；
j) 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；
k) 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的消缺情况；
l) 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；
m) 综合分析系统运行状况，制定安全运维、应急响应方案。

K.4.5 运行测试阶段

a) 制定系统测试方案，对工业控制系统进行功能和性能检测，确认系统运行的可靠性和稳定性，并记录系统运行状况；
b) 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) 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；
d) 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；
e) 应形成和保存工业控制系统的状态和防护情况记录，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；
f) 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；
g) 建立报告的批准和交付程序，保留交付记录；
h) 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；
i) 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；
j) 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；
k) 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。

K.4.6 验收阶段

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；

d) 建立变更程序，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；

e) 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。

附 录 L
（规范性）
云计算安全服务专业能力评价要求

L.1 一级要求

L.1.1 基础能力要求

a) 具有专业的服务团队，确定项目负责人和安全服务负责人，其中项目负责人和安全服务负责人应具备2年以上网络空间安全服务领域工作经历，安全负责人具有相应安全资质；
b) 首次申请不做要求，维持资格最少完成1个云计算安全服务项目；
c) 具备本地12小时、外地24小时应急响应服务能力；
d) 应提供云计算安全服务完整解决方案，制定持续改进计划并实施。

L.1.2 云计算安全技术要求

L.1.2.1 安全运营技术

a) 具备身份鉴别能力，即基于口令认证的方式对登录云计算平台或应用系统的云用户进行身份鉴别的能力；
b) 具备授权管理能力，即基于主体角色的授权机制，基于主体角色授权的访问控制能力；
c) 具备安全审计能力，即建立操作日志能力，能记录对信息采集、传输、存储、使用等处理环节的操作日志，日志内容包括但不限于：时间、IP地址、用户ID、操作内容、操作对象等；
d) 具备实时监控和可视化展示能力，即对云基础设施、安全设备、业务应用运行状态等进行实时监控以及以可视化方式展示；
e) 具备安全漏洞和补丁管理能力，即发现云资产安全漏洞的能力，并能对云资产补丁信息进行获取和管理的能力；
f) 具备安全事件分析和告警的能力，即结合威胁情报信息进行安全事件分析、确认的能力；对威胁事件、安全事件内容可以使用但不限于短信、邮件、工单等方式进行告警发送。

L.1.2.2 安全防护技术

a) 具备入侵检测能力、实时监测能力、被动响应能力；
b) 具备云计算环境下的风险评估能力；
c) 具备数据备份与恢复能力，即应具备定期执行云上数据备份及恢复、实现存储数据的冗余、保护数据的可用性的能力。

L.1.3 云计算安全管理要求

L.1.3.1 安全策略

a) 建立云计算安全服务流程，确保流程合规，满足相关法律法规要求；
b) 建立云计算安全服务规范。

L.1.3.2 组织人员

a) 制定安全团队管理流程，设立安全管理员、安全审计员、数据安全员等负责人岗位，明确安全团队的职责以及能力要求；
b) 定期开展针对各岗位人员与安全相关的管理规范、流程、制度、技能培训，并进行考核。

L.1.3.3 云资产管理

a) 应确保云IT资产合规性，对于资产数据进行不同方式展现；
b) 应具备批量对于IT设备进行升级、加固等操作的能力；
c) 应制定云资产清单，包括资产类别、资产内容、资产位置、资产用途、资产级别、资产负责人等内容。

L.1.4 云计算运营管理

a) 建立相关的安全岗位及职责，制定并发布相关安全管理体系，对运营流程进行管理；
b) 明确相应流程节点中的相关人员的职责关系，确定在各流程节点中对应工作要求的责任人员的工作内容和配合方式，并形成相应记录。

L.1.5 合规性管理

a) 建立符合网络安全法等法律法规的云安全策略、规范、制度和管控措施；
b) 建立管控措施和采用相关的技术手段，避免因人工管理模式改变或机构业务重组等方式而规避重要数据保护要求。

L.1.6 安全评估

a) 具备对云计算环境下的运营资产安全风险评估的能力，评估应包括但不限于系统安全评估和网络安全评估；
b) 系统安全评估应至少包括配置核查、漏洞核查和补丁核查等评估内容；
c) 网络安全评估应至少包含网络访问控制评估、入侵检测评估等评估内容。

L.1.7 应急管理

a) 明确相关安全事件的应急响应要求；
b) 制定应急响应处置流程。

L.1.8 安全监管

a) 对于制定的云服务安全运营、安全防护、安全管理要求，监管其落实情况；
b) 对发现的问题、识别的风险，应进行督促整改。

L.2 二级要求

L.2.1 基础能力要求

a) 具有专业的服务团队，确定项目负责人和安全服务负责人，其中项目负责人和安全服务负责人应具备3年以上网络空间安全服务领域工作经历，安全负责人具有相应安全资质；
b) 近三年内至少有2个云计算安全服务项目，工程按合同要求质量合格，已通过验收，维持资格最少完成1个云计算安全服务项目；
c) 具备本地12小时、外地24小时应急响应服务能力；
d) 应提供云计算安全服务完整解决方案，制定持续改进计划并实施。

L.2.2 云计算安全技术要求

L.2.2.1 安全运营技术

a) 具备身份鉴别能力，即基于口令认证的方式对登录云计算平台或应用系统的云用户进行身份鉴别的能力；
b) 具备授权管理能力，即基于主体角色的授权机制，基于主体角色授权的访问控制能力；
c) 具备安全审计能力，即建立操作日志能力，能记录对信息采集、传输、存储、使用等处理环节的操作日志，日志内容包括但不限于：时间、IP地址、用户ID、操作内容、操作对象等；
d) 具备实时监控和可视化展示能力，即对云基础设施、安全设备、业务应用运行状态等进行实时监控以及以可视化方式展示；
e) 具备安全漏洞和补丁管理能力，即发现云资产安全漏洞的能力，并能对云资产补丁信息进行获取和管理的能力；
f) 具备安全事件分析和告警的能力，即结合威胁情报信息进行安全事件分析、确认的能力；对威胁事件、安全事件内容可以使用但不限于短信、邮件、工单等方式进行告警发送；
g) 具备自动化响应与通知的能力，即针对安全事件、应急事件等进行自动化响应与通知的措施。

L.2.2.2 安全防护技术

a) 具备入侵检测能力、实时监测能力、被动响应能力；
b) 具备云计算环境下的风险评估能力；
c) 具备数据备份与恢复能力，即应具备定期执行云上数据备份及恢复、实现存储数据的冗余、保护数据的可用性的能力，应能够对重要信息进行备份和恢复，应查验关键网络设备、通信线路和数据处理系统的硬件冗余，保证系统的可用性；
d) 应有能力通过设置升级服务器等方式保持系统补丁及时得到更新；
e) 具备恶意代码防范能力，即应安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库；
f) 具备确保数据完整性和一致性检测的能力，即应能够检测到鉴别信息和重要业务数据在传输、存储等过程中完整性或一致性受到破坏；
g) 应同时具备威胁情报分析与利用能力、主动应急响应能力。

L.2.3 云计算安全管理要求

L.2.3.1 安全策略

a) 建立云计算安全服务流程，确保流程合规，满足相关法律法规要求；
b) 建立云计算安全服务规范。

L.2.3.2 组织人员

a) 制定安全团队管理流程，设立安全管理员、安全审计员、数据安全员等负责人岗位，明确安全团队的职责以及能力要求；
b) 定期开展针对各岗位人员与安全相关的管理规范、流程、制度、技能培训，并进行考核；
c) 具备攻击防御团队（蓝方）和攻击模拟团队（红方）。

L.2.3.3 云资产管理

a) 应确保云IT资产合规性，对于资产数据进行不同方式展现；
b) 应具备批量对于IT设备进行升级、加固等操作的能力；
c) 应制定云资产清单，包括资产类别、资产内容、资产位置、资产用途、资产级别、资产负责人等内容；
d) 具备按重要程度对云资产进行标识的能力，规定云资产分类标识的原则和方法，对不同重要程度资产实施分级管理策略。如根据信息的重要程度、敏感程度或用途不同进行分类。

L.2.4 云计算运营管理

a) 建立相关的安全岗位及职责，制定并发布相关安全管理体系，对运营流程进行管理；
b) 明确相应流程节点中的相关人员的职责关系，确定在各流程节点中对应工作要求的责任人员的工作内容和配合方式，并形成相应记录；
c) 对云计算资源共享申请和相关操作进行安全审核，确保共享过程的规范性和安全性。

L.2.5 合规性管理

a) 建立符合网络安全法等法律法规的云安全策略、规范、制度和管控措施；
b) 建立管控措施和采用相关的技术手段，避免因人工管理模式改变或机构业务重组等方式而规避重要数据保护要求；
c) 建立数据监控机制，对相关操作行为进行溯源和合规性分析。

L.2.6 安全评估

a) 具备对云计算环境下的运营资产安全风险评估的能力， 评估应包括但不限于系统安全评估和网络安全评估；
b) 系统安全评估应至少包括配置核查、漏洞核查和补丁核查等评估内容；
c) 网络安全评估应至少包含网络访问控制评估、入侵检测评估等评估内容；
d) 应对云环境信息的传输、存储、使用、交换过程进行安全评估，确保各项操作均不会导致敏感数据泄露或重要数据遭受破坏；
e) 应对云计算服务过程进行安全评估和合规性评估，确保服务过程的规范性和安全性；
f) 应定期对云计算安全服务评价情况进行评估，发现安全问题及时整改。

L.2.7 应急管理

a) 明确相关安全事件的应急响应要求；
b) 制定应急响应处置流程；
c) 应专门制定数据相关安全事件应急响应要求和处置流程；
d) 应制定专门的应急预案，明确应急流程和人员分工，并定期开展应急演练。

L.2.8 安全监管

a) 对于制定的云服务安全运营、安全防护、安全管理要求，监管其落实情况；
b) 对发现的问题、识别的风险，应进行督促整改；
c) 制定云资源共享、开放管理相关流程、制度、机制，并对落实情况进行监管。

L.3 三级要求

L.3.1 基础能力要求

a) 具有专业的服务团队，确定项目负责人和安全服务负责人，其中项目负责人和安全服务负责人应具备3年以上网络空间安全服务领域工作经历，安全负责人具有相应安全资质；
b) 近三年内至少有6个云计算安全服务项目，工程按合同要求质量合格，已通过验收，维持资格最少完成1个云计算安全服务项目；
c) 具备本地6小时、外地12小时应急响应服务能力；
d) 应提供云计算安全服务完整解决方案，制定持续改进计划并实施；
e) 应具备从组织建设、制度流程、技术工具和人员能力四个纬度进行数据安全规划的能力，并编写云计算安全保障整体解决方案；
f) 本级安全服务机构能提供的安全技术能力和安全管理能力应不低于等级保护三级的要求。

L.3.2 云计算安全技术要求

L.3.2.1 安全运营技术

a) 具备身份鉴别能力，即基于口令认证的方式对登录云计算平台或应用系统的云用户进行身份鉴别的能力；
b) 具备授权管理能力，即基于主体角色的授权机制，基于主体角色授权的访问控制能力；
c) 具备安全审计能力，即建立操作日志能力，能记录对信息采集、传输、存储、使用等处理环节的操作日志，日志内容包括但不限于：时间、IP地址、用户ID、操作内容、操作对象等；
d) 具备实时监控和可视化展示能力，即对云基础设施、安全设备、业务应用运行状态等进行实时监控以及以可视化方式展示；
e) 具备安全漏洞和补丁管理能力，即发现云资产安全漏洞的能力，并能对云资产补丁信息进行获取和管理的能力；
f) 具备安全事件分析和告警的能力，即结合威胁情报信息进行安全事件分析、确认的能力；对威胁事件、安全事件内容可以使用但不限于短信、邮件、工单等方式进行告警发送；
g) 具备自动化响应与通知的能力，即针对安全事件、应急事件等进行自动化响应与通知的措施。

L.3.2.2 安全防护技术

a) 具备入侵检测能力、实时监测能力、被动响应能力；
b) 具备云计算环境下的风险评估能力；
c) 具备数据备份与恢复能力，即应具备定期执行云上数据备份及恢复、实现存储数据的冗余、保护数据的可用性的能力，应能够对重要信息进行备份和恢复，应查验关键网络设备、通信线路和数据处理系统的硬件冗余，保证系统的可用性；
d) 应有能力通过设置升级服务器等方式保持系统补丁及时得到更新；
e) 具备恶意代码防范能力，即应支持防恶意代码软件的统一管理；
f) 具备确保数据完整性和一致性检测的能力，即应能够检测到鉴别信息和重要业务数据在传输、存储等过程中完整性或一致性受到破坏；
g) 应同时具备威胁情报分析与利用能力、主动应急响应能力；
h) 应具备为操作系统实施最小安装原则的能力，安装服务应具备仅安装需要的组件和应用程

序的能力；

i） 具备进行渗透测试能力、高级安全分析、恶意文件分析能力；

j） 具备数据加密的能力，应采用加密或其他保护措施实现鉴别信息和重要业务数据在传输、存储等过程中的保密性；

k） 具备数据容错的能力，应具备数据备份和恢复策略，以及容灾技术、数据纠错等技术，保证业务持续性；

l） 根据实际情况不断调整数据分析管理平台分析策略，优化安全管理及预警能力；

m） 定期通过安全分析管理平台进行整体安全分析，并形成安全报告。

L.3.3 云计算安全管理要求

L.3.3.1 安全策略

a） 建立云计算安全服务流程，确保流程合规，满足相关法律法规要求；

b） 建立云计算安全服务规范；

c） 建立相应的责任制度、审计机制、风险识别机制；

d） 应对敏感数据建立有针对性的管理机制和保障措施；

e） 应定期进行安全策略评审，建立变更审批流程，执行变更程序。

L.3.3.2 组织人员

a） 制定安全团队管理流程，设立安全管理员、安全审计员、数据安全员等负责人岗位，明确安全团队的职责以及能力要求；

b） 定期开展针对各岗位人员与安全相关的管理规范、流程、制度、技能培训，并进行考核；

c） 具备攻击防御团队（蓝方）和攻击模拟团队（红方）；

d） 应成立指导安全工作的委员会或领导小组，其最高领导由单位主管领导担任或授权；

e） 应设立数据保护官，负责对个人信息或其他敏感数据进行保护；

f） 对外部单位技术人员和外协人员进行安全管理，签署保密协议，不得进行非授权操作，不得复制和泄露任何敏感信息。

L.3.3.3 云资产管理

a） 确保云IT资产合规性，对于资产数据进行不同方式展现；

b） 具备批量对于IT设备进行升级、加固等操作的能力；

c） 建立云资产台账，台账覆盖范围包含所有的云资产，包括不限于资产内容、资产位置、资产重要程度、责任部门、责任人员等内容；

d） 具备按重要程度对云资产进行标识的能力，规定云资产分类标识的原则和方法，对不同重要程度资产实施分级管理策略，如根据信息的重要程度、敏感程度或用途不同进行分类。

L.3.4 云计算运营管理

a） 建立相关的安全岗位及职责，制定并发布相关安全管理体系，对运营流程进行管理；

b） 明确相应流程节点中的相关人员的职责关系，确定在各流程节点中对应工作要求的责任人员的工作内容和配合方式，并形成相应记录；

c） 对云计算资源共享申请和相关操作进行安全审核，确保共享过程的规范性和安全性；

d） 应对安全运营管理的绩效进行量化以及评价。

L.3.5 合规性管理

a) 建立符合网络安全法等法律法规的云安全策略、规范、制度和管控措施；
b) 建立管控措施和采用相关的技术手段，避免因人工管理模式改变或机构业务重组等方式而规避重要数据保护要求；
c) 建立数据监控机制，对相关操作行为进行溯源和合规性分析；
d) 应建立针对多源数据集汇聚和关联后信息利用的安全风险分析和保护控制措施。

L.3.6 安全评估

a) 具备对云计算环境下的运营资产安全风险评估的能力， 评估应包括但不限于系统安全评估和网络安全评估；
b) 系统安全评估应至少包括配置核查、漏洞核查和补丁核查等评估内容；
c) 网络安全评估应至少包含网络访问控制评估、入侵检测评估等评估内容；
d) 应对云环境信息的传输、存储、使用、交换过程进行安全评估，确保各项操作均不会导致敏感数据泄露或重要数据遭受破坏；
e) 应对云计算服务过程进行安全评估和合规性评估，确保服务过程的规范性和安全性；
f) 应定期对云计算安全服务评价情况进行评估，发现安全问题及时整改；
g) 在安全环境发生变化时应对当前的云计算安全服务情况进行评估，对不符合或不适用情况进行整改。

L.3.7 应急管理

a) 明确相关安全事件的应急响应要求；
b) 制定应急响应处置流程；
c) 应专门制定数据相关安全事件应急响应要求和处置流程；
d) 应制定专门的应急预案，明确应急流程和人员分工，并定期开展应急演练；
e) 应采取技术措施实现实时安全预警，并及时处理发现的攻击事件或安全问题。

L.3.8 安全监管

a) 对于制定的云服务安全运营、安全防护、安全管理要求，监管其落实情况；
b) 对发现的问题、识别的风险，应进行督促整改；
c) 制定云资源共享、开放管理相关流程、制度、机制，并对落实情况进行监管；
d) 应具备采用技术手段实施自动化监控和辅助监管的能力；
e) 应定期/不定期进行安全检查，对人员、环境、行为等进行审查；
f) 应对所有相关操作记录、日志、相关审批记录、工作记录等进行审计；
g) 应对数据实际操作人员、供应商及合作伙伴作业人员的日常数据作业进行重点监控和审计；
h) 应定期进行安全评估活动并出具安全评估报告，应对差距实施整改措施。

L.4 四级要求

L.4.1 基础能力要求

a) 具有专业的服务团队，确定项目负责人和安全服务负责人，其中项目负责人和安全服务负责人应具备5年以上网络空间安全服务领域工作经历，安全负责人具有相应安全资质；

b) 近三年内至少有10个云计算安全服务项目，工程按合同要求质量合格，已通过验收，维持资格最少完成1个云计算安全服务项目；
c) 具备本地2小时、外地4小时应急响应服务能力；
d) 应提供云计算安全服务完整解决方案，制定持续改进计划并实施；
e) 应具备从组织建设、制度流程、技术工具和人员能力四个纬度进行数据安全规划的能力，并编写云计算安全保障整体解决方案；
f) 本级安全服务机构能提供的安全技术能力和安全管理能力应不低于等级保护三级的要求；
g) 应具备自主研发用于云计算安全管理和服务的综合性数据分析管理平台，并至少有一个成功落地的平台建设经验。

L.4.2 云计算安全技术要求

L.4.2.1 安全运营技术

a) 具备身份鉴别能力，即基于口令认证的方式对登录云计算平台或应用系统的云用户进行身份鉴别的能力；
b) 具备授权管理能力，即基于主体角色的授权机制，基于主体角色授权的访问控制能力；
c) 具备安全审计能力，即建立操作日志能力，能记录对信息采集、传输、存储、使用等处理环节的操作日志，日志内容包括但不限于：时间、IP地址、用户ID、操作内容、操作对象等；
d) 具备实时监控和可视化展示能力，即对云基础设施、安全设备、业务应用运行状态等进行实时监控以及以可视化方式展示；
e) 具备安全漏洞和补丁管理能力，即发现云资产安全漏洞的能力，并能对云资产补丁信息进行获取和管理的能力；
f) 具备安全事件分析和告警的能力，即结合威胁情报信息进行安全事件分析、确认的能力；对威胁事件、安全事件内容可以使用但不限于短信、邮件、工单等方式进行告警发送；
g) 具备自动化响应与通知的能力，即针对安全事件、应急事件等进行自动化响应与通知的措施。

L.4.2.2 安全防护技术

a) 具备入侵检测能力、实时监测能力、被动响应能力；
b) 具备云计算环境下的风险评估能力；
c) 具备数据备份与恢复能力，应具备定期执行云上数据备份及恢复、实现存储数据的冗余、保护数据的可用性的能力，应能够对重要信息进行备份和恢复，应查验关键网络设备、通信线路和数据处理系统的硬件冗余，保证系统的可用性；
d) 应有能力通过设置升级服务器等方式保持系统补丁及时得到更新；
e) 具备恶意代码防范能力，即应支持防恶意代码软件的统一管理；
f) 具备确保数据完整性和一致性检测的能力，即应能够检测到鉴别信息和重要业务数据在传输、存储等过程中完整性或一致性受到破坏；
g) 应具备云计算环境下的主动攻击防御的能力，同时具备威胁情报分析与利用能力、主动应急响应和处理能力；
h) 应具备为操作系统实施最小安装原则的能力，安装服务应具备仅安装需要的组件和应用程序的能力；

i） 具备进行渗透测试能力、高级安全分析、恶意文件分析能力；
j） 具备数据加密的能力，应采用加密或其他保护措施实现鉴别信息和重要业务数据在传输、存储等过程中的保密性；
k） 具备数据容错的能力，应具备数据备份和恢复策略，以及容灾技术、数据纠错等技术，保证业务持续性；
l） 根据实际情况不断调整数据分析管理平台分析策略，优化安全管理及预警能力；
m） 定期通过安全分析管理平台进行整体安全分析，并形成安全报告，并出具加固措施，实施安全整改；
n） 应具备自主研发的云计算安全防护设备、安全态势分析管理平台，能统一接入各类安全防护设备数据、访问纪录、操作日志等，进行日志的大数据分析以实现风险的实时持续性监测、预测性评价；
o） 应具备多租户数据安全防护能力，确保业务全生命周期内的安全风险管控。

L.4.3 云计算安全管理要求

L.4.3.1 安全策略

a） 建立云计算安全服务流程，确保流程合规，满足相关法律法规要求；
b） 建立云计算安全服务规范；
c） 建立相应的责任制度、审计机制、风险识别机制；
d） 应对敏感数据建立有针对性的管理机制和保障措施；
e） 应定期进行安全策略评审，建立变更审批流程，执行变更程序；
f） 安全策略的评审结果应至少保留10年。

L.4.3.2 组织人员

a） 制定安全团队管理流程，设立安全管理员、安全审计员、数据安全员等负责人岗位，明确安全团队的职责以及能力要求；
b） 定期开展针对各岗位人员与安全相关的管理规范、流程、制度、技能培训，并进行考核；
c） 具备攻击防御团队（蓝方）和攻击模拟团队（红方）；
d） 应成立指导安全工作的委员会或领导小组，其最高领导由单位主管领导担任或授权；
e） 应设立数据保护官，负责对个人信息或其他敏感数据进行保护，不准许兼任；
f） 对外部单位技术人员和外协人员进行安全管理，签署保密协议，不得进行非授权操作，不得复制和泄露任何敏感信息；
g） 应建立对各岗位人员行为的监控和审计机制。

L.4.3.3 云资产管理

a） 应确保云IT资产合规性，对于资产数据进行不同方式展现；
b） 应具备批量对于IT设备进行升级、加固等操作的能力；
c） 建立云资产台账，台账覆盖范围包含所有的云资产，包括不限于资产内容、资产位置、资产重要程度、责任部门、责任人员等内容；
d） 具备按重要程度对云资产进行标识的能力，规定云资产分类标识的原则和方法，对不同重要程度资产实施分级管理策略，如根据信息的重要程度、敏感程度或用途不同进行分类；
e） 应规定对不同类数据资产的使用、传输和存储的管理办法。

L.4.4 云计算运营管理

a) 建立相关的安全岗位及职责，制定并发布相关安全管理体系，对运营流程进行管理；
b) 明确相应流程节点中的相关人员的职责关系，确定在各流程节点中对应工作要求的责任人员的工作内容和配合方式，并形成相应记录；
c) 对云计算资源共享申请和相关操作进行安全审核，确保共享过程的规范性和安全性；
d) 应对安全运营管理的绩效进行量化以及评价；
e) 安全运营流程管理应至少提供云安全资产管理流程、云安全运维作业管理流程、云安全事件管理流程、云安全合规测评流程等能力。

L.4.5 合规性管理

a) 建立符合网络安全法等法律法规的云安全策略、规范、制度和管控措施；
b) 建立管控措施和采用相关的技术手段，避免因人工管理模式改变或机构业务重组等方式而规避重要数据保护要求；
c) 建立数据监控机制，对相关操作行为进行溯源和合规性分析；
d) 应建立针对多源数据集汇聚和关联后信息利用的安全风险分析和保护控制措施；
e) 应定期对重要数据安全策略、规范、制度和管控措施进行风险评估，并及时调整更新；
f) 应该提供数据的自动化脱敏机制与措施，支持如匿名、泛化、随机、加密等脱敏方法，并应具备数据脱敏有效性的评估能力。

L.4.6 安全评估

a) 具备对云计算环境下的运营资产安全风险评估的能力， 评估应包括但不限于系统安全评估和网络安全评估；
b) 系统安全评估应至少包括配置核查、漏洞核查和补丁核查等评估内容；
c) 网络安全评估应至少包含网络访问控制评估、入侵检测评估等评估内容；
d) 应对云环境信息的传输、存储、使用、交换过程进行安全评估，确保各项操作均不会导致敏感数据泄露或重要数据遭受破坏；
e) 应对云计算服务过程进行安全评估和合规性评估，确保服务过程的规范性和安全性；
f) 应定期对云计算安全服务评价情况进行评估，发现安全问题及时整改；
g) 在安全环境发生变化时应对当前的云计算安全服务情况进行评估，对不符合或不适用情况进行整改；
h) 涉及数据跨境传输的，应对其合规性和安全性进行评估，评估通过后才可进行相应操作；
i) 应对高风险操作可能对平台和数据造成的影响进行评估，评估通过后才可进行相应操作。

L.4.7 应急管理

a) 明确相关安全事件的应急响应要求；
b) 制定应急响应处置流程；
c) 应专门制定数据相关安全事件应急响应要求和处置流程；
d) 应制定专门的应急预案，明确应急流程和人员分工，并定期开展应急演练；
e) 应采取技术措施实现实时安全预警，并及时处理发现的攻击事件或安全问题。

L.4.8 安全监管

a) 对于制定的云服务安全运营、安全防护、安全管理要求，监管其落实情况；
b) 对发现的问题、识别的风险，应进行督促整改；
c) 制定云资源共享、开放管理相关流程、制度、机制，并对落实情况进行监管；
d) 应具备采用技术手段实施自动化监控和辅助监管的能力；
e) 应定期/不定期进行安全检查，对人员、环境、行为等进行审查；
f) 应对所有相关操作记录、日志、相关审批记录、工作记录等进行审计；
g) 应对数据实际操作人员、供应商及合作伙伴作业人员的日常数据作业进行重点监控和审计；
h) 应定期进行安全评估活动并出具安全评估报告，应对差距实施整改措施；
i) 应通过随机约谈相关人员，对安全落实情况进行检查评估。

参 考 文 献

[1] GB/T 20261-2020 信息安全技术 系统安全工程 能力成熟度模型

[2] GB/T 20984-2022 信息安全技术 信息安全风险评估方法

[3] GB/T 27000-2023 合格评定 词汇和通用原则

[4] GB/T 30271—2013 信息安全技术信息安全服务能力评估准则

[5] GB/T 30283-2022 信息安全技术 信息安全服务 分类与代码

[6] RB/T201—2013 信息系统安全集成服务资质认证评价要求

[7] YD/T1621—2007 网络与信息安全服务资质评估准则

[8] YD/T1799—2008 网络与信息安全应急处理服务资质评估方法

[9] YD/T2252—2011 网络与信息安全风险评估服务能力评估方法

[10] ISO/IEC 27001:2005 Information technology-Security techniques-Information security management systems-Requirements

[11] ISO/IEC 27002:2005 Information technology-Security techniques-Code of practice for information security controls

[12] ISO/IEC 27005:2008 Information technology-Security techniques－Information security risk managemen

[13] CNCA/CTS0052-2007 信息安全服务资质认证技术规范