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

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。

在本标准实施过程中，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。

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.org　　电子信箱：cas@china-cas.org

目　　次

前　言

本标准依据 T/CAS 1.1—2017《团体标准的结构和编写指南》编写。

本标准主要起草单位：广东省网络空间安全协会、成都信息网络安全协会、陕西省信息网络安全协会、工业和信息化部电子第五研究所、北京安网联认证服务中心、重庆市信息安全协会、江苏省信息网络安全协会、广西网络安全协会、上海市信息安全行业协会、山东省信息网络安全协会、南宁市信息网络安全协会、金华市信息产业协会、成都工业学院、重庆信息安全产业技术创新联盟、广州华南信息安全测评中心、浙江乾冠信息安全研究院有限公司、安百科技（北京）有限公司、杉树岭网络科技有限公司。

本标准主要起草人：朱江霞、黄丽玲、蒋兆明、刘剑、唐锦奎、鲍厚兵、邓开旭、张昊、张原、郑琼冰、王卫亚、王建、吴敏、刘泽楠、江志聪、李宝强、杨泓彬。

考虑到本标准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。

本标准首次制定。

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

本标准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。

本标准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。

2 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

3 术语和定义

GB/T 27000—2006 界定的以及下述术语和定义适用于本文件。

3.1

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。

3.2

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，以下简称“服务机构”。

3.3

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、专业工具等方面的要求，以下简称“服务等级”。

3.4

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”。

4 网络安全服务类型

4.1 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。

4.2 安全集成服务

服务机构根据服务对象网络与信息系统要求，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。主要包括安全方案设计、实施、测试和验收等。

4.3 安全运维服务

服务机构针对服务对象网络与信息安全问题，通过管理与技术手段保障和提升信息系统安全防护能力所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、安全优化等。

4.4 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。

4.5 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。

4.6 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。

4.7 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。

4.8 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。

5 评定原则与流程

5.1 权威性原则

由评定机构进行评定工作，评定结果在行业内得到普遍承认。

5.2 自愿原则

网络安全服务机构等级评定由网络安全服务企业自愿向相关机构提出申请，然后由评定机构进行评定。

5.3 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标准进行评定，以保证服务能力等级评定在不同区域的一致性。

5.4 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。

5.5 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。

5.6 培训流程

网络安全服务机构等级培训流程按附录 A 的规定执行。

5.7 评定流程

网络安全服务机构等级评定流程按附录 B 的规定执行。

6 基本能力要求

6.1 综述

基本能力要求是对网络安全服务机构的从业时间、法律资格、人员状况、财务资信、制度流程、经营业绩和服务设施等方面的要求。根据服务机构基本能力的不同将其划分为四个级别，从 1 级到 4 级依次递增。

6.2 1 级要求

6.2.1 从业时间

网络安全服务机构的从业时间要求：从事与申报类别一致的网络安全服务。

6.2.2 法律资格

网络安全服务机构的法律资格要求：在中华人民共和国境内注册的、具备相应法律资格的独立法人组织，产权关系明确。

6.2.3 财务资信

网络安全服务机构的财务资信要求：注册资金不低于100万元人民币，近3个月经营状况良好，财务数据真实可信，提供在中华人民共和国境内登记注册的会计师事务所出具的上一年度财务审计报告或近三个月财务报表。

6.2.4 办公场所

网络安全服务机构的办公场所要求：拥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。

6.2.5 人员状况

网络安全服务机构的人员状况要求：

a) 机构负责人拥有1年以上（含1年）信息技术领域管理经历；
b) 技术负责人从事网络安全技术工作1年以上（含1年）；
c) 从事网络安全服务人员5名以上（含5名）；
d) 拥有与申报类别一致的网络安全专业技术人员3名以上（含3名）。

6.2.6 经营业绩

网络安全服务机构的经营业绩要求：年度监督前需签订至少 1 个与申报类别一致的网络安全服务项目。

6.2.7 管理制度

网络安全服务机构的管理制度要求：

a) 具备健全的财务、人力资源管理制度；
b) 建立文档控制程序，明确文档管理职责；
c) 建立项目管理制度和实施细则；
d) 建立专业人员业务技能培训计划和能力考核指标；
e) 制定保密管理制度，明确岗位保密责任；
f) 对服务对象敏感信息和知识产权予以保护；
g) 与相关人员签订保密协议，并进行保密教育。

6.2.8 合同要求

网络安全服务机构的合同要求：

a) 确定网络安全服务范围；
b) 服务内容和手段符合网络安全法律法规要求；
c) 签订网络安全服务合同或服务级别协议（SLA）；
d) 具备满足所涉及安全服务要求的能力，若需向第三方转包应告知客户并得到许可。

6.2.9 服务流程

网络安全服务机构的服务流程要求：

a) 建立与申报类别一致的网络安全服务流程，并按照流程执行；
b) 制定与申请类别一致的网络安全服务规范，并按照规范实施。

6.3 2级要求

6.3.1 从业时间

网络安全服务机构的从业时间要求：从事与申报类别一致的网络安全服务1年（含1年）以上。

6.3.2 法律资格

网络安全服务机构的法律资格要求：在中华人民共和国境内注册的、具备相应法律资格的独立法人组织，产权关系明确。

6.3.3 财务资信

网络安全服务机构的财务资信要求：注册资金不低于300万元人民币，近1年经营状况良好，财务数据真实可信，提供在中华人民共和国境内登记注册的会计师事务所出具的上一年度财务审计报告。

6.3.4 办公场所

网络安全服务机构的办公场所要求：要拥有固定的办公场所和相应的办公条件，办公场所面积100（含100）平方米以上，能够满足机构设置及其业务需要。

6.3.5 人员状况

网络安全服务机构的人员状况要求：

a) 机构负责人拥有2年以上（含2年）信息技术领域管理经历；
b) 技术负责人从事网络安全技术工作2年以上（含2年）；
c) 财务负责人具有财务系列初级以上职称；
d) 从事网络安全服务人员10名以上（含10名）；
e) 拥有与申报类别一致的网络安全专业技术人员6名以上（含6名）。

6.3.6 经营业绩

网络安全服务机构的经营业绩要求：

a) 近二年内签订并完成至少3个与申报类别一致的网络安全服务项目；
b) 近二年完成与申报类别（非安全咨询服务）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；
c) 近二年完成与申报类别（安全咨询服务）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。

6.3.7 管理制度

网络安全服务机构的管理制度要求：

a) 具备健全的财务、人力资源管理制度；
b) 建立文档控制程序，明确文档管理职责；

c) 建立项目管理制度和实施细则；
d) 建立专业人员业务技能培训计划和能力考核指标；
e) 制定保密管理制度，明确岗位保密责任；
f) 对服务对象敏感信息和知识产权予以保护；
g) 与相关人员签订保密协议，并进行保密教育。

6.3.8 合同要求

网络安全服务机构的合同要求：
a) 确定网络安全服务范围；
b) 服务内容和手段符合网络安全法律法规要求；
c) 签订网络安全服务合同或服务级别协议（SLA）；
d) 具备满足所涉及安全服务要求的能力，若需向第三方转包应告知客户并得到许可。

6.3.9 服务流程

网络安全服务机构的服务流程要求：
a) 建立与申报类别一致的网络安全服务流程，并按照流程执行；
b) 制定与申请类别一致的网络安全服务规范，并按照规范实施。

6.4 3级要求

6.4.1 从业时间

网络安全服务机构的从业时间要求：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 3 级资质 2 年（含 2 年）以上。

6.4.2 法律资格

网络安全服务机构的法律资格要求：在中华人民共和国境内注册的、具备相应法律资格的独立法人组织，产权关系明确。

6.4.3 财务资信

网络安全服务机构的财务资信要求：注册资金不低于 500 万元人民币，近 3 年经营状况良好，财务数据真实可信，提供在中华人民共和国境内登记注册的会计师事务所出具的近 3 年财务审计报告。

6.4.4 办公场所

网络安全服务机构的办公场所要求：拥有固定办公场所和相适应的办公条件，办公场所面积 200（含 200）平方米以上，能够满足机构设置及其业务需要。在办公场所中还应有与申报类别一致的基础设施，如监测预警服务机构要求有监测预警的平台、工业控制系统安全服务应有服务对象的信息安全测试床等等。

6.4.5 人员状况

网络安全服务机构的人员状况要求：
a) 机构负责人拥有 3 年以上（含 3 年）信息技术领域管理经历；
b) 技术负责人从事网络安全技术工作 3 年以上（含 3 年）；

c) 财务负责人具有财务系列中级以上职称；
d) 从事网络安全服务人员 20 名（含 20 名）以上；
e) 拥有与申报类别一致的网络安全专业技术人员 10 名（含 10 名）以上。

6.4.6 专业工具

网络安全服务机构的专业工具要求：
a) 具备独立的测试环境及必要的软、硬件设备，用于技术培训和模拟测试；
b) 具备承担与申报类别一致的网络安全服务项目所需的安全工具，如漏洞扫描工具、渗透测试工具、协议分析仪等，并对工具进行管理和版本控制。

6.4.7 经营业绩

网络安全服务机构的经营业绩要求：
a) 近二年内签订并完成至少 6 个与申报类别一致的网络安全服务项目；
b) 近二年完成与申报类别（非安全咨询服务）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；
c) 近二年完成与申报类别（安全咨询服务）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。

6.4.8 管理制度

网络安全服务机构的管理制度要求：
a) 具备健全的财务、人力资源管理制度；
b) 建立文档控制程序，明确文档管理职责；
c) 建立项目管理制度和实施细则；
d) 建立专业人员业务技能培训计划和能力考核指标；
e) 制定保密管理制度，明确岗位保密责任；
f) 对服务对象敏感信息和知识产权予以保护；
g) 与相关人员签订保密协议，并进行保密教育。

6.4.9 合同要求

网络安全服务机构的合同要求：
a) 了解客户及所处的行业对网络安全服务的特定要求；
b) 确定网络安全服务范围；
c) 服务内容和手段符合网络安全法律法规要求；
d) 签订网络安全服务合同或服务级别协议（SLA）；
e) 具备满足所涉及安全服务要求的能力，若需向第三方转包应告知客户并得到书面许可。

6.4.10 服务流程

网络安全服务机构的服务流程要求：
a) 建立与申报类别一致的网络安全服务流程，并按照流程执行；
b) 参照国际或国内标准，建立信息网络安全服务的质量管理体系；
c) 制定与申请类别一致的网络安全服务规范，并按照规范实施。

6.5 4级要求

6.5.1 从业时间

网络安全服务机构的从业时间要求：从事与申报类别一致的网络安全服务5年以上（含5年），或取得网络安全服务4级资质2年（含2年）以上。

6.5.2 法律资格

网络安全服务机构的法律资格要求：在中华人民共和国境内注册的、具备相应法律资格的独立法人组织，产权关系明确。

6.5.3 财务资信

网络安全服务机构的财务资信要求：注册资金不低于1000万元人民币，近3年经营状况良好，财务数据真实可信，提供在中华人民共和国境内登记注册的会计师事务所出具的近3年财务审计报告。

6.5.4 办公场所

网络安全服务机构的办公场所要求：拥有固定办公场所和相适应的办公条件，办公场所面积500（含500）平方米以上，能够满足机构设置及其业务需要。在办公场所中还应有与申报类别一致的基础设施，如监测预警服务机构要求有监测预警的平台、工业控制系统安全服务应有服务对象的信息安全测试床等等。

6.5.5 人员状况

网络安全服务机构的人员状况要求：

a) 机构负责人拥有3年以上（含3年）信息网络技术领域管理经历；
b) 技术负责人从事网络安全技术工作5年以上（含5年）；
c) 财务负责人拥有财务系列高级职称，或取得中级职称3年以上（含3年）；
d) 从事网络安全技术服务人员30名以上（含30名）；
e) 拥有与申报类别一致的网络安全专业技术人员20名以上（含20名）。

6.5.6 专业工具

网络安全服务机构的专业工具要求：

a) 具备独立的测试环境及必要的软、硬件设备，用于技术培训和模拟测试；
b) 具备承担与申报类别一致的网络安全服务项目所需的安全工具，如漏洞扫描工具、渗透测试工具、协议分析仪等，并对工具进行管理和版本控制。

6.5.7 经营业绩

网络安全服务机构的经营业绩要求：

a) 近二年内至少签订并完成10个网络安全服务项目；
b) 近二年完成与申报类别（非安全咨询服务）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；
c) 近二年完成与申报类别（安全咨询服务）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。

6.5.8 管理制度

网络安全服务机构的管理制度要求：

a) 具备健全的财务、人力资源管理制度；
b) 建立文档控制程序，明确文档管理职责；
c) 建立项目管理制度和实施细则；
d) 建立专业人员业务技能培训计划和能力考核指标；
e) 制定保密管理制度，明确岗位保密责任；
f) 对服务对象敏感信息和知识产权予以保护；
g) 与相关人员签订保密协议，并进行保密教育。

6.5.9 合同要求

网络安全服务机构的合同要求：

a) 了解客户及所处的行业对网络安全服务的特定要求；
b) 确定网络安全服务范围；
c) 服务内容和手段符合网络安全法律法规要求；
d) 签订网络安全服务合同或服务级别协议（SLA）；
e) 具备满足所涉及安全服务要求的能力，若需向第三方转包应告知客户并得到书面许可。

6.5.10 服务流程

网络安全服务机构的服务流程要求：

a) 建立与申报类别一致的网络安全服务流程，并按照流程执行；
b) 制定与申请类别一致的网络安全服务规范，并按照规范实施；
c) 参照国际或国内标准，建立网络安全服务的质量管理体系；
d) 参照国际或国内标准，建立信息网络安全管理体系或信息网络技术服务管理体系。

7 专业能力要求

专业能力要求是对安全服务机构在服务过程中的专业技能、专业工具和服务成果等方面的综合要求。各类服务等级根据专业能力的不同分为四个级别，从 1 级到 4 级依次递增，详见本标准附录 C～附录 J。

附 录 A
（规范性附录）
培训流程

开展网络安全服务机构相关培训，按照图 A.1 规定的流程进行。

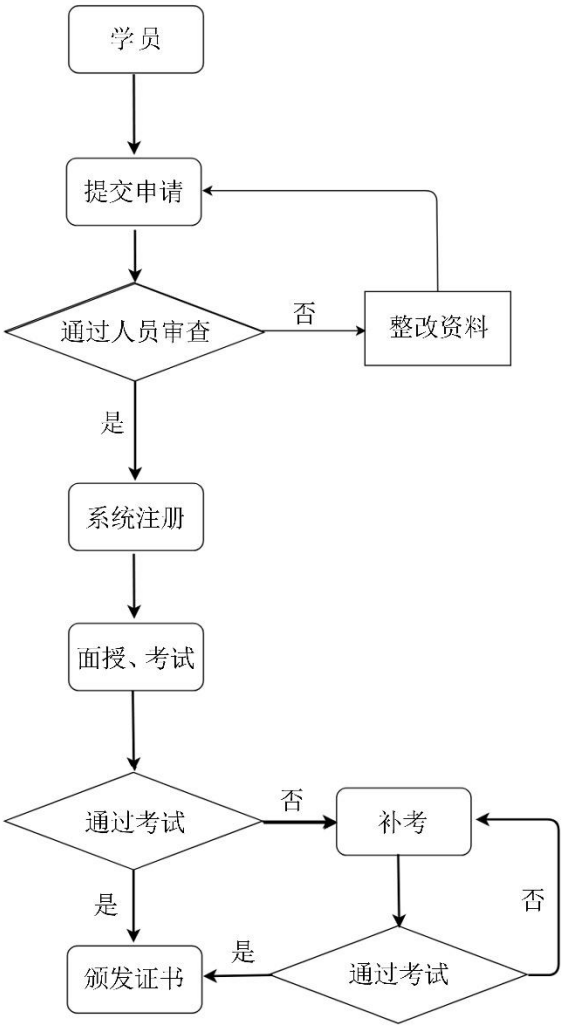

图 A.1 培训流程

附 录 B
（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 B.1 规定的流程进行。

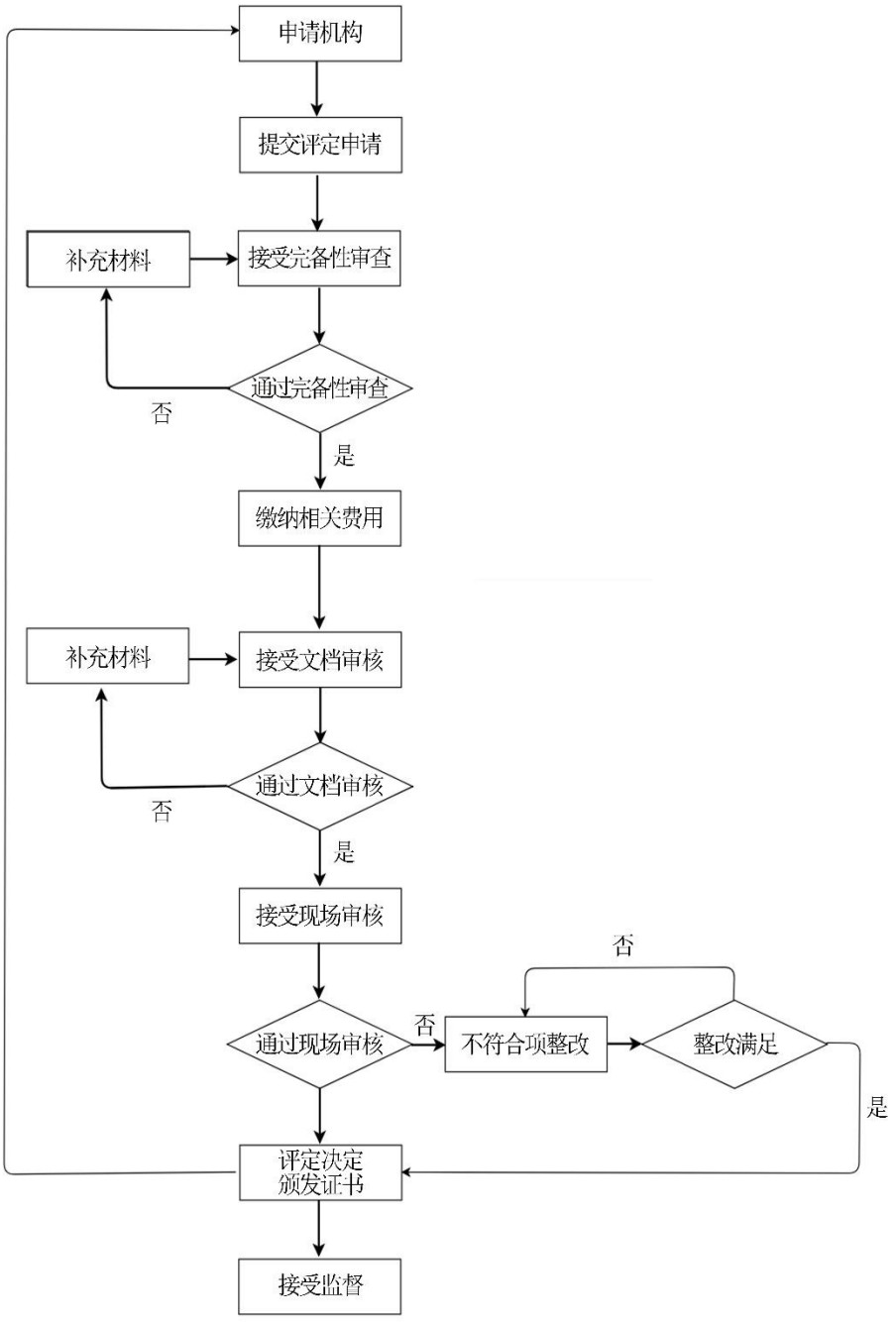

图 B.1 评定流程

附 录 C
（规范性附录）
安全咨询服务机构评价要求

C.1 1级要求

C.1.1 准备阶段

准备阶段要求：服务机构要了解服务对象的安全需求，分析业务状况，进行风险评估，明确实施范围和所需资源，进行前期或后期培训。本阶段包括：

a) 组建不少于3人的安全咨询项目团队，包括技术咨询人员和管理咨询人员，指定项目负责人；
b) 确定安全标准以及客户的要求；
c) 了解服务对象安全现状，分析与有关标准要求的差距；
d) 业务分析：对核心与支持业务以及业务对资源的需求开展访谈调查，完成业务影响分析；
e) 风险评估：对资产、威胁、弱点、风险等做基本的识别与评估。

C.1.2 实施阶段

实施阶段要求：

a) 通过预调研后，咨询顾问制定咨询计划，包括工作方法、日程安排、咨询人员、工作时间、预期目标、大致的费用等，并以书面形式提交客户，作为双方咨询合同商讨的基础；
b) 对客户现有信息网络系统从物理安全、网络安全、应用安全、管理安全等方面进行调查和评估；
c) 分步确定调查目标、制定调查方案、界定调查范围，经审核并协调成功后执行；
d) 通过调查，准确分析出问题及原因，提出可行方案，并为方案实施做必要准备；
e) 分析问题的实质，找出问题的根本原因，同时分析解决问题的可能性与条件，为制定改善方案打下基础；
f) 根据调查及分析结果，形成安全技术风险评估报告、安全管理风险评估报告；
g) 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，对实施方案进行修改；
h) 把正式咨询调查分析的成果及改善方案撰写成文字简练、图示清晰的咨询报告，提交给客户。

C.1.3 验证阶段

验证阶段要求：咨询服务结束后还应为服务对象提供后续服务，对前期咨询服务的目标和效果进行验证。本阶段包括：

a) 定期进行回访；
b) 评述实施的进程，对实施过程中遇到的各种问题给予及时解答；
c) 协助服务对象采取纠正措施，研究是否有新的问题出现。

C.2 2级要求

C.2.1 基本要求

除满足1级能力要求外，还要满足C.2.2～C.2.4的要求。

C.2.2 准备阶段

组建不少于5人的安全咨询项目团队，包括技术咨询人员和管理咨询人员，指定项目负责人。

C.2.3 实施阶段

把正式咨询调查分析的成果及改善方案撰写成文字简练、图示清晰的咨询报告，提交给客户并要求书面确认。

C.2.4 验证阶段

定期进行回访，并形成书面回访记录。

C.3 3级要求

C.3.1 基本要求

除满足2级能力要求外，还要满足C.3.2～C.3.4要求。

C.3.2 准备阶段

准备阶段要求：服务机构要建立总体的安全管理方针，进行详细的风险评估，包括：

a) 组建不少于10人的安全咨询项目团队，包括技术咨询人员和管理咨询人员，并指定项目负责人，咨询人员中至少有5人具有相关信息安全方面的认证；
b) 确定安全标准以及客户的要求，完成安全需求分析报告；
c) 了解服务对象网络安全现状和需求，分析与有关标准要求的差距，结合相关标准找出差距，形成差距分析报告；
d) 对服务对象的资产进行相应的赋值，明确资产的威胁和脆弱点；
e) 确定安全标准以及客户的要求；
f) 了解服务对象安全现状，分析与有关标准要求的差距。

C.3.3 实施阶段

实施阶段要求：服务机构相关项目小组要组织有关资源，依据风险评估结果选择控制措施，为实施有效的风险处理做好计划，同时编写、测试、修订并完善运行和认证所需的文档体系，包括：

a) 帮助客户建立起一套有效的、全面的、多层次安全策略、安全组织和安全运行体系；
b) 针对风险，编写网络安全规划和技术方案；
c) 编写网络安全应急管理制度，并由管理层讨论确认；
d) 配合管理层发布网络安全管理体系文件，并指导管理体系文件的实施；
e) 配合服务对象的应急响应计划进行演练，结合演练情况对计划进行修订；
f) 对全员进行网络安全意识培训，实施推广培训，并进行必要的考核。

C.3.4 验证阶段

验证阶段要求： 服务机构的网络安全体系建立之后，要通过一定时间的试运行来检验其有效性和稳定性。在此阶段，应培训专门人员，建立起内部审核机制，通过内部审计、管理评审来检查已建立的规范是否符合相关标准及已有规范的要求，包括：

a) 对相关人员进行专业技能培训；
b) 配合网络安全管理组织，对网络安全体系的运行情况进行整体审核，并对不合理的地方进行调整、纠正。

C.4 4级要求

C.4.1 基本要求

除满足3级能力要求外，还要满足C.4.2～C.4.4的要求。

C.4.2 准备阶段

准备阶段要求：

a) 组建不少于20人的安全咨询项目团队，包括技术咨询人员和管理咨询人员，并指定项目负责人，咨询人员中至少有10人具有相关网络安全方面的认证资质；
b) 结合相关标准，为服务对象提供标准体系建设、安全审计、管理体系、业务连续性保障等方面的咨询。

C.4.3 实施阶段

实施阶段要求：

a) 挖掘服务对象系统潜在风险，根据服务对象的实际IT应用情况和客观需求，设计出针对性的网络安全基础架构；
b) 能自己开发风险评估工具，对服务对象的信息网络系统进行风险评估，为客户提供相关认证工作的咨询服务；
c) 识别对关键业务功能的潜在威胁，建立有效的备用体系和流程；
d) 制定业务连续性保障计划，协助服务对象改进业务连续性管理体系，从而最大限度地减少突发事件造成的影响；
e) 建立合理的安全备份与恢复机制以及紧急事件的响应机制，并且对事件响应的过程有文档记录，记录包括：起因、现象、影响、处理过程、处理结果等。

C.4.4 验证阶段

验证阶段要求：服务机构要对已有的体系、规范制定审核计划，并定期检查和内部审核，对不符合项形成整改文件。

附 录 D
（规范性附录）
安全集成服务机构评价要求

D.1 1级要求

D.1.1 准备阶段

准备阶段要求：

a) 成立项目实施小组，小组成员包括：设备采购组、项目负责人、项目管理组、实施组，其中实施组成员不少于3人，并应包含网络实施人员及安全策略实施人员；
b) 根据服务对象的需求，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，并编写技术方案；
c) 基于系统建设需求，提出产品选型方案和建设预算；
d) 明确范围、目标、时间、内容、质量等；
e) 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。

D.1.2 设计阶段

设计阶段要求：

a) 根据系统建设需求，编制实施方案；
b) 结合技术方案和实施方案，与客户进行沟通，对方案进行确认。

D.1.3 实施阶段

实施阶段要求：

a) 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；
b) 项目实施人员按时提交施工记录和工程日志，及时向服务对象汇报项目进度；
c) 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。

D.1.4 保障阶段

D.1.4.1 系统测试

系统测试要求：

a) 编写系统联调及测试计划书；
b) 依据系统测试计划，对系统进行联调和系统测试，完整记录测试过程相关信息，形成测试报告，经双方责任人签字确认。

D.1.4.2 系统试运行

系统运行要求：

a) 系统初验后需进行试运行，并记录系统运行状况，试运行周期至少一个月；
b) 基于系统运行情况，及时对系统进行调整和维护。

D.1.5 验收阶段

验收阶段要求：

a) 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；
b) 根据合同约定，组织项目验收，出具项目验收报告。

D.2 2级要求

D.2.1 基本要求

除满足1级能力要求外，还要满足D.2.2～D.2.5的要求。

D.2.2 准备阶段

准备阶段要求：

成立项目实施小组，小组成员包括：设备采购组、项目负责人、项目管理组、实施组，其中实施组成员不少于5人，并须包含网络实施人员及安全策略实施人员。

D.2.3 设计阶段

设计阶段要求：

结合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。

D.2.4 实施阶段

实施阶段要求：

a) 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；
b) 项目实施人员按时提交施工记录和工程日志，及时向服务对象汇报项目进度；
c) 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。

D.2.5 保障阶段

D.2.5.1 系统测试

系统测试要求：

a) 编写系统联调及测试计划书；
b) 依据系统测试计划，对系统进行联调和系统测试，完整记录测试过程相关信息，形成测试报告，经双方责任人签字确认。

D.2.5.2 系统试运行

系统运行要求：

a) 系统初验后需进行试运行，并记录系统运行状况，试运行周期至少一个月；
b) 基于系统运行情况，及时对系统进行调整和维护。

D.3 3级要求

D.3.1 基本要求

除满足2级能力要求外，还要满足D.3.2～D.3.5要求。

D.3.2 准备阶段

准备阶段要求：

a) 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；
b) 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；
c) 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) 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。

D.3.3 设计阶段

设计阶段要求：

a) 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；
b) 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；
c) 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。

D.3.4 实施阶段

D.3.4.1 实施集成

实施集成要求：

a) 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；
b) 对项目实施过程中的成本进行有效的管理；
c) 对产品、设备采购、安装调试过程，完整记录相关信息；
d) 项目建设施工完成后，提交完工报告；
e) 项目实施完成后，相关过程记录及时归档，并统一保管。

D.3.4.2 监督管理

监督管理要求：服务机构要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。

D.3.5 保障阶段

D.3.5.1 系统测试

系统测试要求：

a) 依据技术方案具体指标要求，制定系统测试计划；
b) 由第三方机构进行系统测试，并出具系统测试报告，提交服务对象，作为初次验收依据。

D.3.5.2 系统试运行

系统试运行要求：

a) 提供一个月以上的试运行记录；
b) 对系统运行中存在的问题及时整改；
c) 试运行结束后，项目组编写系统试运行报告，提交服务对象。

D.4 4级要求

D.4.1 基本要求

除满足3级能力要求外，还要满足D.4.2～D.4.5的要求。

D.4.2 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。

a) 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；
b) 建立安全集成服务和安全制度建设管理程序。

D.4.3 设计阶段

设计阶段要求：

a) 结合项目需要，编制安全集成项目施工手册和作业指导书并由服务对象责任人确认；
b) 对于新建系统，建设实施过程应重点关注信息系统的功能、性能和安全性等方面要求；
c) 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；
d) 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。

D.4.4 实施阶段

D.4.4.1 实施集成

实施集成要求：

a) 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；
b) 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；
c) 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。

D.4.4.2 监督管理

监督管理要求：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。

D.4.5 保障阶段

D.4.5.1 系统测试

系统测试要求：

a) 基于建设系统的安全要求，制定系统安全性测试方案，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试；
b) 基于系统的稳定性、承载能力要求，制定系统安全性测试方案，有专门的系统压力测试工具，对系统的稳定性进行测试；
c) 由第三方机构进行系统测试，出具系统测试报告，提交服务对象，作为初次验收依据。

D.4.5.2 系统试运行

系统试运行要求：

a) 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；
b) 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；
c) 提供三个月以上的试运行记录和报告；
d) 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 E
（规范性附录）
安全运维服务机构评价要求

E.1 1级要求

E.1.1 准备阶段

准备阶段要求：

a) 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；
b) 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。

E.1.2 实施阶段

实施阶段要求：

a) 初始服务，主要包括资产识别、定期配置项的更新和维护、实施相关运维流程；
b) 安全设备运维服务，主要包括日常维护、状态检查、定期查杀、故障处理、保养、更新、升级、故障检测及排除等，对安全设备出现的故障进行统计记录。

E.1.3 评审阶段

评审阶段要求：

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。

E.1.4 改进阶段

改进阶段要求：

在运维过程和监视过程中识别改进项目，制定持续改进计划。

E.2 2级要求

E.2.1 基本要求

除满足1级能力要求外，还要满足E.2.2～E.2.5的要求。

E.2.2 准备阶段

准备阶段要求：

a) 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；
b) 采集系统配置、流量信息、系统状态等安全信息，收集和分析网络、安全设备、服务器、操作系统、应用、数据库等日志。

E.2.3 实施阶段

实施阶段要求：

a) 日常巡检服务，主要包括安全设备监控、病毒监测、查杀及网络防病毒维护，且形成相关记录；
b) 健康检查服务，主要包括安全设备、业务系统的健康检查服务；
c) 具有处置一般突发性网络安全事件的能力；
d) 具有根据业务的需要熟练地使用成熟工具的能力。 该工具应是正版授权使用或者购买获得。

E.2.4 评审阶段

评审阶段要求：

建立和分析服务对象的满意度调查记录。

E.2.5 改进阶段

改进阶段要求：

a) 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；
b) 应该采取预防措施，消除潜在不符合项的原因，防止其发生。

E.3 3级要求

E.3.1 基本要求

除满足2级能力要求外，还要满足E.3.2～E.3.5的要求。

E.3.2 准备阶段

准备阶段要求：

a) 识别与分析信息网络系统运维过程中的历史数据，提出系统运维的保障策略和解决方案；
b) 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；
c) 建立信息网络系统安全运维的问题管理程序；
d) 建立知识管理程序及初步形成知识库；
e) 编制信息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；
f) 采用流程化管理方法，基于安全事件处理流程、安全培训服务流程、渗透测试流程进行标准化的信息系统安全运维工作。

E.3.3 实施阶段

实施阶段要求：

a) 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；
b) 实施安全事件审计服务，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；
c) 组建运维服务台职能，培养服务台人员的专业能力；

d) 建立网络安全事件管理程序和服务请求管理程序；
e) 实施运维监控与分析并形成记录。

E.3.4 评审阶段

评审阶段要求：
a) 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；
b) 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；
c) 定期回顾安全运维服务，确保其持续适用和有效；
d) 管理评审输入，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。

E.3.5 改进阶段

改进阶段要求：
a) 改进机会应划分优先级，策划被批准的改进机会；
b) 改进活动应进行管理，包括设定改进目标、确保批准的改进活动被实施、报告被实施的改进计划等。

E.4 4级要求

E.4.1 基本要求

除满足3级能力要求外，还要满足E.4.2～E.4.5的要求。

E.4.2 准备阶段

准备阶段要求：
a) 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；
b) 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；
c) 编制安全运维项目作业指导书；
d) 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；
e) 改造过程中应制定测试计划及回退措施；
f) 编写安全运维服务目录，包括安全通告、漏洞分析、应急响应服务等；
g) 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；
h) 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；
i) 建立应急响应和灾难恢复机制，形成业务连续性计划。

E.4.3 实施阶段

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

b) 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；
c) 实施应急响应服务：制定应急响应预案，对应急事件及时响应，并对应急事件的处置开展演练，形成相关记录；
d) 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；
e) 制定运维应急处置方案和恢复策略，对运维过程中的应急事件及时响应。

E.4.4 评审阶段

评审阶段要求：

a) 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；
b) 定期评审服务对象对安全运维服务的满意度。

E.4.5 改进阶段

评审阶段要求：

a) 持续服务改进，形成持续服务改进文化和意识；
b) 基于运维服务的缺陷，提出改进策略和方案；
c) 分析运维服务的数据并进行服务预测。

附 录 F
（规范性附录）
监测预警服务机构评价要求

F.1 1级要求

F.1.1 准备阶段

准备阶段要求：

a) 制定监测预警服务规范和流程；
b) 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；
c) 取得服务对象的监测委托书或授权书；
d) 建有专门部门负责监测预警任务的接收和发布，并对监测服务合同进行审核。

F.1.2 实施阶段

实施阶段要求：

a) 根据项目实施要求，部署监测平台或将监测目标加入监测平台，对监测目标进行安全监测；
b) 定期对安全服务报告进行汇总分析，了解系统脆弱性，形成阶段性安全服务报告。

F.1.3 总结阶段

总结阶段要求：

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。

F.2 2级要求

F.2.1 基本要求

除满足1级能力要求外，还要满足F.2.2～F.2.4的要求。

F.2.2 准备阶段

准备阶段要求：

a) 具备专用监测平台、工具或仪器设备，对目标系统进行安全监测与预警；
b) 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。

F.2.3 实施阶段

实施阶段要求：

对监测目标进行周期性监测，有专人负责监测结果分析，对异常安全事件预警并跟踪分析，同时提交监测或预警报告。

F.2.4 总结阶段

总结阶段要求：
定期为服务对象提供安全监测预警的总结和分析报告。

F.3 3级要求

F.3.1 基本要求

除满足2级能力要求外，还要满足F.3.2～F.3.4的要求。

F.3.2 准备阶段

准备阶段要求：
a) 具有自建的网络安全监测平台；
b) 至少有一项自主研发的用于网络安全领域系统检测分析工具或仪器设备；
c) 组织项目成员对监测目标的网络环境、资产详情等进行现场或远程调研，根据服务对象需求制定监测预警方案。

F.3.3 实施阶段

实施阶段要求：
a) 根据项目实施要求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，要对监测目标进行安全监测预警的影响进行分析和测试，并形成分析、测试报告，报告能被客户认可；
b) 对监测目标提供不间断地实施监测与预警服务；
c) 对网络安全事件进行跟踪和评估，制定并定期修订网络安全事件应急预案。

F.3.4 总结阶段

总结阶段要求：
a) 向服务对象提供安全监测的影响分析报告；
b) 向服务对象提供处置预案；
c) 定期向服务对象提供网络安全态势分析报告。

F.4 4级要求

F.4.1 基本要求

除满足3级能力要求外，还要满足F.4.2～F.4.4要求。

F.4.2 准备阶段

准备阶段要求： 建有独立的监测预警和应急指挥中心。

F.4.3 实施阶段

实施阶段要求：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。

F. 4. 4　总结阶段

总结阶段要求：主要参照监测预警服务的 3 级要求总结阶段执行。

附 录 G
（规范性附录）
应急响应服务机构评价要求

G.1 1级要求

G.1.1 准备阶段

准备阶段要求：

a) 明确服务对象应急需求内容；
b) 向服务对象提供应急处理服务流程；
c) 具备本市内 8 小时、外地 12 小时应急响应服务能力；
d) 配备应急处理服务人员，能处理一般网络安全事件能力。

G.1.2 检测阶段

检测阶段要求：

a) 确定检测对象及范围，并得到用户的授权；
b) 对发生异常的系统进行信息的收集与分析，判断是否真正发生了安全事件，与服务对象共同确定应急处理方案。

G.1.3 抑制阶段

抑制阶段要求：

a) 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，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) 抑制措施要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。

G.1.4 根除阶段

根除阶段要求：

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。

G.1.5 恢复阶段

恢复阶段要求：

a) 在帮助服务对象重建系统前需进行全面的数据备份，备份的数据要确保是没有被攻击者改变过的数据；
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，应该选择通过原有的备份数据进行系统恢复；
d) 系统恢复后，要通过备份数据对系统数据进行恢复。

G.1.6 总结阶段

总结阶段要求：
对事件处理过程进行总结和分析。

G.2 2级要求

G.2.1 基本要求

除满足1级能力要求外，还要满足G.2.2～G.2.7的要求。

G.2.2 准备阶段

准备阶段要求：
a) 具备本市内6小时、外地8小时应急响应服务能力；
b) 配备处理网络安全事件的工具包，并定期更新工具包。

G.2.3 检测阶段

检测阶段要求：
a) 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；
b) 与服务对象充分沟通，评估应急处理方案可能造成的影响。

G.2.4 抑制阶段

抑制阶段要求：
a) 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，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) 抑制措施要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。

G.2.5 根除阶段

根除阶段要求：
a) 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；
b) 找出导致安全事件发生的原因，并予以消除。

G.2.6 恢复阶段

恢复阶段要求：
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。

G.2.7 总结阶段

总结阶段要求：
a) 提供事件处理报告；
b) 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。

G.3 3级要求

G.3.1 基本要求

除满足2级能力要求外，还要满足G.3.2～G.3.7的要求。

G.3.2 准备阶段

准备阶段要求：

a) 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；
b) 向服务对象提供规范化应急处理服务流程；
c) 具备本地4小时、外地8小时应急响应服务能力；
d) 配备有处理网络安全事件工具包，并对工具包实行制度化管理；
e) 具有处理较大网络安全事件的能力。

G.3.3 检测阶段

检测阶段要求：

a) 检测对象及范围应得到服务对象的书面授权；
b) 建立有针对常规应用系统、安全设备、常见网络安全事件的检测技术规范；
c) 协助服务对象确定安全事件等级；
d) 根据应急预案制定本次应急方案，应急处理方案应该包含实施方案失败的应变和回退措施。

G.3.4 抑制阶段

抑制阶段要求：

a) 在采取抑制措施之前，应该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；
b) 严格执行抑制处理方案中规定的内容，如有必要更改，应取得书面授权。

G.3.5 根除阶段

根除阶段要求：

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，并协助客户进行实施；
b) 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；
c) 找出导致网络安全事件发生的原因，并予以消除。

G.3.6 恢复阶段

恢复阶段要求：

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) 帮助服务对象对重建后的系统建立备份。

G.3.7 总结阶段

总结阶段要求：

a) 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；
b) 提供详实的事件处理报告。

G.4 4级要求

G.4.1 基本要求

除满足3级能力要求外，还要满足G.4.2～G.4.7的要求。

G.4.2 准备阶段

准备阶段要求：

a) 建立有体系化的应急处理服务流程；
b) 具备本地2小时、外地4小时应急响应服务能力；
c) 具有自主开发专业检测工具的能力；
d) 具有处理重大及特别重大网络安全事件的能力。

G.4.3 检测阶段

检测阶段要求：

a) 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；
b) 具有挖掘系统设备及业务系统安全漏洞的能力；
c) 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。

G.4.4 抑制阶段

抑制阶段要求：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.4.5 根除阶段

根除阶段要求：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。

G.4.6 恢复阶段

恢复阶段要求：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。

G.4.7 总结阶段

总结阶段要求：

a) 对事件进行总结和分析，针对典型案例存入事件知识库；
b) 提供详实的事件处理报告，关闭安全事件管理程序；
c) 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 H
（规范性附录）
软件安全服务机构评价要求

H.1 1级要求

H.1.1 准备阶段

准备阶段要求：

a) 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；
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。

H.1.2 需求阶段

需求阶段要求：

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。

H.1.3 设计阶段

设计阶段要求：

a) 根据软件项目需求，编制软件设计说明书；
b) 软件设计说明书明确系统/子系统的功能和非功能设计要求；
c) 软件设计说明书明确包含安全功能要求，包括标识与鉴别、访问控制、安全审计和安全管理。

H.1.4 编码阶段

编码阶段要求：

a) 制定统一的代码安全编码规范，确保开发人员参照规范安全编码；
b) 依据详细设计说明书，对软件进行安全编码；
c) 软件代码要经过安全检查、评审，对于发现的漏洞能有效修复。

H.1.5 测试阶段

测试阶段要求：

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

H.1.6 验收交付

H.1.6.1 系统试运行

系统试运行阶段要求：

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

H.1.6.2 验收交付

验收交付阶段要求：

a) 根据合同约定，向客户提交完整的项目资料及交付物，并提出验收申请；
b) 根据合同约定，进行项目验收，形成项目验收报告。

H.1.7 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，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。

H.2 2级要求

H.2.1 基本要求

除满足1级能力要求外，还要满足H.2.2～H.2.8的要求。

H.2.2 准备阶段

准备阶段要求：

a) 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；
b) 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) 使用配置管理工具对软件项目进行配置管理；
d) 配备专职的测试人员；
e) 建立独立的测试环境，确保测试环境与开发环境隔离。

H.2.3 需求阶段

需求阶段要求：

a) 准确识别和综合分析软件项目在可用性、完整性、真实性、机密性、不可否认性、可控性和可靠性等方面的安全需求；
b) 对于数据采集、产生、使用，明确识别安全保护要求；
c) 基于客户需求，开展需求分析，编制具有软件安全需求的分析报告；
d) 需求分析报告中明确项目开发中使用的安全技术标准、规范。

H.2.4 设计阶段

H.2.4.1 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。

H.2.4.2 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。

H.2.5 编码阶段

软件代码的安全检查、评审工作应形成记录。

H.2.6 测试阶段

H.2.6.1 单元测试

单元测试要求：

a) 明确单元测试策略，制定单元测试计划；
b) 依据详细设计说明书和测试计划进行单元测试设计，并执行单元测试，形成测试记录。

H.2.6.2 集成测试

集成测试要求：

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。

H.2.6.3 系统测试

系统测试要求：

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。

H.2.7 验收交付

H.2.7.1 系统试运行

试运行结束后，制定系统试运行报告，并提交客户。

H.2.7.2 验收交付

提交软件安全测评报告。

H.2.8 维保阶段

维保阶段要求：

a) 制定系统运行计划、安全事件响应计划、安全事件应急预案，建立应急响应服务保障团队;
b) 及时应对突发安全事件，并向用户提供安全事件解决报告。

H.3 3级要求

H.3.1 基本要求

除满足2级能力要求外，还要满足H.3.2～H.3.8的要求。

H.3.2 准备阶段

准备阶段要求：

a) 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；
b) 建立软硬件设备和工具等资源安全使用规范；
c) 配备安全管理人员；
d) 建立变更控制委员会。

H.3.3 需求阶段

需求阶段要求：

a) 应基于软件安全威胁开展需求分析；
b) 基于软件项目需求分析建立软件安全开发模型。

H.3.4 设计阶段

H.3.4.1 概要设计

概要设计要求：

a) 概要设计说明书中应明确基于软件安全威胁分析的安全要求；
b) 当开发场景适用时，概要设计说明书中应明确抗抵赖、安全标记、可信路径等安全功能要求。

H.3.4.2 详细设计

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。

H.3.5 编码阶段

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

H.3.6 测试阶段

H.3.6.1 单元测试

对单元测试结果进行分析，形成分析报告。

H.3.6.2 集成测试

对集成测试结果进行分析，形成分析报告。

H.3.6.3 系统测试

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

H.3.7 验收交付

H.3.7.1 系统试运行

系统试运行验收要求：

a) 提供 1 个月以上的试运行记录和报告；
b) 综合软件系统试运行状态，建立软件系统运行策略和安全指南。

H.3.7.2 验收交付

提交软件产品第三方安全测评报告或安全认证证书。

H.3.8 维保阶段

维保阶段要求：

a) 制定软件健康检查计划、方案，定期实施，提交相应的系统健康检查报告、巡检报告；
b) 根据健康检查报告进行分析，持续优化系统。

H.4 4级要求

H.4.1 基本要求

除满足3级能力要求外，还要满足H.4.2～H.4.8的要求。

H.4.2 准备阶段

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。

H.4.3 需求阶段

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。

H.4.4 设计阶段

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。

H.4.5 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。

H.4.6 测试阶段

测试阶段要求：

a) 进行额外的模糊测试，增加模糊测试范围和持续时间；
b) 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。

H.4.7 验收交付

H.4.7.1 系统试运行

系统试运行验收要求：

a) 提供3个月以上的试运行记录和报告；
b) 需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。

H.4.7.2 验收交付

提交软件产品第三方安全测评报告或安全认证证书。

H.4.8 维保阶段

维保阶段要求：

a) 审计人员采取措施来识别报告的问题是否有效解决；
b) 对于未修改的应提供理由，理由应合理，需从安全方面及业务需求方面进行综合分析；
c) 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；
d) 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 I
（规范性附录）
工业控制系统安全服务机构评价要求

I.1 1级要求

I.1.1 准备阶段

准备阶段要求：

a) 服务机构至少拥有1名自动化专业人员及1名信息安全专业人员；
b) 服务机构成立项目团队，确定项目负责人；
c) 服务机构与服务对象确认项目情况，至少包括项目范围、项目目标、组织机构、目标业务系统、物理位置、项目管理机制、验收标准等；
d) 服务机构与服务对象确认服务过程中的分工界面，明确双方的责任，签订保密协议，落实工作环境，签署服务授权书，开展入厂安全培训并遵守其他的工业现场特殊规定等；
e) 服务机构具备工业控制系统安全防护产品的安全集成能力；
f) 服务机构使用的工业控制系统安全防护产品需支持3种以上通用工业控制系统通信协议，包括但不限于Modbus/TCP、OPC、DNP3等。

I.1.2 规划阶段

规划阶段要求：

a) 编制服务方案或工业控制系统安全防护解决方案，根据服务对象的需求，编制技术方案并明确建设预算；
b) 服务机构与服务对象进行沟通，对方案进行评审、修改及确认。

I.1.3 实施阶段

实施阶段要求：

a) 服务机构依据已确认的服务方案或工业控制系统安全防护解决方案，对项目进行建设实施；
b) 服务机构应做好施工日志、项目进度等工程实施过程中的文档管理，及时向服务对象汇报；
c) 服务机构应确保工业控制系统网络安全产品采购和使用符合国家或服务对象所属工业行业的有关规定；
d) 服务机构在安全防护项目中需编写测试方案，对部署产品整体测试，记录测试流程及信息，形成测试报告，由双方责任人签字。

I.1.4 总结阶段

总结阶段要求：

a) 服务机构向服务对象提交完整的项目竣工资料及交付物；
b) 根据合同约定，组织项目验收，签署项目验收报告。

I.2 2级要求

I.2.1 基本要求

除满足1级能力要求外，还要满足I.2.2～I.2.5的要求。

I.2.2 准备阶段

准备阶段要求：

a) 服务机构至少拥有3名自动化专业人员及3名信息安全专业人员；
b) 服务机构成立项目团队，确认项目负责人，成员具有工业控制系统安全服务经验；制定项目工作策略和方针，包含进度跟踪、成果评审、质量监督及人员职能等；
c) 服务机构开展项目启动会，对服务对象开展前期培训，使相关技术人员掌握基本的工业控制系统网络安全知识，提升安全意识；
d) 服务机构拥有服务所需工业控制系统安全防护产品，具备相应工业控制系统安全防护产品的安全集成能力；
e) 服务机构的工业控制系统安全防护产品需支持10种以上工业控制系统通信协议，包括但不限于Modbus/TCP、OPCDA、DNP3、S7、IEC104等。

I.2.3 规划阶段

规划阶段要求：

编制服务方案或工业控制系统安全防护解决方案，根据服务对象的需求，编制技术方案并明确建设预算，其中工业控制系统安全防护技术至少要包含边界隔离防护及核心区域监测审计。

I.2.4 实施阶段

实施阶段要求：

a) 服务机构应能准确识别服务对象重要业务系统、软件系统等，包括但不限于DCS、SCADA、PLC、MES、SIS以及其他具有行业特性的工业控制异构系统，结合已确认的服务方案或工业控制系统安全防护解决方案，对项目进行建设实施；
b) 服务机构的工业控制系统网络安全防护隔离类产品需具备Bypass功能，满足设备在断电情况下的正常运行要求；
c) 服务机构具备工业控制系统网络流量监测审计、网络隔离防护等实施能力，应在网络边界配置针对工业通信协议的访问控制规则以及白名单策略；
d) 服务机构做好安全设备资产、备品管理及工业控制系统网络安全产品配置变更管理。

I.2.5 总结阶段

总结阶段要求：

a) 服务机构编写总结报告、汇报材料，接受服务对象的评审；
b) 服务机构交付工业控制系统安全设备的配置说明和操作手册，及时更新配置变更清单。

I.3 3级要求

I.3.1 基本要求

除满足2级能力要求外，还要满足I.3.2～I.3.5的要求。

I.3.2 准备阶段

准备阶段要求：

a) 服务机构至少拥有 5 名自动化专业人员及 5 名信息安全专业人员，具有中小型自动化、信息安全集成项目实施经验；
b) 成立项目团队，项目团队需包括应急小组，制定应急保障计划；
c) 由从事 3 年以上网络安全技术的人员担任技术负责人；
d) 服务机构具备本地 12 小时、外地 24 小时应急响应服务能力；
e) 服务机构具备独立的工业控制系统漏洞库以及工业控制设备指纹库；
f) 服务机构具备搭建不同工业控制系统厂家工业控制系统网络测试床的能力；
g) 服务机构拥有工业控制系统风险评估工具，具备实施风险评估服务的能力；
h) 服务机构拥有自主研发的工业控制系统安全防护系列产品，具备工业控制系统安全防护产品的安全集成能力；
i) 服务机构的工业控制系统安全防护技术包括自主知识产权的行为白名单安全防护以及工业协议深度包解析功能；
j) 服务机构的工业控制系统安全防护产品需支持 15 种以上工业控制系统通信协议，包括但不限于 Modbus/TCP、OPCDA、DNP3、S7、IEC104、MMS、Profinet、GOOSE、SV、Ethernet/IP、OPCUA_TCP 等。

I.3.3 规划阶段

规划阶段要求：

a) 服务机构立足服务对象的需求，依据《中华人民共和国网络安全法》、工信部《工业控制系统信息安全防护指南》、《信息安全等级保护》等要求，编制合规性工业控制系统安全解决方案，对服务对象工业控制系统与企业其他系统之间划分不同安全域，区域间应采用技术隔离手段；对工业控制系统内部网络进行分域、分区规划设计；
b) 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，对方案进行评审、修改及确认。

I.3.4 实施阶段

实施阶段要求：

a) 服务机构应制定工业控制系统应急处置方案和备份恢复策略，应包含重要数据的本地数据备份与恢复功能；
b) 服务机构应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补，确保对工业控制系统运行无影响扰动；
c) 服务机构在与服务对象相同厂家工业控制系统网络离线测试环境中对工业控制系统安全防护产品部署策略进行验证；
d) 服务机构具备对原本工业控制系统配置或网络改动后进行回归测试的能力；
e) 服务机构具备工业控制系统主机防护实施能力，应采用经过离线环境中充分验证测试的防病毒软件或应用程序白名单软件；
f) 服务机构具备工业控制系统网络安全统一集中管理实施能力，集中管理服务对象中的各个工业控制系统网络安全设备；
g) 记录工业控制系统联调试运行状况，至少持续保持一个月。

I.3.5 总结阶段

总结阶段要求：

a) 服务机构配合服务对象组织自动化专业以及信息化专业的专家对服务项目进行安全性测试内部评审、验收；
b) 服务机构有能力协助服务对象进行具有工业领域特点的专利申请或者知识产权申报、论文发表；
c) 服务机构应对负责运行维护的技术人员定期提供相应的技能培训。

I.4 4级要求

I.4.1 基本要求

除满足3级能力要求外，还要满足I.4.2～I.4.5的要求。

I.4.2 准备阶段

准备阶段要求：

a) 服务机构至少拥有10名自动化专业人员，且具备大型DCS、PLC、SCADA等自动化项目实施经验；服务机构至少拥有10名信息安全专业人员，且具有大型信息安全集成项目实施经验；
b) 由从事5年以上网络安全技术的人员担任技术负责人；
c) 服务机构具备本地6小时、外地12小时应急响应服务能力；
d) 服务机构具备搭建各工业行业工艺流程高仿真工业控制系统网络测试床的能力；
e) 服务机构具备工业控制系统安全定制化平台类产品开发的能力；
f) 服务机构所属公司在国内注册，拥有自主研发、核心知识产权的工业控制系统安全防护系列产品，具备工业控制系统安全防护产品的安全集成能力；
g) 服务机构拥有国产自研的工业控制系统风险评估工具，具备工业控制设备无损识别、基于政策法规的基线评估以及报告自动生成等功能；
h) 服务机构的工业控制系统安全防护技术包括自主知识产权的智能机器学习、工业协议深度包解析以及黑白名单功能；
i) 服务机构的工业控制系统安全防护产品需支持20种以上工业控制系统通信协议，包括但不限于Modbus/TCP、OPCDA、DNP3、S7、IEC104、MMS、Profinet、GOOSE、SV、Ethernet/IP、OPCUA_TCP、PNRTDCP、PNRTIO、s7mms、 BACnet等，支持协议需覆盖主流的自动化供应商，如西门子、ABB、施耐德、霍尼韦尔、浙江中控等；
j) 服务机构拥有工业控制系统漏洞挖掘工具，具有匹配工业控制系统特性的测试用例，具有挖掘工业控制系统与工业控制设备0-day漏洞的能力。

I.4.3 规划阶段

规划阶段要求：

a) 服务机构针对服务对象的需求，定制设计适用于服务对象的工业控制安全软硬件平台，如工业控制系统统一监测预警平台、工业控制系统安全风险中心、工业控制系统安全态势感知平台等；
b) 服务机构对所提供的服务以及定制化产品的开发编制详细的进度、质量、变更等计划书；
c) 服务机构除依据国家相关政策法规要求外，还需结合各工业行业以及企业集团自身的工业

控制系统安全标准、规范的要求，对服务对象设计编制工业控制系统安全解决方案；

d) 服务机构具备为服务对象制定基于工业互联网或智能制造网络安全规划的能力。

I.4.4 实施阶段

实施阶段要求：

a) 服务机构应在经过充分测试评估后，在不影响系统安全稳定运行的情况下对控制设备进行补丁更新、固件更新等工作；
b) 服务机构具备工业控制系统安全态势感知系统实施、部署能力；
c) 服务机构在与服务对象相同业务系统、工艺流程高仿真工业控制系统网络离线测试环境中进行工业控制系统安全防护策略验证以及安全应急演练；
d) 记录工业控制系统联调试运行状况，至少持续保持三个月。

I.4.5 总结阶段

总结阶段要求：

a) 服务机构配合第三方机构进行系统测试，将测试报告作为验收依据；
b) 服务机构具备定期向服务对象提供工业控制系统网络安全风险分析、工业控制系统安全态势感知报告的能力。

附 录 J
（规范性附录）
数据安全服务机构评价要求

J.1 1级要求

J.1.1 准备阶段

准备阶段要求：
a) 具有3人及以上的服务团队和3人及以上的软件技术团队；
b) 具有针对数据安全某细分领域提供安全服务能力；
c) 根据服务对象需求，明确安全需求和建设目标，明确数据安全要求；
d) 具备本地12小时、外地24小时应急响应服务能力。

J.1.2 实施阶段

实施阶段要求：
a) 依据已确认的技术方案和实施方案，对项目进行建设实施；
b) 编制项目实施结果报告，包括实施内容、实施进展、主要成果、问题与建议等。

J.1.3 改进阶段

改进阶段要求：
在安全服务过程中识别改进项目，制定持续改进计划。

J.2 2级要求

J.2.1 基本要求

除满足1级能力要求外，还要满足J.2.2～J.2.4的要求。

J.2.2 准备阶段

准备阶段要求：
a) 具有5人及以上的服务团队和5人及以上的软件技术团队；
b) 具有专用设备或平台支撑服务方案落地；
c) 具备本地12小时、外地24小时应急响应服务能力；
d) 根据数据安全级别及涉密范围签订相应的保密合同；
e) 具备识别并分析服务对象数据安全风险能力，并编写相应的数据防护措施。

J.2.3 实施阶段

实施阶段要求：
结合技术方案和实施方案，对第三方配合人员进行业务和技能培训。

J.2.4 改进阶段

改进阶段要求：

a) 持续跟踪安全服务成效，优化调整防护设备或平台运行参数指标及服务计划；
b) 定期收集和分析安全服务结果数据，并结合需求对服务方案进行优化调整；
c) 定期进行风险再识别及评估，并结合需求对服务方案进行优化调整。

J.3 3级要求

J.3.1 基本要求

除满足2级能力要求外，还要满足J.3.2～J.3.4的要求。

J.3.2 准备阶段

准备阶段要求：

a) 具有10人及以上的服务团队和30人及以上的软件技术团队；
b) 具备本地6小时、外地12小时应急响应服务能力；
c) 具备数据安全保障建设规划能力，并编写整体技术解决方案；
d) 具备自主研发用于数据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；
e) 明确运维方式，包括驻场值守方式、定期巡检方式、远程值守方式等。

J.3.3 实施阶段

实施阶段要求：

a) 根据项目实施要求部署数据安全防护设备和综合性数据分析管理平台，同时统一接入各类数据安全防护设备数据、访问纪录、操作日志等进入平台；
b) 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；
c) 安全分析人员定期通过数据分析管理平台进行整体安全分析，并形成安全报告。

J.3.4 改进阶段

改进阶段要求：

a) 对安全防护及管理效果进行评估，未能实现的目标应采取纠正预防措施；
b) 对安全分析平台的功效进行评估，未能满足需求的应采取改进策略和方案。

J.4 4级要求

J.4.1 基本要求

除满足3级能力要求外，还要满足J.4.2～J.4.4的要求。

J.4.2 准备阶段

准备阶段要求：

a) 确定服务对象的数据安全目标、战略和策略，以及数据安全要求；
b) 识别并分析对组织数据的安全威胁，以及数据安全风险；

c) 建立工作领导小组，包括服务机构和服务对象相关人员；
d) 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，并编写数据安全保障整体解决方案。

J.4.3 实施阶段

实施阶段要求：

a) 根据服务对象的数据目标及业务现状，选取以下相应建设方案并实施：
   1) 制定安全策略与规程，实现对数据全生命周期的安全风险管控；
   2) 制定数据安全工作组织和人员管理方案，包括组织管理、人员管理、角色管理、人员培训；
   3) 制定数据与系统资产管理方案，实现资产类型、管理模式方面的统一管理要求；
   4) 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；
   5) 制定数据供应链管理方案，包括数据供应链、数据服务接口；
   6) 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；
   7) 制定数据分类分级方案，对生成/采集的数据进行数据分类分级的标示；
   8) 制定数据采集安全方案，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；
   9) 制定数据传输安全方案，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；
   10) 制定数据存储安全方案，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；
   11) 制定数据处理安全方案，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；
   12) 制定数据交换安全方案，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；
   13) 制定数据销毁安全方案，包括介质使用管理、数据销毁处置、介质销毁处置；
b) 不断和服务对象相关人员充分沟通，分析数据安全实践情况，不断优化建设方案；
c) 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；
d) 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。

J.4.4 改进阶段

改进阶段要求：

根据组织的整体目标，不断改进和优化安全过程。

参 考 文 献

[1] GB/T 20261—2006　信息技术系统安全工程能力成熟度模型

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

[3] GB/T 30283—2013　信息安全技术信息安全服务分类

[4] RB/T 201—2013　信息系统安全集成服务资质认证评价要求

[5] YD/T 1621—2007　网络与信息安全服务资质评估准则

[6] YD/T 1799—2008　网络与信息安全应急处理服务资质评估方法

[7] YD/T 2252—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/CTS 0052-2007　信息安全服务资质认证技术规范

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

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

[12] ISO 27005:2008 Information technology - Security techniques – Information security risk management

ICS 03.120.20
A 00
关键词：网络安全、服务机构、等级评定