ICS 03.120.20

A 00

团体标准

T/CAS 375—2019

网络安全服务机构等级评定规范

Grade assessment specification   
of cyber security service institutions

（征求意见稿）

2019-09-25 发布 2019-09-25 实施

中国标准化协会  
北京网络空间安全协会

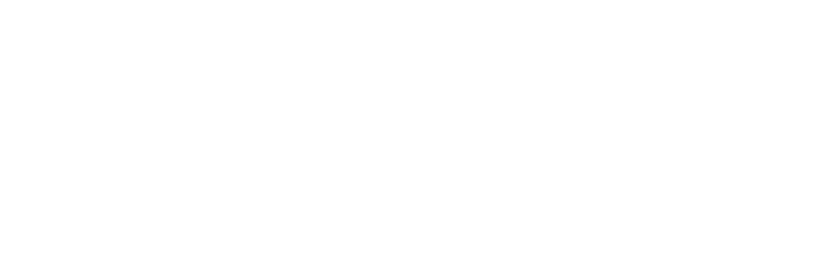
发 布

中国标准化协会（CAS）是组织开展国内、国际标准化活动的全国性社会团体。制定中国标准化协会标准（以下简称：中国标协标准），满足企业需要，推动企业标准化工作，是中国标准化协会的工作内容之一。中国境内的团体和个人，均可提出制、修订中国标协标准的建议并参与有关工作

中国标协标准按《中国标准化协会标准管理办法》进行制定和管理。

中国标协标准草案经向社会公开征求意见，并得到参加审定会议的75%以上的专家、成员的投票赞同，方可作为中国标协标准予以发布。

在本文件实施过程中，如发现需要修改或补充之处，请将意见和有关资料寄给中国标准化协会以便修订时参考。



本标准版权为中国标准化协会和北京网络空间安全协会所有。除了用于国家法律或事先得到中国标准化协会和北京网络空间安全协会文字上的许可外，不许以任何形式复制该标准。

中国标准化协会地址：北京市海淀区增光路 33 号中国标协写字楼邮政编码：100048 电话：010-68487160 传真：010-68486206

网址：[www.china-cas.](http://www.china-cas.com/)org 电子信箱：[cas@china-cas.org](mailto:cas@china-cas.org)

目 次

[前言 II](#_Toc3022)

[引言 III](#_Toc16820)

[1 范围 1](#_Toc24281)

[2 规范性引用文件 1](#_Toc21107)

[3 术语和定义 1](#_Toc28450)

[4 网络安全服务类型 2](#_Toc2835)

[5 评定原则与流程 4](#_Toc485)

[6 服务机构等级划分 4](#_Toc15706)

[7 基本能力要求 5](#_Toc15317)

[附录A 评定流程 12](#_Toc11572)

[附录B 安全咨询服务 13](#_Toc26961)

[附录C 信息系统安全集成服务 16](#_Toc10446)

[附录D 信息系统安全运维服务 22](#_Toc30348)

[附录E 监测预警服务 27](#_Toc8981)

[附录F 应急响应服务 30](#_Toc27141)

[附录G 软件安全服务 35](#_Toc28081)

[附 录H 工业控制系统安全服务 42](#_Toc19030)

[附录I 数据安全服务 45](#_Toc12920)

[附 录J 信息安全风险评估服务 49](#_Toc6993)

[附录K 云计算安全服务 54](#_Toc31510)

[附 录L 信息系统安全审计服务 64](#_Toc15478)

[附录M 渗透测试服务 69](#_Toc27447)

[参考文献 74](#_Toc2899)

# 前 言

本文件按照 GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件起草单位：。

本文件主要起草人：。

考虑到本文件中的某些条款可能涉及专利，中国标准化协会、北京网络空间安全协会不负责对任何该类专利的鉴别。

本文件首次修订。

# 引 言

随着互联网的普及应用，网络安全已成为国家安全战略重要组成部分。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。2017年6月1日，《中华人民共和国网络安全法》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、安全运转、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《网络安全服务机构等级评定规范》，按照标准要求实施网络安全服务机构等级评定，客观公正地评价服务机构的资格和服务能力，既可作为服务机构开展自我评价的规范和标准，也可为用户在维护网络安全工作中选择服务机构提供依据，有利于规范市场秩序、避免恶性竞争、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，切实保护我国网络的安全。

# 网络安全服务机构等级评定规范

1. 范围

本文件规定了网络安全服务机构（以下简称“服务机构”）应具备的基本能力要求、专业能力要求及评定要求。

本文件适用于第三方机构对服务机构进行资信和能力评价，可作为服务机构开展自我评价的依据，并可为服务对象选择服务机构提供依据。

1. 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 27000—2006 合格评定 词汇和通用原则

1. 术语和定义

下列术语和定义适用于本文件。



网络安全服务 cyber security service

由服务机构为服务对象提供的全面或部分网络安全解决方案的服务。主要包括网络与信息系统安全工程的设计、实施、运行、维护和数据保护与应用，以及相关的咨询和培训等活动。



网络安全服务机构 cyber security service institutions

按照合同或协议的约定为服务对象提供网络安全服务的组织，也称为网络安全服务提供商。



网络安全服务机构等级 cyber security service institution grade

用于评定网络安全服务机构服务能力的级别，主要包括从业时间、法律资格、财务资信、制度及流程、人员状况、技术能力、专业能力等方面的要求，以下简称“服务等级”。



网络安全服务机构等级评定组织 grading organization of cyber security service Institutions

行业内有影响力的专业机构、专业协会和专业组织等对网络安全服务机构的服务能力按照相应标准进行等级评估的第三方组织，简称“评定机构”。

1. 网络安全服务类型
   1. 安全咨询服务

服务机构根据服务对象网络与信息系统所支持的业务和管理，通过知识传递、工作辅导和系统规划等形式提供的网络安全服务。主要包括安全规划、安全管理体系咨询、安全风险评估、安全应急管理咨询、业务连续性管理咨询等。

* 1. 信息系统安全集成服务

服务机构根据服务对象对网络安全服务的需求，提供和实施的安全需求界定、安全设计、安全实施、安全保障等网络安全服务。主要服务流程包括安全方案设计、实施、测试和验收等。

* 1. 信息系统安全运维服务

为保障和提升服务对象的信息系统安全防护能力，及时解决出现的网络安全问题，由服务机构通过管理与技术手段提供的网络安全服务。主要包括安全巡检、病毒查杀、备份和恢复、安全审计、安全优化、渗透测试、风险评估等。

* 1. 监测预警服务

服务机构依托专业知识和技能，利用专业工具对及时发现的网络安全风险进行持续跟踪、分析和预警，并按照规程进行上报的服务。主要包括漏洞检测、攻击监测、恶意代码检测、安全态势感知和安全通报等。

* 1. 应急响应服务

服务机构根据服务对象信息安全应急管理体系，针对各类突发信息安全事件做出快速响应，及时而有效进行事件处理，最大程度减少事件造成的影响和损失，或根据服务对象已有的应急预案， 在设备、系统、业务、组织等不同层面进行测试和演练，从而提高服务对象应对各类突发事件的能力。主要包括应急响应、应急预案和应急演练等。

* 1. 软件安全服务

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

* 1. 工业控制系统安全服务

服务机构针对服务对象工业网络与信息安全问题，通过管理与技术手段保护服务对象的工业控制系统的软硬件、网络及其中数据，使其不因偶然的或者恶意原因而遭受破坏、更改泄露，保障工业控制系统连续正常地运行所提供的一系列安全服务。主要包括工业控制系统调研、工业控制系统风险评估、安全解决方案设计、安全加固与防护实施、运维管理体系建设等。

* 1. 数据安全服务

服务机构根据服务对象数据管理要求提供的数据权属、数据保护、数据安全共享、数据权益保障、数据交易应用等网络安全服务。主要包括数据的分级、权属、注册、保护、共享、应用、交易、评估、权益、溯源等。

* 1. 信息安全风险评估服务

服务机构通过对信息系统提供风险评估服务，系统地分析网络与信息系统所面临的威胁及其存在的威胁性，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安全整改措施。

* 1. 云计算安全服务

服务机构根据服务对象的云计算业务范围确定其云服务模型，从基础能力、管理能力和技术能力这三方面出发，提供符合客户业务场景的最佳实践指导的安全服务。从管理保障角度做好法律法规遵守、合规和审计、信息治理、业务连续性和灾备管理、供应商管理控制的工作；从技术保障角度做好基础设施安全保障、虚拟化和容器安全保护、应用安全保护、数据安全保护、权限访问管理、应急响应控制的工作。

* 1. 信息系统安全审计服务

服务机构根据服务对象网络与信息系统现状情况，能通过收集和评价审计证据，检查和促进被审计单位信息系统及其内部控制的真实性、正确性、完整性、安全性、可靠性和经济性等要素。使被服务对象的内控目标得以有效地实现、使组织的资源得到高效地使用。主要包括IT治理层审计、重要信息系统层审计等。

* 1. 渗透测试服务

服务机构根据服务对象的测试需求，模拟黑客攻击的手法，进行的非破坏性的攻击性测试，以期发现可能被黑客利用对系统进行入侵的安全漏洞和隐患及攻击路径，并将入侵的过程和漏洞细节产生报告给服务对象，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。

1. 评定原则与流程
   1. 权威性原则

由评定机构依据本文件公开、公正、公平的原则进行评定。

* 1. 自愿原则

网络安全服务机构等级评定由服务机构自愿向评定机构提出申请，评定机构收到申请后依据本文件进行评定。

* 1. 一致性原则

网络安全服务能力具有本地化特征，网络安全服务企业在不同区域的服务能力由相应区域的评定机构依照该文件进行评定，以保证服务能力等级评定在不同区域的一致性。

* 1. 公平性原则

评定机构相关人员要进行统一培训，采用相同的评定实施规则和流程，以保证评定的公平性。

* 1. 综合评定原则

网络安全服务机构评定的等级要求同时满足该等级的基本能力要求和专业能力要求，若基本能力和专业能力评定的等级不一致，取较低的等级作为网络安全服务机构的最终评定等级。

* 1. 评定流程

网络安全服务机构等级评定流程按附录A的规定执行。

1. 服务机构等级划分

网络安全服务机构等级评定要求包含基本能力要求、技术服务能力要求。基本能力要求包含法律资格、财务资信、人员状况、办公场所、从业时间、经营业绩、管理制度、合同管理等，具体要求见第7章。技术服务能力要求包含基本要求、准备阶段、设计阶段、实施阶段、服务保障阶段等4个阶段的服务过程要求，具体要求见规范性附录B-M。依据服务机构的基本能力和技术服务能力要求分为一级、二级、三级、四级，其中四级最高，一级最低。

1. 基本能力要求
   1. 第一级要求
      1. 法律资格

应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。

* + 1. 财务资信

应有健全的财务管理制度，财务数据真实可信。

* + 1. 办公场所

应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。

* + 1. 人员能力要求

网络安全服务机构的服务人员要求：

* + - 1. 机构负责人应拥有1年以上（含1年）信息技术领域管理经历；
      2. 技术负责人应从事网络安全技术工作1年以上（含1年）；
      3. 应从事网络安全服务人员5名以上（含5名）；
      4. 应拥有与申报类别一致的网络安全专业技术人员证书3名以上（含3名）。
    1. 从业时间

首次申请不做要求。

* + 1. 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安全服务项目。

* + 1. 管理制度

网络安全服务机构管理制度要求：

* + - 1. 应具备健全的人力资源管理制度，服务人员能持续满足业务需求；
      2. 应建立文档控制程序，明确文档管理职责；
      3. 应建立项目管理制度和实施细则；
      4. 应制定专业人员业务技能培训计划和能力考核指标；
      5. 应制定保密管理制度，明确岗位保密责任，对服务对象敏感信息和知识产权予以保护，与相关人员签订保密协议，并进行保密教育。
    1. 合同管理

网络安全服务机构的合同要求：

* + - 1. 应具有健全的合同管理制度；
      2. 应具有健全的合同评审程序；
      3. 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。
  1. 第二级要求
     1. 法律资格

应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，应具有相应的经营范围。

* + 1. 财务资信

应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。

* + 1. 办公场所

应具有固定的办公场所和相应的办公条件，办公场所面积能够满足机构设置及其业务需要。

* + 1. 人员能力

安全服务机构的服务人员要求：

* + - 1. 机构负责人应拥有2年以上（含2年）信息技术领域管理经历；
      2. 技术负责人应从事网络安全技术工作2年以上（含2年）；
      3. 应从事网络安全服务人员10名以上（含10名）；
      4. 应拥有与申报类别一致的网络安全专业技术人员证书6名以上（含6名）。
    1. 从业时间

应从事与申报类别一致的网络安全服务1年以上。

* + 1. 经营业绩

服务机构的经营业绩要求：

* + - 1. 近二年内应签订并完成至少3个与申报类别一致的网络安全服务项目；
      2. 非安全咨询服务近二年应完成与申报类别一致的服务业绩累积达50（含50）万元以上，其中至少有一个与申报类别一致的单个服务项目合同额10（含10）万元以上；安全咨询服务近二年完成与申报类别一致的服务业绩累积达20（含20）万元以上，其中至少有一个与申报类别一致的单个服务项目合同额5（含5）万元以上。
    1. 管理制度

服务机构的管理制度要求：

* + - 1. 应具备健全的人力资源管理制度，服务人员能持续满足业务需求；
      2. 应建立文档控制程序，明确文档管理职责；
      3. 应建立项目管理制度和实施细则；
      4. 应制定专业人员业务技能培训计划和能力考核指标；
      5. 应制定保密管理制度，明确岗位保密责任，对服务对象敏感信息和知识产权予以保护，与相关人员签订保密协议，并进行保密教育。
    1. 合同管理

服务机构的合同管理要求：

* + - 1. 应具有健全的合同管理制度；
      2. 应具有健全的合同评审程序；
      3. 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。
  1. 第三级要求
     1. 法律资格

应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，应具有相应的经营范围。

* + 1. 财务资信

应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。

* + 1. 办公场所

应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。

* + 1. 人员能力

服务机构的服务人员要求：

* + - 1. 机构负责人应拥有3年以上（含3年）信息技术领域管理经历；
      2. 技术负责人应从事网络安全技术工作3年以上（含3年）；
      3. 应从事网络安全服务人员20名（含20名）以上；
      4. 应拥有与申报类别一致的网络安全专业技术人员证书10名（含10名）以上。
    1. 从业时间

应从事与申报类别一致的网络安全服务3年以上，或取得网络安全服务等级评定资质2级满1年以上。

* + 1. 经营业绩

服务机构的经营业绩要求：

* + - 1. 近二年内应签订并完成至少6个与申报类别一致的网络安全服务项目；
      2. 非安全咨询服务近二年应完成与申报类别一致的服务业绩累积达100（含100）万元以上，其中至少有一个与申报类别一致的单个服务项目合同额30（含30）万元以上；安全咨询服务近二年完成与申报类别一致的服务业绩累积达50（含50）万元以上，其中至少有一个与申报类别一致的单个服务项目合同额10（含10）万元以上。
    1. 管理制度

服务机构的管理制度要求：

* + - 1. 应具备健全的人力资源管理制度，服务人员能持续满足业务需求；
      2. 应建立文档控制程序，明确文档管理职责；
      3. 应建立项目管理制度和实施细则；
      4. 应制定专业人员业务技能培训计划和能力考核指标；
      5. 应制定保密管理制度，明确岗位保密责任，对服务对象敏感信息和知识产权予以保护，与相关人员签订保密协议，并进行保密教育；
      6. 应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。
    1. 合同管理

服务机构的合同要求：

* + - 1. 应具有健全的合同管理制度；
      2. 应具有健全的合同评审程序；
      3. 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。
    1. 专业工具

服务机构的专业工具要求：

* + - 1. 应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；
      2. 应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。
  1. 第四级要求
     1. 法律资格

应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，应具有相应的经营范围。

* + 1. 财务资信

应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。

* + 1. 办公场所

应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。

* + 1. 人员能力

服务机构的服务人员要求：

* + - 1. 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；
      2. 技术负责人应从事网络安全技术工作5年以上（含5年）；
      3. 应从事网络安全技术服务人员30名以上（含30名）；
      4. 拥有与申报类别一致的网络安全专业技术人员证书20名以上（含20名）。
    1. 从业时间

应从事与申报类别一致的网络安全服务5年以上，或取得网络安全服务等级评定资质3级满1年以上。

* + 1. 经营业绩

服务机构的经营业绩要求：

* + - 1. 近二年内应至少签订并完成10个网络安全服务项目；
      2. 非安全咨询服务近二年应完成与申报类别一致的服务业绩累积达200（含200）万元以上，其中至少有一个与申报类别一致的单个服务项目合同额100（含100）万元以上；安全咨询服务近二年完成与申报类别一致的服务业绩累积达100（含100）万元以上，其中至少有一个与申报类别一致的单个服务项目合同额20（含20）万元以上。
    1. 管理制度

服务机构的管理制度要求：

* + - 1. 应具备健全的人力资源管理制度，服务人员能持续满足业务需求；
      2. 应建立文档控制程序，明确文档管理职责；
      3. 应建立项目管理制度和实施细则；
      4. 应制定专业人员业务技能培训计划和能力考核指标；
      5. 应制定保密管理制度，明确岗位保密责任，对服务对象敏感信息和知识产权予以保护，与相关人员签订保密协议，并进行保密教育；
      6. 应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。
      7. 应参照国际或国内标准，建立信息安全管理体系并有效运行。
    1. 合同管理
       1. 应具有健全的合同管理制度；
       2. 应具有健全的合同评审程序；
       3. 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。
    2. 专业工具

服务机构的专业工具要求：

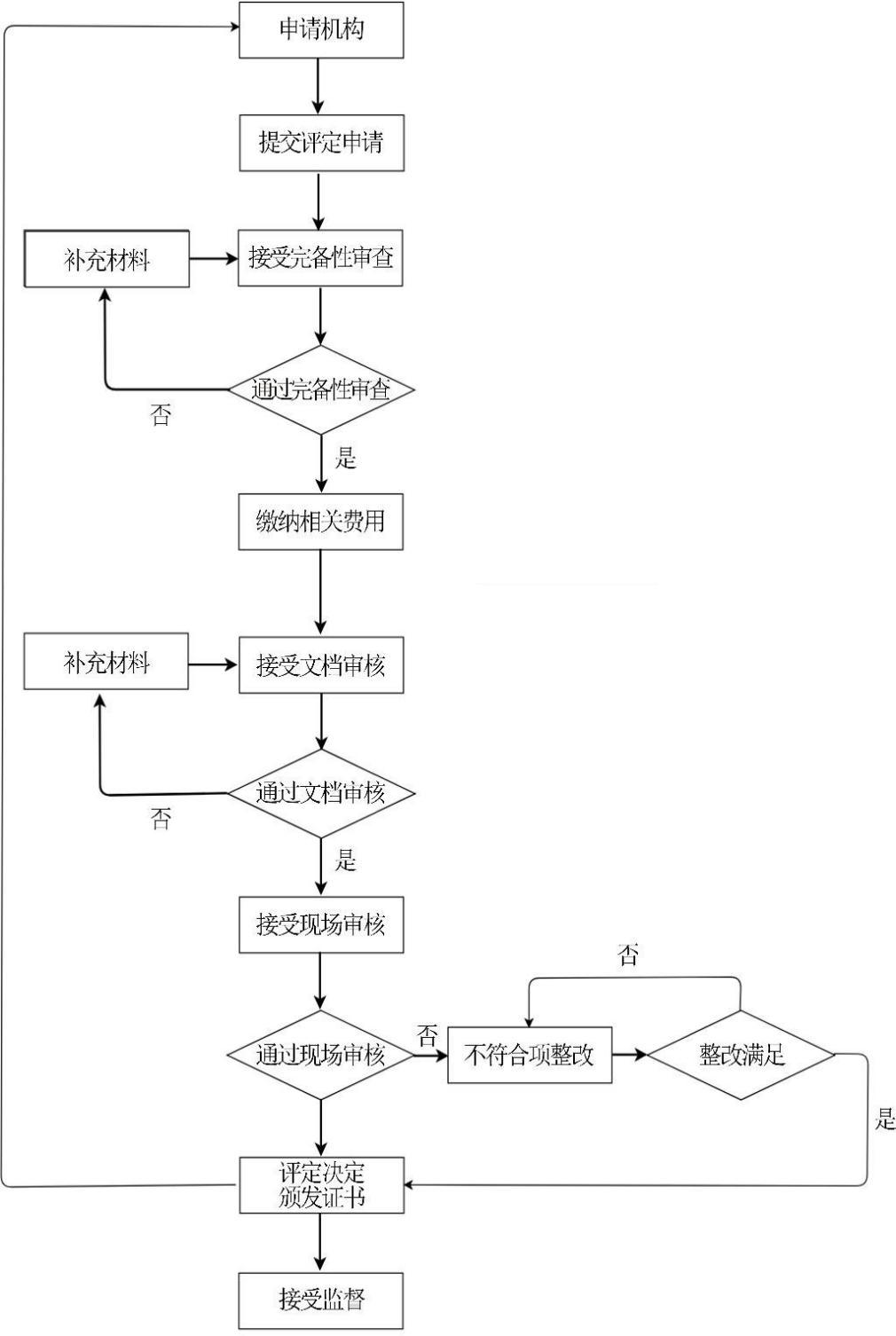
* + - 1. 应具备独立的测试环境及必要的软、硬件设备，用于技术培训和模拟测试；
      2. 应具备承担与申报类别一致的网络安全服务项目所需的安全工具，并对工具进行管理和版本控制。

附 录 A

（规范性附录）

评定流程

开展网络安全服务机构等级评定，按照图A.1规定的流程进行。



图A..1评定流程

附 录 B

（规范性附录）

安全咨询服务机构评价要求

* 1. 第一级要求
     1. 准备阶段
        1. 应编制安全咨询服务方案、安全咨询服务模板，并在项目实施过程中按照模板实施；
        2. 应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；
        3. 应根据项目需求准备必要的工具；
        4. 应对项目团队实施安全咨询服务前进行培训。
     2. 实施阶段
        1. 应面向组织操作层，了解组织业务流程、技术应用和数据开发利用情况；
        2. 应形成安全咨询服务的解决方案；
        3. 应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；
        4. 应提交满足安全咨询服务方案的结果；
        5. 应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，必要时对实施方案进行修改。
     3. 改进阶段
        1. 应建立服务能力管理改进和创新机制；
        2. 应提供项目风险管理记录；
        3. 应具备安全咨询服务指南性文件和质量手册。
  2. 第二级要求
     1. 基本要求

除满足一级能力要求外，还应满足B.2.2～B.2.4的要求。

* + 1. 准备阶段
       1. 应开展项目前期调研，形成组织基本现状、需求和目标，明确项目范围；
       2. 应根据项目目标和前期调研结果，确定项目实施方案。
    2. 实施阶段
       1. 应面向组织操作层和执行层，了解组织的业务流程、技术应用、数据开发利用和人财物资源配置管理情况；
       2. 实施成果在交付之前，应进行项目内部评审。
    3. 改进阶段
       1. 应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；
       2. 应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。
  1. 第三级要求
     1. 基本要求

除满足二级能力要求外，还应满足B.3.2～B.3.4要求。

* + 1. 准备阶段
       1. 应确定安全标准以及用户需求，完成安全需求分析报告；
       2. 项目实施方案应同相关方进行评审。
    2. 实施阶段
       1. 应面向组织操作层、执行层和管理层，了解组织的组织结构、业务流程、技术应用、数据开发利用、人财物资源配置管理和绩效考核情况；
       2. 应调查用户满意度，并对服务能力实施的结果进行评价，支持服务改进；
       3. 针对用户应开展安全咨询服务成果培训。
    3. 改进阶段
       1. 应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；
       2. 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。
  1. 第四级要求
     1. 基本要求

除满足三级能力要求外，还应满足B.4.2～B.4.4的要求。

* + 1. 准备阶段
       1. 应采取相关措施，保障工具管理的规范性；
       2. 应制定覆盖项目准备阶段、实施阶段和改进阶段的培训方案，明确培训对象、培训内容、培训计划等。
    2. 实施阶段

实施阶段要求：

* + - 1. 应面向组织操作层、执行层、管理层和决策层，了解组织的战略规划、业务流程、组织结构、技术应用、数据开发利用、人财物资源配置管理和绩效考核情况；
      2. 应采用多种咨询方法进行服务实施；
      3. 针对项目成果应组织召开专家评审会。
    1. 改进阶段
       1. 应具备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；
       2. 应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；
       3. 应建立安全咨询服务专家库，能够满足项目需要。

附 录 C

(规范性目录)

信息系统安全集成技术服务能力评价要求

* 1. 第一级要求
     1. 基本要求
     2. 准备阶段

准备阶段要求：

* + - 1. 应组建不少于3人的安全集成项目团队，包括技术人员和管理人员，指定项目负责人；
      2. 应根据服务对象的需求，确定系统集成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，并编写技术方案；
      3. 应基于系统建设安全需求，提出产品选型方案和建设预算；
      4. 应明确范围、目标、时间、内容、质量等；
      5. 应与服务对象确定项目安全集成过程中的分工界面，明确双方的责任。
    1. 设计阶段

设计阶段要求：

* + - 1. 应根据系统安全建设需求，编制网络安全技术方案；
      2. 应结合网络安全实施方案，与客户进行沟通，对方案进行确认。
    1. 实施阶段

实施阶段要求：

* + - 1. 应依据已确认的实施方案，对项目进行建设实施；
      2. 项目实施人员应按时提交实施记录和相关文档，及时向服务对象汇报项目进度；
      3. 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，并交服务对象签字确认。
    1. 保障阶段（质量保障阶段）三级四级要有符合性测试。
       1. 系统测评

系统测评要求：

* + - 1. 应编写系统安全测试计划；
      2. 应依据系统测评计划，对系统进行系统安全评估，完整记录评估过程相关信息，形成评估报告，经双方责任人签字确认；
      3. 应符合性安全测试。
      4. 系统试运行

系统运行要求：

* + - 1. 系统初验后应进行试运行，并记录系统运行状况，试运行周期至少一个月（三级企业试运行一周或一个月）；
      2. 应基于系统运行情况，及时对系统进行调整和维护。
    1. 验收阶段（质保阶段）

验收阶段要求：

* + - 1. 应根据合同约定，向服务对象提交完整的项目资料及交付物，并提出验收申请；
      2. 应根据合同约定，组织项目验收，出具项目验收报告。
  1. 第二级要求
     1. 基本要求

除满足一级能力要求外，还应满足C.2.2～C.2.5的要求。

* + 1. 准备阶段

准备阶段要求：

应组建不少于5人的安全集成项目团队，包括技术人员和管理人员，指定项目负责人。

* + 1. 设计阶段

设计阶段要求：

应结合项目技术方案和实施方案，与客户进行沟通，对方案进行书面确认。

* + 1. 实施阶段

实施阶段要求：

* + - 1. 应依据已确认的安全集成项目技术方案和实施方案，对项目进行建设实施；
      2. 项目实施人员应按时提交实施记录和相关文档，及时向服务对象汇报项目进度；
      3. 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，并交服务对象签字确认。
    1. 保障阶段
       1. 系统测评（测试应该是安全性测试，而非联调测试或软件测试）

系统测评要求：

* + - 1. 应编写系统安全评估计划；
      2. 应依据系统评估计划，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；
      3. 应依据系统安全测评的要求，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。
      4. 系统试运行

系统运行要求：

* + - 1. 系统初验后应进行试运行，并记录系统运行状况，试运行周期至少一个月；
      2. 应基于系统运行情况，及时对系统进行调整和维护。
  1. 第三级要求
     1. 基本要求

除满足二级能力要求外，还应满足C.3.2～C.3.5要求。

* + 1. 准备阶段

准备阶段要求：

* + - 1. 项目小组应包括应急组，应急组成员必须具有信息安全相关认证资质；
      2. 应准确识别和综合分析系统在安全方面的需求，提出系统安全保障策略和建议；
      3. 应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；
      4. 应根据服务对象的需求以及未来发展的需要，确定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，并编写技术建议方案。
    1. 设计阶段

设计阶段要求：

* + - 1. 应结合需求，分析服务对象在保障系统安全方面的标准及安全建设投入的能力，提供系统建设安全设计说明书，明确系统架构、产品功能、性能及配置等参数；
      2. 应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；
      3. 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。
    1. 实施阶段
       1. 实施集成

实施集成要求：

* + - 1. 应与服务对象确定项目集成过程中的分工界面，明确双方的责任；
      2. 应对项目实施过程中的成本进行有效的管理；
      3. 应对产品、设备采购、安装调试过程，完整记录相关信息；
      4. 项目建设施工完成后，应提交完工报告；
      5. 项目实施完成后，相关过程记录应及时归档，并统一保管。
      6. 监督管理

监督管理要求：

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、产品质量等应由服务对象和项目监理方进行监督管理，所有设备入库、变更应由监理方或服务对象责任人签字确认。

* + 1. 保障阶段
       1. 系统测评

系统测评要求：

* + - 1. 应依据技术方案具体指标要求，制定系统测评计划；
      2. 应由第三方机构进行系统测评，并出具系统测评报告，提交服务对象，作为初次验收依据；
      3. 应依据系统安全测评的要求，对系统进行新上线前安全测试或安全符合性测试，形成测评报告，经双方责任人签字确认。
      4. 系统试运行

系统试运行要求：

* + - 1. 应提供一个月以上的试运行记录；
      2. 应对系统运行中存在的问题及时整改；
      3. 试运行结束后，项目组应编写系统试运行报告，提交服务对象。
  1. 第四级要求
     1. 基本要求

除满足三级能力要求外，还应满足C.4.2～C.4.5的要求。

* + 1. 准备阶段

安全集成服务4级服务机构的准备阶段要增加需求调研与分析。

* + - 1. 应准确识别和综合分析服务对象在系统安全、数据安全及安全管理方面的需求，提出系统安全保障策略、制度改进等方面建议；
      2. 应建立安全集成服务和安全制度建设管理程序。
    1. 设计阶段

设计阶段要求：

* + - 1. 应结合项目需要，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；
      2. 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；
      3. 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；
      4. 应基于安全集成项目需求和进度计划，编制网络安全产品和工具定制开发计划。
    1. 实施阶段
       1. 实施集成

实施集成要求：

* + - 1. 应具备专门的项目管理工具对项目整个实施过程进行有效的管理；
      2. 应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；
      3. 应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、处理结果等等。
      4. 监督管理

监督管理要求：

服务机构应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。

* + 1. 保障阶段
       1. 系统测评

系统测评要求：

* + - 1. 应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；
      2. 应基于系统的稳定性、承载能力要求，制定系统安全性测评方案，有专门的系统压力测评工具，对系统的稳定性进行测评；
      3. 应由第三方机构进行系统测评，出具系统测评报告，提交服务对象，作为初次验收依据。
      4. 应依据系统安全测评的要求，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。
      5. 系统试运行

系统试运行要求：

* + - 1. 应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；
      2. 应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；
      3. 应提供三个月以上的试运行记录和报告；
      4. 应对系统试运行中存在的问题及时整改，由第三方机构进行回归测试合格后，进行项目最终验收。

附 录 D

（规范性附录）

信息系统安全运维服务机构评价要求

* 1. 第一级要求
     1. 准备阶段

准备阶段要求：

* + - 1. 应与服务对象进行沟通，对需求达成共识，确定服务内容，主要包括初始服务、安全设备运维、日常巡检服务、病毒查杀、安全事件审计、安全加固、漏洞扫描服务、渗透测试服务、风险评估等；
      2. 应明确安全运维方式，包括驻场值守方式、定期巡检方式、远程值守方式等。
    1. 实施阶段

实施阶段要求：

* + - 1. 初始服务，主要应包括资产识别、定期配置项的更新和维护、实施相关安全运维流程；
      2. 安全设备运维服务，主要应包括日常维护、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、安全加固、漏洞扫描服务、渗透测试服务等，对安全设备出现的故障进行统计记录。
    1. 评审阶段

评审阶段要求：

应定期收集和分析网络安全运维报告的数据，包括异常报告及时率、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、安全事件次数等。

* + 1. 改进阶段

改进阶段要求：

在运维过程和监视过程中应识别改进项目，制定持续改进计划。

* 1. 第二级要求
     1. 基本要求

除满足一级能力要求外，还应满足D.2.2～D.2.5的要求。

* + 1. 准备阶段

准备阶段要求：

应对信息网络系统相关的IT资产进行识别，约定安全运维服务方式、检查频次和检查内容等。

* + 1. 实施阶段

实施阶段要求：

* + - 1. 日常巡检服务，主要应包括安全设备监控、病毒监测、查杀及网络防病毒维护，且形成相关记录；
      2. 健康检查服务，主要应包括安全设备、业务系统、漏洞扫描、渗透测试的健康检查服务；
      3. 应具有处置一般突发性网络安全事件的能力；
      4. 应具有根据业务的需要熟练地使用成熟工具和安全加固的能力。该工具应是正版授权使用或者购买获得。
    1. 评审阶段

评审阶段要求：

应建立和分析服务对象的满意度调查记录。

* + 1. 改进阶段

改进阶段要求：

* + - 1. 应具有文件化的程序，用以识别、记录、批准、评估、测量和报告改进措施；
      2. 应采取预防措施，消除潜在不符合项的原因，防止其发生。
  1. 第三级要求
     1. 基本要求

除满足二级能力要求外，还应满足D.3.2～D.3.5的要求。

* + 1. 准备阶段

准备阶段要求：

* + - 1. 应识别与分析信息网络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；
      2. 应分析服务对象对信息网络系统安全服务的需求和类型，编写安全运维服务目录，包括运维监控与分析、终端安全监控、合规性运维等；
      3. 应建立信息网络系统安全运维的问题管理程序；
      4. 应建立知识管理程序及初步形成知识库；
      5. 应编制信息网络系统的可用性计划，监控可用性事件，报告可用性执行，指导可用性的改进；
      6. 采用流程化管理方法，应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。
    1. 实施阶段

实施阶段要求：

* + - 1. 应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；
      2. 实施安全事件审计服务，应包括网络及安全设备日志和服务器、操作系统、网络应用等日志，并进行记录；
      3. 应组建运维服务台职能，培养服务台人员的专业能力；
      4. 应建立网络安全事件管理程序和服务请求管理程序；
      5. 应实施运维监控与分析并形成记录。
    1. 评审阶段

评审阶段要求：

* + - 1. 应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；
      2. 应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要求，并有效实施和维护；
      3. 应定期回顾安全运维服务，确保其持续适用和有效；
      4. 管理评审输入，应包括服务对象反馈、服务流程执行情况的符合性，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和改进机会等。
    1. 改进阶段

改进阶段要求：

* + - 1. 改进机会应划分优先级，策划被批准的改进机会；
      2. 改进活动应进行管理，包括设定改进目标、确保批准的改进活动被实施、报告被实施的改进计划等。
  1. 第四级要求
     1. 基本要求

除满足三级能力要求外，还应满足D.4.2～D.4.5的要求。

* + 1. 准备阶段

准备阶段要求：

* + - 1. 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；
      2. 应基于信息网络系统安全的生命周期，建立安全运维的整体策略；
      3. 应编制安全运维项目作业指导书；
      4. 建设实施过程中应关注系统的功能、性能和安全性方面要求；
      5. 改造过程中应制定测试计划及回退措施；
      6. 编写安全运维服务目录，应包括安全通告、漏洞分析、应急响应服务等；
      7. 应有自主研发的安全工具，并且具备著作权或者专利权证书。基于安全测试流程管理，进行标准化的信息网络系统安全运维工作；
      8. 应建立系统应急事件响应机制和恢复保障；出现安全事故时，要详细记录事故的起因、现象、影响、处理方式、处理结果等，并且形成文档；
      9. 应建立应急响应和灾难恢复机制，形成业务连续性计划。
    1. 实施阶段

实施阶段要求：

* + - 1. 实施安全通告及漏洞分析服务：应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；
      2. 对已发现的信息网络系统安全漏洞及风险，应进行系统安全加固与优化；
      3. 实施应急响应服务：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；
      4. 应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；
      5. 应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响应。
    1. 评审阶段

评审阶段要求：

* + - 1. 应形成体系化的运维质量审核机制和体系化的服务监视管理，形成审核机制；
      2. 应定期评审服务对象对安全运维服务的满意度。
    1. 改进阶段

评审阶段要求：

* + - 1. 持续服务改进，应形成持续服务改进文化和意识；
      2. 应基于运维服务的缺陷，提出改进策略和方案。

附 录 E

（规范性附录）

监测预警服务机构评价要求

* 1. 第一级要求
     1. 准备阶段

准备阶段要求：

1. 应制定监测预警服务规范和流程；
2. 应了解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；
3. 应取得服务对象的监测委托书或授权书；
4. 应建有专门部门负责开展网络安全监测预警服务工作。
   * 1. 实施阶段

实施阶段要求：

1. 应建成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；
2. 应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。
   * 1. 总结阶段

总结阶段要求：

1. 应保存监测与预警工作日志；
2. 应及时向服务对象提供安全通报或预警通报。
   1. 第二级要求
      1. 基本要求

除满足一级能力要求外，还应满足E.2.2～E.2.4的要求。

* + 1. 准备阶段

准备阶段要求：

1. 应具备专用监测平台、工具或仪器设备，对目标系统及设备进行安全监测与预警；
2. 接收监测预警任务后，应明确监测内容，并对内容进行详细解读，明确与服务对象之间的服务级别协议，明确项目成员及项目负责人。
   * 1. 实施阶段

实施阶段要求：

应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。

* + 1. 总结阶段

总结阶段要求：

应定期为服务对象提供安全监测预警的总结和分析报告。

* 1. 第三级要求
     1. 基本要求

除满足二级能力要求外，还应满足E.3.2～E.3.4的要求。

* + 1. 准备阶段

准备阶段要求：

1. 应具有自建的网络安全监测预警平台；
2. 应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；
3. 应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方案。
   * 1. 实施阶段

实施阶段要求：

1. 部署监测预警平台或将监测目标加入安全监测预警平台前，应对监测目标进行安全监测影响分析和测试，形成分析、测试报告，报告通过服务对象审查；
2. 在服务期间应提供不间断的实时监测与预警服务；
3. 应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。
   * 1. 总结阶段

总结阶段要求：

1. 应向服务对象提供安全监测分析报告；
2. 应向服务对象提供安全应急处置预案；
3. 应定期向服务对象提供网络安全威胁情报。
   1. 第四级要求
      1. 基本要求

除满足三级能力要求外，还应满足E.4.2～E.4.4要求。

* + 1. 准备阶段

准备阶段要求：

应建有独立的监测预警和应急指挥中心。

* + 1. 实施阶段

实施阶段要求：

1. 应建立与网络安全监测预警一致的、完善的企业管理信息系统，系统能有效运行并支撑企业信息安全监测预警服务工作的开展；
2. 应实现安全监测预警指令全流程线上闭环管理。
   * 1. 总结阶段

总结阶段要求：

主要应参照监测预警服务的三级要求总结阶段执行。

附 录 F

（规范性附录）

应急响应服务机构评价要求

* 1. 第一级要求
     1. 准备阶段

准备阶段要求：

* + - 1. 应明确服务对象应急需求内容；
      2. 应向服务对象提供应急处理服务流程；
      3. 应具备本市内6小时、外地8小时应急响应服务能力；
      4. 应配备应急处理服务人员，能处理一般网络安全事件能力。
    1. 检测阶段

检测阶段要求：

* + - 1. 应确定检测对象及范围，并得到用户的授权；
      2. 应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，与服务对象共同确定应急处理方案。
    1. 抑制阶段

抑制阶段要求：

* + - 1. 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；
      2. 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；
    1. 根除阶段

根除阶段要求：

应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。

* + 1. 恢复阶段

恢复阶段要求：

* + - 1. 在帮助服务对象重建系统前应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；
      2. 应告知服务对象系统的恢复方法及可能存在的风险；
      3. 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；
      4. 系统恢复后，应通过备份数据对系统数据进行恢复。
    1. 总结阶段

总结阶段要求：

应对事件处理过程进行总结和分析。

* 1. 第二级要求
     1. 基本要求

除满足一级能力要求外，还应满足F.2.2～F.2.7的要求。

* + 1. 准备阶段

准备阶段要求：

* + - 1. 应具备本地4小时、外地6小时应急响应服务能力；
      2. 应配备处理网络安全事件的工具包，并提供工具包定期更新记录。
    1. 检测阶段

检测阶段要求：

* + - 1. 应与服务对象确认应急响应检测范围，实施检测时应经服务对象授权同意，机密性数据信息未经授权不应访问；
      2. 应与服务对象充分沟通，评估应急处理方案可能造成的影响。
    1. 抑制阶段

抑制阶段要求：

* + - 1. 应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；
      2. 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。
    1. 根除阶段

根除阶段要求：

* + - 1. 应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；
      2. 应找出导致安全事件发生的原因，并予以消除或控制。
    1. 恢复阶段

恢复阶段要求：

应协助客户验证恢复后的系统是否运行正常，并确认与原有系统保持一致。

* + 1. 总结阶段

总结阶段要求：

* + - 1. 应提供事件处理报告；
      2. 应提供建议和意见，并协助服务对象对系统安全建设进行完善。
  1. 第三级要求
     1. 基本要求

除满足二级能力要求外，还应满足F.3.2～F.3.7的要求。

* + 1. 准备阶段

准备阶段要求：

* + - 1. 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，要协助建立；
      2. 应向服务对象提供规范化应急处理服务流程；
      3. 应具备本地2小时、外地4小时应急响应服务能力；
      4. 应对网络安全事件工具包实行制度化管理；
      5. 应具有处理较大网络安全事件的能力。
    1. 检测阶段

检测阶段要求：

* + - 1. 应建立有针对常规应用系统、安全设备、常见网络安全事件的检测技术规范；
      2. 应协助服务对象确定安全事件等级；
      3. 根据应急预案制定本次应急方案，应急处理方案应包含实施方案失败的应变和回退措施。
    1. 抑制阶段

抑制阶段要求：

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，并达成协议。

* + 1. 根除阶段

根除阶段要求：

* + - 1. 应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，并协助客户进行实施；
      2. 应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；
      3. 应找出导致网络安全事件发生的原因，并予以消除。
    1. 恢复阶段

恢复阶段要求：

* + - 1. 应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；
      2. 应帮助服务对象对重建后的系统建立备份。
    1. 总结阶段

总结阶段要求：

* + - 1. 应及时检查事件处理记录是否具备可追溯性，并对处理过程进行总结和分析；
      2. 应提供详实的事件处理报告。
  1. 第四级要求
     1. 基本要求

除满足三级能力要求外，还应满足F.4.2～F.4.7的要求。

* + 1. 准备阶段

准备阶段要求：

* + - 1. 应建立有体系化的应急处理服务流程；
      2. 应具备本地7\*24小时、外地4小时应急响应服务能力；
      3. 应具有自主开发专业检测工具的能力；
      4. 应具有处理重大及特别重大网络安全事件的能力。
    1. 检测阶段

检测阶段要求：

* + - 1. 应建立完善的检测技术规范，并具有应对高技术入侵的检测能力；
      2. 应具有挖掘系统设备及业务系统安全漏洞的能力；
      3. 应保留完整的安全事件的检测步骤和文档，能作为司法程序的相关证据。
    1. 抑制阶段

抑制阶段要求：

* + - 1. 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；
      2. 应具备可靠的网络防御和攻击追踪溯源能力；
      3. 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。
    1. 根除阶段

根除阶段要求：

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。

* + 1. 恢复阶段

恢复阶段要求：

应帮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。

* + 1. 总结阶段

总结阶段要求：

* + - 1. 应对事件进行总结和分析，针对典型案例存入事件知识库；
      2. 应提供详实的事件处理报告，关闭安全事件管理程序；
      3. 应告知服务对象所发生的事件可能涉及法律诉讼方面的法律要求或影响。

附 录 G

（规范性附录）

软件安全服务机构评价要求

* 1. 第一级要求
     1. 准备阶段

准备阶段要求：

* + - 1. 应拥有软件项目安全开发团队不少于5人，安全服务不少于3人并明确各岗位、人员、职责；
      2. 应制定软件项目安全开发管理计划，明确开发过程管控措施；
      3. 应建立软件开发的配置管理计划，明确配置管理的安全要求；
      4. 应建立变更控制制度，明确软件项目变更控制的安全要求；
      5. 应制定软件项目安全培训计划，对相关人员进行安全培训；
      6. 应建立独立的开发环境，确保开发环境与运行环境隔离。
    1. 需求阶段

需求阶段要求：

* + - 1. 调研项目背景信息，应收集项目需求，明确软件功能、性能及安全方面的要求；
      2. 应结合软件项目需求、安全需求，与用户充分沟通，达成共识并形成记录。
    1. 设计阶段

设计阶段要求：

* + - 1. 应根据软件项目需求，编制软件设计说明书；
      2. 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；
      3. 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。
    1. 编码阶段

编码阶段要求：

* + - 1. 应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；
      2. 依据详细设计说明书，应对软件进行安全编码；
      3. 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。
    1. 测试阶段

测试阶段要求：

* + - 1. 依据软件设计说明书应对软件功能、安全功能进行测试；
      2. 应对测试发现的漏洞进行分析并有效修复。
    1. 验收交付
       1. 系统试运行

系统试运行阶段要求：

* + - 1. 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；
      2. 基于系统试运行相关记录，应及时对软件进行调整、维护。
      3. 验收交付

验收交付阶段要求：

* + - 1. 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；
      2. 根据合同约定，应进行项目验收，形成项目验收报告。
    1. 维保阶段

维保阶段要求：

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。

* 1. 第二级要求
     1. 基本要求

除满足一级能力要求外，还应满足G.2.2～G.2.8的要求。

* + 1. 准备阶段

准备阶段要求：

* + - 1. 应拥有软件项目安全开发团队不少于10人，安全服务不少于5并明确各岗位、人员、职责；
      2. 应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；
      3. 应使用配置管理工具对软件项目进行配置管理；
      4. 应配备专职的测试人员；
      5. 应建立独立的测试环境，确保测试环境与开发环境隔离。
    1. 需求阶段

需求阶段要求：

* + - 1. 应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；
      2. 对于数据采集、产生、使用，应明确识别安全保护要求；
      3. 应基于客户需求，开展需求分析，编制具有软件安全需求的分析报告；
      4. 需求分析报告中应明确项目开发中使用的安全技术标准、规范。
    1. 设计阶段
       1. 概要设计

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

* + - 1. 详细设计

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

* + 1. 编码阶段

软件代码的安全检查、评审工作应形成记录。

* + 1. 测试阶段
       1. 单元测试

单元测试要求：

* + - 1. 应明确单元测试策略，制定单元测试计划；
      2. 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。
      3. 集成测试

集成测试要求：

* + - 1. 应明确集成测试策略，制定集成测试计划；
      2. 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。
      3. 系统测试

系统测试要求：

* + - 1. 应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；
      2. 应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；
      3. 应对系统测试结果进行分析，形成分析报告。
    1. 验收交付
       1. 系统试运行

试运行结束后，应制定系统试运行报告，并提交客户。

* + - 1. 验收交付

应提交软件安全测评报告。

* + 1. 维保阶段

维保阶段要求：

* + - 1. 应制定系统运行计划、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；
      2. 应及时应对突发安全事件，并向用户提供安全事件解决报告。
  1. 第三级要求
     1. 基本要求

除满足二级能力要求外，还应满足G.3.2～G.3.8的要求。

* + 1. 准备阶段

准备阶段要求：

* + - 1. 应拥有软件项目安全开发团队不少于15人，安全服务不少于7人并明确各岗位、人员、职责；
      2. 应建立软硬件设备和工具等资源安全使用规范；
      3. 应配备安全管理人员；
      4. 应建立变更控制委员会。
    1. 需求阶段

需求阶段要求：

* + - 1. 应基于软件安全威胁开展需求分析；
      2. 应基于软件项目需求分析建立软件安全开发模型。
    1. 设计阶段
       1. 概要设计

概要设计要求：

* + - 1. 概要设计说明书中应明确基于软件安全威胁分析的安全要求；
      2. 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。
      3. 详细设计

应依据安全设计和概要说明书，明确基于软件安全威胁分析进行详细设计。

* + 1. 编码阶段

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

* + 1. 测试阶段
       1. 单元测试

应对单元测试结果进行分析，形成分析报告。

* + - 1. 集成测试

应对集成测试结果进行分析，形成分析报告。

* + - 1. 系统测试

应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。

* + 1. 验收交付
       1. 系统试运行

系统试运行验收要求：

* + - 1. 应提供1个月以上的试运行记录和报告；
      2. 应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。
      3. 验收交付

应提交软件产品第三方安全测评报告或安全认证证书。

* + 1. 维保阶段

维保阶段要求：

* + - 1. 应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；
      2. 应根据健康检查报告进行分析，持续优化系统。
  1. 第四级要求
     1. 基本要求

除满足三级能力要求外，还应满足G.4.2～G.4.8的要求。

* + 1. 准备阶段

应拥有软件项目安全开发团队不少于20人，软件安全服务10人并明确各岗位、人员、职责。

* + 1. 需求阶段

应基于软件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。

* + 1. 设计阶段

应基于软件软件的业务流程开展安全威胁和安全隐进行详细设计，如：隐私影响评级。

* + 1. 编码阶段

开发团队使用的编辑器、链接器等相关工具，应与团队进行安全分析来决定是否使用，并对源代码以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。

* + 1. 测试阶段

测试阶段要求：

* + - 1. 应进行额外的模糊测试，增加模糊测试范围和持续时间；
      2. 测试结果应体现多少条符合条款，多少条不符合条款，不符合条款的编号并分析可能造成的严重后果。
    1. 验收交付
       1. 系统试运行

系统试运行验收要求：

* + - 1. 应提供3个月以上的试运行记录和报告；
      2. 应提供对可能发生的软件功能方面级安全方面提供可靠性指导说明书。
      3. 验收交付

应提交软件产品第三方安全测评报告或安全认证证书。

* + 1. 维保阶段

维保阶段要求：

* + - 1. 审计人员应采取措施来识别报告的问题是否有效解决；
      2. 对于未修改的提供理由，理由应合理，需从安全方面及业务需求方面进行综合分析；
      3. 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；
      4. 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 H

（规范性附录）

工业控制系统安全服务机构评价要求

1. 第一级要求
   1. 基本要求
2. 应拥有1名获得工业控制系统安全专业认证技术人员；
3. 近一年应具备1个工业控制系统安全服务相关成功案例。
   1. 能力要求
4. 应具备工业控制系统资产识别、脆弱性识别、威胁识别的能力；
5. 应具备根据《工业控制系统安全测评扩展要求》、《工业控制系统信息安全防护指南》开展管理制度检查、安全配置核查、漏洞扫描的能力；
6. 应具备编制核查、漏洞问题清单，提供加固建议的能力；
7. 应具备工业控制系统安全风险分析和提出安全风险处置能力。
8. 第二级要求

除满足一级能力要求外，还应满足H.2.1～H.2.2的要求。

1. 基本要求
2. 应拥有2名获得工业控制系统安全专业认证技术人员及5名以上信息安全专业技术人员；
3. 近一年应具备3个工业控制系统安全服务相关成功案例。
4. 能力要求
5. 应具备修复工业控制系统安全漏洞及补丁的能力；
6. 应具备提供工业控制系统安全软件选择与管理能力，如集成工业控制系统防病毒软件、应用程序白名单软件；验证和测试安全管理软件的功能性、兼容性及安全性等；为服务对象建立防病毒和恶意软件入侵管理机制等；
7. 应具备提供工业控制系统安全配置和补丁管理能力，如何修复工业控制系统安全漏洞及补丁；提供重大工控安全漏洞及其补丁情报；为服务对象建立相应的配置清单、配置变更管理机制等。
8. 第三级要求

除满足二级能力要求外，还应满足H.3.1～H.3.2的要求。

1. 基本要求
2. 应拥有5名获得工业控制系统安全专业认证技术人员及15名以上信息安全专业技术人员、2名以上自动化专业技术人员；
3. 近一年应具备8个工业控制系统安全服务相关成功案例；
4. 应至少拥有1-2款自主知识产权的数据安全相关产品，且有成功建设案例；
5. 应具备工业控制系统漏洞挖掘能力，并向CNVD或CNNVD提交过2个以上的漏洞。
6. 能力要求
7. 应具备工业控制系统边界安全防护、安全审计、视频监控等设备系统的集成服务能力，如工业防火墙、工业网闸、单向隔离设及企业定制的边界安全防护网关等；
8. 应具备工业控制系统安全监测服务能力，如对网络攻击和异常行为进行识别、报警、记录的网络安全监测；
9. 应具备工业控制系统安全应急响应服务能力，如应急预案制定（应急计划的策略和规程、应急计划培训、应急计划测试与演练、应急处理流程、事件监控措施、应急事件报告流程、应急支持资源、应急响应计划等内容。）；应急演练（桌面演练、单项演练、综合演练等）；安全事件的处置等。
10. 第四级要求

除满足三级能力要求外，还应满足H.4.1～H.4.2的要求。

1. 基本要求
2. 应拥有8名获得工业控制系统安全专业认证技术人员及20名以上信息安全专业技术人员、4名以上自动化专业技术人员；
3. 近一年应具备20个工业控制系统安全服务相关成功案例；
4. 应至少拥有5-10款自主知识产权的数据安全相关产品，且有成功建设案例；
5. 应具备工业控制系统漏洞挖掘能力，并向CNVD或CNNVD提交过10个以上的漏洞。
6. 能力要求
7. 应具备工业控制系统安全态势感知服务能力，如整合设备资产、网络流量、安全漏洞、安全配置、安全日志、设备运行状态、业务故障日志等信息，通过大数据分析获取工业控制系统安全风险和态势；
8. 应具备处理工业控制系统所面临的病毒木马、端口扫描、暴力破解、异常流量、异常指令、工业控制系统协议包伪造等网络攻击或异常行为的能力；
9. 应具备提供Modbus、S7、Ethernet/IP、OPC等主流工业控制系统协议进行深度包检测、分析和过滤的防护设备的能力；
10. 应具备提供物理和环境安全防护、身份认证、远程访问、资产安全、数据安全、供应链管理的工业控制系统综合安全解决方案的能力。如双因子认证系统；基于国密的IPS/SSLVPN技术；资产管理系统；数据加密、脱敏、审计等防护治理系统等；
11. 应具备为服务对象建立工业控制系统安全管理、安全防护技术、业务连续性等体系的服务能力。

附 录 I

(规范性附录）

数据安全服务机构评价要求

1. 第一级要求
2. 基本要求
3. 应具有2名获得数据安全认证的专业技术人员和1名及以上的数据库技术人员；
4. 应具有1个数据安全服务相关成功案例；
5. 应具备提供基于Oracle\mysql\mssql等通用OLTP关系型数据类型的安全检测、评估等能力。
6. 能力要求
7. 应具备根据服务对象的数据安全目标及业务现状，编制《数据安全风险评估方案》的能力，方案内容可包括评估目标、评估对象、评估内容、评估方法、评估流程、评估工具、评估人员安排、评估计划、项目管理、交付物等；
8. 应具备根据服务对象的数据安全目标及业务现状，制定《数据分类分级方案》，并提供数据资产梳理，对生成/采集的数据进行数据分类分级的标示，提供数据资产可化管理的服务能力，如数据分布管理、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；
9. 应具备数据安全脆弱性识别能力、威胁识别能力；
10. 应具备根据相关法规、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能力；
11. 应具备编制核查及漏洞问题清单，提供加固建议的能力；
12. 应具备数据安全风险分析，提供风险处置建议的能力。如重要数据的种类、数量，收集、存储、加工、使用数据的情况，面临的数据安全风险及其应对措施等。
13. 第二级要求

除满足一级能力要求外，还应满足I.2.1～I.2.2的要求。

1. 基本要求
2. 应具有4名获得数据安全认证的专业技术人员和2名及以上的数据库技术人员；
3. 应具有3个数据安全风险检测、评估、治理相关成功案例；
4. 应具备本地6小时、外地24小时应急响应服务能力；
5. 应具有基于oracle\mysql\mssql\DB2\达梦\南大通用\人大金仓等通用OLTP关系型数据类型的安全防护、安全应急、安全加固等能力。
6. 能力要求
7. 应具备数据安全应急响应服务能力，如编制数据安全应急预案、演练方案、开展应急演练并记录、处理应急安全事件等；
8. 应具备数据安全加固服务能力，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；
9. 应具备数据安全审计、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的集成能力，如技术方案、实施方案及计划、技术白皮书、操作手册等；
10. 应具备项目管理能力，如制定项目实施及管理计划，对进度、范围、变更、沟通等进行有效管理。
11. 第三级要求

除满足二级能力要求外，还应满足I.3.1～I.3.2的要求。

1. 基本要求
2. 应具有8名获得数据安全认证的专业技术人员和3名及以上的数据库技术人员和30名及以上研发人员；
3. 应具有5个数据安全风险检测、评估、治理相关成功案例；
4. 应具备本地3小时、外地12小时应急响应服务能力；
5. 应具有基于OLTP结构化数据、非结构化数据、OLAP分布式数据仓库等数据类型的安全检测、防护、应急响应、方案设计等能力；
6. 应至少拥有1-2款自主知识产权的数据安全相关产品，且有成功建设案例；
7. 应具备数据库系统漏洞挖掘能力，并向CNVD或CNNVD提交过2个以上的漏洞；
8. 应具备标准化项目实施方案、工作流程、过程文件、报告等交付物模版；
9. 应符合国内或国际质量管理体系标准要求。
10. 能力要求
11. 应具备数据安全流转监控、数据安全集中管控、数据安全接入认证、数据加密网关等系统平台的集成服务能力。如技术方案、实施方案及计划、技术白皮书、操作手册等；
12. 应具备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；
13. 应具备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；
14. 应具备项目质量管控能力，有效实施质量控制，做好质量管控记录；
15. 应具备项目风险管控能力，跟踪实施过程，执行必要的风险管控措施，做好相关记录。
16. 第四级要求

除满足三级能力要求外，还要满足I.4.1～I.4.2的要求。

1. 基本要求
2. 应具有10名获得数据安全认证的专业技术人员和6名及以上的数据库技术人员和30名及以上研发人员；
3. 应具有10个数据安全风险检测、评估、治理相关成功案例；
4. 应具备提供本地驻场服务能力；
5. 应具有基于OLTP结构化数据、非结构化数据、OLAP分布式数据仓库、大数据平台等数据类型的安全检测、防护、应急响应、方案设计、数据安全治理等能力；
6. 应至少拥有5-10款自主知识产权的数据安全相关产品，且有成功建设案例；
7. 应符合国内或国际质量管理体系标准要求；
8. 应符合国内或国际信息安全管理体系标准要求。
9. 能力要求
10. 应具备数据安全治理体系方案设计及集成服务能力，包括不限于以下方案：
11. 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；
12. 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；
13. 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；
14. 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；
15. 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；
16. 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；
17. 数据供应链管理方案，包括数据供应链、数据服务接口。
18. 应具备数据安全态势感知服务能力，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；
19. 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能力，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；
20. 应面向服务对象开展数据安全培训，提升员工的数据安全意识和数据安全能力水平。

附 录 J

(规范性附录）

信息安全风险评估服务机构评价要求

1. 第一级要求
2. 准备阶段
3. 服务需求界定
4. 应确定评估目标，并充分了解评估对象，了解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，确定系统执行的关键功能，并确定执行这些功能所需的特定系统资源；
5. 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：
   * 业务系统的业务逻辑边界；
   * 网络及设备载体边界；
   * 组织管理权限边界；
   * 其他。
6. 服务方案制定
7. 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；
8. 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。
9. 人员和工具准备
10. 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；
11. 应根据评估的需求准备必要工具。
12. 风险识别阶段
13. 资产识别
14. 应参考国家或国际标准，对资产进行分类；
15. 应识别重要信息资产，行程资产清单；
16. 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；
17. 对资产应根据其在保密性、完整性和可用性上的等级分析分析结果，经过综合评定进行赋值。
18. 脆弱性识别
19. 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；
20. 应对脆弱性进行赋值；
21. 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。
22. 威胁识别
23. 应该参考国家或国标标准，对威胁进行分类；
24. 应识别所评估信息资产存在的潜在威胁；
25. 应识别威胁利用脆弱性的可能性；
26. 应分析威胁利用脆弱性对组织可能造成的影响；
27. 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；
28. 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。
29. 已有安全措施确认
30. 应识别组织已采取的安全措施；
31. 应评价已采取的安全措施的有效性。
32. 风险分析阶段
33. 风险分析模型建立
34. 应构建风险分析模型；
35. 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；
36. 应根据分析模型确定的方法计算出风险值。
37. 风险评价

应根据风险评价准则确定风险等级。

1. 风险评估报告
2. 应向客户提供风险评估报告；
3. 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。
4. 第二级要求
5. 基本要求

除满足一级能力要求外，还应满足J.2.2～J.2.4的要求。

1. 准备阶段
2. 人员和工具准备
3. 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；
4. 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。
5. 风险识别阶段
6. 威胁识别

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。

1. 风险分析阶段
2. 风险分析模型建立

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。

1. 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。

1. 风险评价

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。

1. 风险评估报告
2. 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；
3. 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。
4. 风险处置阶段
5. 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。

1. 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。

1. 第三级要求
2. 基本要求

除满足二级能力要求外，还要满足J.3.2～J.3.4的要求。

1. 准备阶段
2. 人员和工具准备

应采取相关措施，保障工具管理的规范性。

1. 风险识别阶段
2. 脆弱性识别

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。

1. 威胁识别

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。

1. 风险处置阶段
2. 组织评审会
3. 应协助被评估组织召开评审会；
4. 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。
5. 残余风险处置
6. 应对组织提出完整的风险处置方案；
7. 必要时，应对残余风险进行再评估。
8. 第四级要求

满足三级能力全部要求。

附 录 K

(规范性附录）

云计算安全服务机构评价要求

1. 第一级要求
   * + 1. 基础能力要求
2. 服务团队应至少具有5人的服务团队和5人的软件技术团队；
3. 服务机构成立组织机构，应确定项目负责人和安全负责人，其中项目负责人和安全服务负责人应具备2年以上计算机信息系统安全服务领域工作经历，安全负责人具有相应安全资质；
4. 服务机构应至少有1项计算机信息系统安全服务项目，工程按合同要求质量合格，已通过验收并投入实际应用；
5. 应具备本地12小时、外地24小时应急响应服务能力；
6. 应提供云计算安全服务完整解决方案，能制定持续改进计划并实施。
   * + 1. 云计算安全技术要求
7. 安全运营技术
8. 应具备身份鉴别能力。应具备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；
9. 应具备授权管理能力。应具备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。
10. 应具备安全审计能力。应具备建立操作日志能力，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；
11. 应具备实时监控和可视化展示能力。应有能力对云基础设施、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；
12. 应具备安全漏洞和补丁管理能力。应具备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；
13. 应具备安全事件分析和告警的能力。应具备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。
14. 安全防护技术
15. 应具备为云计算环境提供入侵防范、恶意代码防范安全防范措施的能力；
16. 应具备入侵检测能力、实时监测能力、被动响应能力；
17. 应具备云计算环境下的风险评估能力；
18. 应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。
    * + 1. 云计算安全管理要求
           1. 安全策略

应建立相应云计算安全服务流程，并进行规范，确保流程合规，满足相关法律法规要求。

* + - * 1. 组织人员

1. 对安全团队应制定相应团队管理流程，明确安全团队的职责以及能力；
2. 应设立安全管理员等负责人岗位，明确岗位职责；
3. 应定期开展针对各岗位人员安全相关的安全知识和技能培训，并进行考核。
   * + - 1. 云资产管理
4. 服务机构应掌控和确保云IT资产合规性，对于资产数据进行不同方式展现；
5. 服务机构应具备批量对于IT设备进行升级、加固等操作的能力；
6. 服务机构应制定云资产清单。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。
   * + - 1. 云计算运营管理

针对云服务，应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。

* + - * 1. 合规性管理

应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。

* + - * 1. 安全评估

1. 应具备对云计算环境下的运营资产安全风险评估的能力；
2. 评估应包括但不限于系统安全评估和网络安全评估；
3. 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；
4. 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。
   * + - 1. 应急管理

应明确相关安全事件的应急响应要求和处置流程。

* + - * 1. 安全监管

1. 对于制定的云服务安全运营、安全防护、安全管理要求，应具备落实情况并进行监管的能力；
2. 对发现的问题、识别的风险应具备进行督促整改的能力。
3. 第二级要求
4. 本级应在满足第一级保护要求的基础上，还要满足K.2.1～K.2.3的评价条件；
5. 本级安全服务机构能提供的安全技术和安全管理能力应不低于等级保护二级的要求。
6. 基础能力要求
7. 服务团队应至少具有10人的服务团队和10人的软件技术团队；
8. 服务机构的组织机构中项目负责人和安全服务负责人应具备3年以上计算机信息系统安全服务领域工作经历；
9. 近3年完成计算机信息系统安全服务项目总额600万元以上；服务费用（含系统设计费、软件开发费、系统集成费和技术服务费）应占工程项目总额的30％以上；
10. 具有落地的专用平台支撑服务方案或行业解决方案。
11. 云计算安全技术要求
12. 安全运营技术
13. 应具备身份鉴别能力。应建立统一的身份认证机制，对系统用户实现统一身份管理；
14. 应具备授权管理能力。应建立统一的权限管理机制，实现系统用户的统一授权；应在基于主体角色的授权机制基础上建立基于客体属性的授权机制；应建立基于共享、开放任务的访问控制授权机制；
15. 应具备安全审计能力。应定期对日志进行监测审计、对操作异常行为进行识别分析，并对安全风险进行整改；
16. 应具备实时监控和可视化展示能力。应能够针对不同用户的角色提供多样化的数据和监控呈现模式，同时应具备支持WEB端、移动端、大屏等多种展示方式的能力；
17. 应具备安全漏洞和补丁管理能力。应具备对云资产的漏洞检查、漏洞跟踪处置、漏洞和补丁统计分析的能力；具备测试并修复云资产漏洞的能力；
18. 应具备安全事件分析和告警的能力。应具备多租户数据文件流转、跨租户访问操作的事件监控和分析能力；应具备唯一且确定的时钟，以保证各种数据的管理和分析在时间上的一致性；
19. 应具备自动化响应与通知的能力。针对安全事件、应急事件等进行自动化响应与通知的措施。
20. 安全防护技术
21. 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；
22. 应具备数据备份与恢复能力。应能够对重要信息进行备份和恢复；应提供关键网络设备、通信线路和数据处理系统的硬件冗余，保证系统的可用性；
23. 应具备恶意代码防范能力。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；
24. 应具备确保数据完整性和一致性检测的能力。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；
25. 应同时具备威胁情报分析与利用能力、主动应急响应能力。
26. 云计算安全管理要求
27. 安全策略
28. 应建立相应的云计算安全管理策略，对云计算服务的操作规范、保护措施、管理人员职责等进行规定；
29. 应建立相应的管理流程、审核制度。
30. 组织人员
31. 应设立安全管理员、安全审计员、数据安全员等负责人岗位，明确岗位职责；
32. 应定期开展针对各岗位人员的安全相关管理规范、流程、制度培训，并进行考核；
33. 应具备攻击防御团队（蓝方）和攻击模拟团队（红方）。
34. 云资产管理
35. 应具有云资产台账。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；
36. 应具备按重要程度对云资产进行标识的方法，规定云资产分类标识的原则和方法。
37. 云计算运营管理
38. 应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；
39. 应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。
40. 合规性管理
41. 应建立管控措施和技术手段，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；
42. 应建立数据监控机制，对相关操作行为进行溯源和合规性分析。
43. 安全评估
44. 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；
45. 应对云计算服务过程进行安全评估，确保服务过程的规范性和安全性；
46. 应定期对安全状况和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。
47. 应急管理
48. 应专门制定数据相关安全事件应急响应要求和处置流程；
49. 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。
50. 安全监管
51. 应具备云资源共享、开放管理相关流程、制度、机制，并对落实情况进行监管的能力；
52. 第三级要求
53. 本级应在满足第二级保护要求的基础上，还要满足K.3.1～K.3.3的评价条件。
54. 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。
55. 基础能力要求
56. 服务团队应至少具有15人的服务团队和15人的软件技术团队；
57. 服务机构的组织机构中项目负责人和安全服务负责人应具备4年以上计算机信息系统安全服务领域工作经历；
58. 近3年应完成计算机信息系统安全服务项目总额2500万元以上，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；
59. 应具备本地6小时、外地12小时应急响应服务能力；
60. 应具备数据安全保障建设规划能力，并能编写整体技术解决方案；
61. 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。
62. 云计算安全技术要求
63. 安全运营技术
64. 应具备身份鉴别能力。应采用数字证书的实名认证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；应采用双因子认证进行用户身份鉴别，应针对重要操作或重要数据的访问建立技术管理者多方认证机制；
65. 应具备授权管理能力。应制定操作主体最小操作权限和最小数据集的规则并执行；应及时收回过期的数据访问权限；
66. 应具备安全审计能力。应确保日志保存期限不少于六个月，且保证记录不可伪造和篡改。
67. 应具备实时监控和可视化展示能力。应具备自主研发的安全管控平台，对安全资产、人员、防护措施等进行综合展示能力；
68. 应具备安全漏洞和补丁管理能力。应具备漏洞信息管理、漏洞发现工具管理、漏洞跟踪管理、补丁信息管理的能力；
69. 应具备安全事件分析和告警的能力。应能对安全事件进行多种条件或维度的筛选，并能进行安全事件的预处理等操作；
70. 应具备自动化响应与通知的能力。应具备与第三方安全设备、防护措施进行自动化响应、联动处置的能力。
71. 安全防护
72. 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；
73. 应具备恶意代码防范能力。应支持防恶意代码软件的统一管理；
74. 应具备进行渗透测试能力、高级安全分析、恶意文件分析能力；
75. 应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；
76. 应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；
77. 机构应安排人员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；
78. 机构应安排安全分析人员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。
79. 云计算安全管理要求
80. 安全策略
81. 应建立相应的责任制度、审计机制、风险识别机制；
82. 应对敏感数据建立有针对性的管理机制和保障措施；
83. 应定期进行安全策略的评审，建立变更审批流程，执行变更。
84. 组织人员
85. 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；
86. 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；
87. 应加强对外部单位技术人员和外协人员的安全管理，必须签署保密协议，不得进行非授权操作，不得复制和泄露任何敏感信息。
88. 云资产管理

应具备将云资产台账按重要程度对资产进行标识的能力，并具备制定信息分类标识的原则和方法的能力，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。

1. 云计算运营管理
2. 应具备自定义、可扩展的安全运营流程管理能力，包括但不限于发起、审批、发布、执行、审核、归档和结束等能力；
3. 应能对安全运营管理的绩效进行量化以及评价。
4. 合规性管理
5. 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；
6. 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。
7. 安全评估
8. 应在安全环境发生变化时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；
9. 应对云计算服务过程进行合规性和安全性评估，评估通过后才再进行执行相关操作规范。
10. 应急管理

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。

1. 安全监管
2. 应具备采用技术手段实施自动化监控和辅助监管的能力；
3. 应定期/不定期进行安全检查，对人员、环境、行为等进行审查；
4. 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；
5. 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；
6. 应定期进行安全评估活动并出具安全评估报告，定对差距实施整改措施。
7. 第四级要求
8. 本级应在满足第三级保护要求的基础上，还要满足K.4.1～K.4.3的评价条件。
9. 本级安全服务机构能提供的安全技术和安全管理能力应不低于等级保护四级的要求。
10. 基础能力要求
11. 服务团队应至少具有20人的服务团队和20人的软件技术团队；
12. 服务机构的组织机构中的项目负责人和安全负责人应具备5年以上计算机信息系统安全服务领域工作经历；
13. 近3年应完成计算机信息系统安全服务项目总额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；
14. 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。
15. 云计算安全技术要求
16. 安全运营技术
17. 应具备安全审计能力。应建立对审计日志的大数据分析与事件挖掘机制，主动发现安全风险和隐患；
18. 应具备安全漏洞和补丁管理能力。应具备对多厂家漏洞检测工具/设备以提供对接、策略下发、任务执行、结果提取的能力；
19. 应具备安全事件分析和告警的能力。应具备对安全事件进行告警生成、场景分析等处理手段，并具备对安全事件分析后攻击溯源的能力；
20. 应具备实时监控和可视化展示能力。应具备自主研发的态势感知平台，可进行灵活配置、多维度定义的视图展现，并根据合规要求展示和输出报表、报告；
21. 应具备自动化响应与通知的能力。对确认的事件告警的自动化响应时间、联动处理响应时间不应超过5分钟。
22. 安全防护
23. 应具备自研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；
24. 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；
25. 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；
26. 应具备根据实际情况不断调整安全防护策略的能力，具备优化安全管理及预警、响应和处理能力；
27. 安全分析人员应定期形成安全报告，并出具加固措施，实施安全整改。
28. 云计算安全管理要求
29. 安全策略

安全策略的评审结果应至少保留10年。

1. 组织人员
2. 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；
3. 应设立专职的数据保护官，不可兼任；
4. 应建立对各岗位人员行为的监控和审计机制。
5. 云资产管理

应规定对不同类数据资产的使用、传输和存储的管理办法。

1. 云计算运营管理

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。

1. 合规性管理

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。

1. 安全评估
2. 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；
3. 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。
4. 应急管理

应具备本地2小时、外地4小时应急响应服务能力。

1. 安全监管

应通过随机约谈相关人员，对安全落实情况进行检查评估。

附 录 L

(规范性附录）

信息系统安全审计服务机构评价要求

## 第一级要求

### 基本要求

1. 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；
2. 应具有1个信息系统审计成功案例；
3. 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。

### 审计过程要求

#### 计划阶段要求

1. 应根据被审计方需求，确定审计对象、审计目的、审计范围；
2. 应组建审计小组，明确相关职责；
3. 应制定审计方案及计划，明确安全审计依据；
4. 应编制业务情况调研表，并按照调研表收集有效信息；
5. 应编制信息系统资产情况调研表，并按照调研表收集信信息。

#### 审计取证与评价阶段要求

1. 应确认审计取证方法，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；
2. 应分析被审计方的组织结构、岗位职责；
3. 应分析被审计方IT管理情况、IT支撑业务的对应关系；
4. 应审查被审计方的信息技术治理情况、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，并提供审计工作底稿。

#### 审计报告阶段要求

1. 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；
2. 应建立审计报告的批准和交付程序，保留交付记录；
3. 应审计工作底稿应经被审计方签字确认。

## 第二级要求

### 基本要求

1. 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；
2. 应具有6个及以上信息系统审计成功案例；
3. 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。

### 审计过程要求

除满足一级能力要求外，还应满足L.2.2.1～L.2.2.3的要求。

#### 计划阶段要求

1. 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；
2. 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；
3. 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。

#### 审计取证与评价阶段要求

1. 应建立信息系统安全审计服务流程；
2. 应制定信息系统安全审计服务规范并按照规范实施；
3. 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），并提供审计工作底稿。

#### 审计报告阶段要求

1. 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；
2. 应要素齐全、格式规范，完整反映审计中发现的重要问题；
3. 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。

## 第三级要求

### 基本要求

1. 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；
2. 应具有10个及以上信息系统审计成功案例；
3. 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；
4. 应符合国内或国际质量管理体系标准要求。

### 审计过程要求

除满足二级能力要求外，还应满足L.3.2.1～L.3.2.3的要求。

#### 计划阶段要求

1. 应搜集并确定检查的部门政策、标准和指南；
2. 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；
3. 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；
4. 应利用应用系统工具来建立和管理审计对象库；
5. 应对信息系统审计的风险进行初步评价；
6. 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；
7. 应编制完整审计调研报告，并说明审计重点审计项。

#### 审计取证与评价阶段要求

1. 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；
2. 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；
3. 应当根据跟踪审计的实施过程和结果编制跟踪审计报告；
4. 审计质量控制程序应覆盖审计质量责任、审计职业道德、审计人力资源、审计业务执行、审计质量监控等；
5. 应建立审计质量控制程序，以确保遵守审计相关法规和准则，作出准确的审计结论。

#### 审计报告阶段要求

1. 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；
2. 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。

## 第四级要求

### 基本要求

1. 应至少具有10名获得信息系统审计师专业认证的技术人员，以及15名及以上安全服务技术人员；
2. 应具有10个及以上信息系统审计成功案例；
3. 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；
4. 应符合国内或国际质量管理体系标准要求；
5. 应符合国内或国际信息安全管理体系标准要求。

### 审计过程要求

除满足三级能力要求外，还应满足L.4.2.1～L.4.2.3的要求。

#### 计划阶段要求

1. 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；
2. 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；
3. 应具备为被审计方提供审计对象管理工具的能力。

#### 审计取证与评价阶段要求

1. 应具备至少利用一种网络安全审计工具执行审计取证的能力；
2. 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；
3. 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；
4. 应至少具备和使用数据分析类、漏洞和缺陷扫描类、系统配置和运行日志检查类等类型的审计工具的能力；
5. 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；
6. 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；
7. 应监督网络安全审计实施的过程；
8. 应定期开展网络安全审计质量检查。

#### 审计报告阶段要求

1. 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；
2. 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；
3. 应利用应用系统工具来归档和保管审计工作底稿；
4. 应具备为被审计方提供审计工作底稿管理工具的能力；
5. 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；
6. 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；
7. 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；
8. 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；
9. 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，必须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；
10. 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；
11. 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 M

(规范性附录）

渗透测试服务机构评价要求

1. 第一级要求
2. 准备阶段

准备阶段要求：

* + - 1. 应了解服务对象渗透测试范围和需求，取得服务对象书面的渗透测试授权书；
      2. 应与用户方签署保密协议，与项目组成员签署保密协议，并开展保密教育；
      3. 应准备渗透测试工具，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，所有工具都有合法正规的来源，对漏洞扫描工具进行漏洞库与规则库更新；
      4. 应制定渗透测试风险告知书，告知用户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措施；
      5. 应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、禁止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；
      6. 应向用户报备渗透测试过程中可能使用的IP地址。

1. 实施阶段

实施阶段要求：

* + - 1. 应对渗透对象进行全面的信息收集，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；
      2. 使用漏洞扫描系统，应对渗透测试目标进行全面漏洞扫描；
      3. 应对被测对象开展渗透测试，保存渗透测试结果；
      4. 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；
      5. 应告知服务对象渗透结束。

1. 报告阶段

报告阶段要求：

* + - 1. 应对已验证存在的安全漏洞进行汇总分析，根据GB/T30279安全漏洞等级划分指南开展漏洞等级判定；
      2. 应对漏洞成因、验证过程、可能造成的危害进行分析，对所有问题提出合理高效安全的解决方案，形成渗透测试报告。

1. 复测阶段

复测阶段要求：

* + - 1. 应对服务对象已整改的漏洞进行复测；
      2. 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。

1. 总结阶段

无要求。

1. 第二级要求

除满足一级能力要求外，还应满足M.2.1～M.2.5的要求。

1. 准备阶段

准备阶段要求：

* + - 1. 应与用户方明确渗透测试目标、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；
      2. 应向用户报备渗透测试过程中可能使用的工具；
      3. 应针对渗透测试过程中可能存在的风险制定应急处置预案。

1. 实施阶段

实施阶段要求：

应具有渗透测试测试表单，表单上列出所有需测试的内容，渗透测试内容全面，渗透测试人员根据测试表单逐项开展测试，并对漏洞扫描和渗透测试结果进行详细记录，包括测试过程产生的冗余数据和文件，留存渗透过程记录，渗透人员签字确认。

1. 报告阶段

实施阶段要求：

测试报告中应包含测试记录、漏洞扫描记录等信息。

1. 复测阶段

复测阶段要求：

应留存复测记录，复测人员在复测记录上签字，同时提交渗透测试复测报告。

1. 总结阶段

无要求。

1. 第三级要求

除满足二级能力要求外，还应满足M.3.1～M.3.5的要求。

1. 准备阶段

准备阶段要求：

* + - 1. 应召开项目启动会议，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；
      2. 应组织项目成员对渗透测试目标的网络环境、资产详情等进行现场或远程调研，根据服务对象需求制定渗透测试方案和实施计划；
      3. 应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。

1. 实施阶段

实施阶段要求：

* + - 1. 应对渗透测试发现的漏洞，有专人负责漏洞的复核；
      2. 当用户提出要求时，应对渗透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。

1. 报告阶段

报告阶段要求：

应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。

1. 复测阶段

复测阶段要求：

* + - 1. 应对服务对象已整改的漏洞进行复测，并安排人员进行复测结果复核；
      2. 当用户提出要求时，应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。

1. 总结阶段

总结阶段要求：

应定期向服务对象提供最新安全漏洞预警。

1. 第四级要求

除满足三级能力要求外，还应满足M.4.1～M.4.5的要求。

1. 准备阶段

准备阶段要求：

* + - 1. 应针对渗透对象的业务需求，包括业务和系统可用性、完整性、保密性要求，针对性的制定渗透测试方案和实施计划；
      2. 应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；
      3. 应具有原创漏洞的挖掘能力，在CNVD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；
      4. 应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。

1. 实施阶段

实施阶段要求：

* + - 1. 漏洞应进一步深入验证，获得用户方的再次确认和授权；
      2. 应对渗透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。

1. 报告阶段

报告阶段要求：

应对服务对象的安全漏洞评估影响范围，给出漏洞处置预案，并形成处置分析报告，报告能被客户认可。

1. 复测阶段

复测阶段要求：

应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。

1. 总结阶段

总结阶段要求：

应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。

参 考 文 献

1. GB/T20261—2006 信息技术系统安全工程能力成熟度模型
2. GB/T30271—2013 信息安全技术信息安全服务能力评估准则
3. GB/T30283—2013 信息安全技术信息安全服务分类
4. RB/T201—2013 信息系统安全集成服务资质认证评价要求
5. YD/T1621—2007 网络与信息安全服务资质评估准则
6. YD/T1799—2008 网络与信息安全应急处理服务资质评估方法
7. YD/T2252—2011 网络与信息安全风险评估服务能力评估方法
8. CCRC-ISV-C01:2018 信息安全服务规范
9. CNCA/CTS0052-2007 信息安全服务资质认证技术规范
10. ISO27001:2005 Informationtechnology-Securitytechniques-Informationsecuritymanagementsystems-Requirements
11. ISO27002:2005 Informationtechnology-Securitytechniques-Codeofpracticeforinformationsecuritycontrols
12. ISO27005:2008 Informationtechnology-Securitytechniques–Informationsecurityriskmanagement

## ICS03.120.20

**A00**

**关键词：网络安全、服务机构、等级评定**