ICS 03.120.20
CCS L 70

团　　体　　标　　准

T/BJCSA 06-2025
T/GDCSA 028-2025

计算机信息系统安全服务机构等级评定规范

Specification for grading of computer information system security service institutions

2025-09-01 发布　　2025-09-01 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、广州电力设计院有限公司、深圳市常行科技有限公司、广州华南检验检测中心有限公司、国源天顺科技产业集团有限公司、广东关键信息基础设施保护中心、广东新兴国家网络安全和信息化发展研究院、安徽省计算机信息网络安全协会、广州华南信息安全测评中心、广东中证声像资料司法鉴定所。

本文件主要起草人：成珍苑、程正刚、郭义、张德方、庄严、李峰、何丽萍、冷令、王伟彬、陈庆亮、郝瑞、董满、许学添、吴晓光、晏圣华、李晶、李佳春、何雄韬、何建忠、郭乐、梁展明、王湛泽、梁力文、覃丽娟、黄珊珊、黎韵婷、贺锋、董晓静、蔡美玲。

计算机信息系统安全服务机构等级评定规范

1 范围

本文件规定了计算机信息系统安全服务机构的等级划分、基本能力要求、分级能力要求、服务实施能力要求、评定方法等内容。

本文件适用于第三方评审机构对从事计算机信息系统安全服务的机构进行等级评定，评定结果可作为政府部门和企事业单位选用安全服务时的参考依据；也可作为从事计算机信息系统安全服务的机构改进自身服务能力的指导。

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 25069-2022 信息安全技术 术语

GB/T 30271-2013 信息安全技术 信息安全服务能力评估准则

3 术语和定义

GB/T 25069-2022和GB/T 30271-2013 界定的以及下列术语和定义适用于本文件。

3.1

计算机信息系统 computer information system

由计算机及相关的和配套的设备、设施（含网络）构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。

3.2

计算机信息系统安全 computer information system security

采取适当措施保护数据和资源，使计算机信息系统免受偶然或恶意的修改、损害、访问、泄露等操作的危害。

3.3

信息安全服务 information security service

面向组织或个人的各类信息安全保障需求，由服务提供方按照服务协议所执行的一个信息安全过程或服务。

3.4

安全服务机构 security service institutions

按照服务协议，通过专业计算机信息系统安全服务人员提供信息安全服务的各类组织机构。

3.5

第三方评审机构 third-party assessment organization

独立于信息安全服务相关方的专业评估机构。

4 安全服务机构等级划分

依据安全服务机构的基本资格、管理能力、技术服务能力等分为一级、二级、三级和四级，其中一级最高，四级最低。

5 基本能力要求

5.1 基本条件

安全服务机构应具备的基本条件包括：

a) 具有中华人民共和国境内注册的独立法人资格，并具有相关部门颁发的合法经营资格；
b) 拥有长期固定的办公场所，具有能满足业务需求的设备和环境；
c) 有健全的财务制度，财务数据真实可信；
d) 遵守国家现行法律、法规，无违法记录。

5.2 基本管理能力要求

安全服务机构应具备的基本管理能力包括：

a) 建立人员管理制度和能力考核指标，制定相关培训计划，定期开展培训；
b) 建立文档管理制度，确保项目文档资料妥善保管；
c) 建立项目管理制度，有健全的监督检查机制；
d) 建立保密管理制度，确保客户信息安全可控。

6 分级能力要求

6.1 基本资格分级要求

各级别必须在满足5.1的要求基础上，同时满足该级别的所有的要求，详见表1。

表1 基本资格分级要求

安全服务机构等级	人员构成与素质要求				业绩要求	
	技术负责人	安全服务负责人	财务负责人	技术人员	从业时间	近三年安全服务项目要求
四级	2 年以上计算机信息系统安全服务领域管理经历。	2 年以上计算机信息系统安全服务领域工作经历。	具有财务工作经历。	技术团队不少于2人，其中至少1人具有计算机相关或相近的学历证书及相关机构颁发的与计算机相关的资质证书。	无。	首次申请不作要求，维持资质至少需要完成1个计算机信息系统安全服务项目。
三级	3 年以上计算机信息系统安全服务领域管理经历；具有信息安全相关或相近专业技术资格。	3 年以上计算机信息系统安全服务领域工作经历；具有计算机信息系统安全相关或相近专业技术资格。	具有财务工作经历。	技术团队不少于5人，其中至少2人具有计算机相关或相近的学历证书及相关机构颁发的与计算机相关的资质证书。	从事安全服务一年以上。	近三年至少完成2个计算机信息系统安全服务项目，维持资质至少需要完成1个计算机信息系统安全服务项目。

安全服务机构等级	人员构成与素质要求				业绩要求	
	技术负责人	安全服务负责人	财务负责人	技术人员	从业时间	近三年安全服务项目要求
二级	4 年以上计算机信息系统安全服务领域管理经历；具有信息安全相关或相近专业中级或以上技术资格。	4 年以上计算机信息系统安全服务领域工作经历；具有计算机信息系统安全相关或相近专业中级或以上技术资格。	具有财务系列初级或以上技术资格。	技术团队不少于10人，其中至少6人具有计算机相关或相近的学历证书及相关机构颁发的与计算机相关的资质证书。	从事安全服务三年以上或获取三级证书满一年以上。	近三年至少完成5个计算机信息系统安全服务项目，维持资质至少需要完成1个计算机信息系统安全服务项目。
一级	5 年以上计算机信息系统安全服务领域管理经历；具有信息安全相关或相近专业高级技术资格。	5 年以上计算机信息系统安全服务领域工作经历；具有计算机信息系统安全相关或相近专业高级技术资格。	具有财务系列中级或以上技术资格。	技术团队不少于20人，其中至少12人具有计算机相关或相近的学历证书及相关机构颁发的与计算机相关的资质证书。	从事安全服务五年以上，获得二级等级证书满一年以上。	近三年至少完成10个计算机信息系统安全服务项目，维持资质至少需要完成1个计算机信息系统安全服务项目。

6.2 管理能力分级要求

各级别管理能力分级要求详见表2。

表2 管理能力分级要求

安全服务机构等级	管理能力分级要求
四级	满足5.2 所有要求。
三级	满足5.2 所有要求外，还需满足以下条件： 参照国际或国内标准，建立质量管理体系，并提供有效运行的证明材料。
二级	满足5.2 所有要求外，还需满足以下条件： a）参照国际或国内标准，建立质量管理体系，并提供有效运行的证明材料； b）具有项目风险预防和规避制度与措施。
一级	满足5.2 所有要求外，还需满足以下条件： a）参照国际或国内标准，建立质量管理体系，并提供有效运行的证明材料； b）具有项目风险预防和规避制度与措施； c）参照国际或国内标准，建立信息安全管理体系，并提供有效运行的证明材料。

6.3 技术能力特殊要求

各级别技术能力特殊要求见表3。

表3 技术能力特殊要求

安全服务机构等级	技术能力特殊要求
四级	无
三级	无
二级	需满足以下条件： a）服务团队核心人员熟悉相关的信息安全标准； b）具备独立的测试环境及必要的软、硬件设备，用于技术培训或模拟测试； c）具有先进、完整的软件及系统开发环境和设备，有较高的技术开发水平。
一级	需满足以下条件： a）服务团队核心人员熟悉相关的信息安全标准； b）具备独立的测试环境及必要的软、硬件设备，用于技术培训或模拟测试； c）有先进、完整的软件及系统开发环境和设备，有较高技术开发水平，至少有1种自主开发的信息安全产品。

7 服务实施能力要求

安全服务机构应具备的服务实施能力要求包括：

a） 制定安全服务流程和规范。

b） 服务过程至少包含准备阶段、设计阶段、实施阶段、服务保障阶段：

1） 准备阶段：

——服务需求界定：编写需求调研报告。

——服务合同签订：明确服务范围、时间、内容等。

2） 设计阶段：

——服务方案制定：根据客户需求，编制技术方案和实施方案，方案明确人员、进度、质量、沟通、风险等方面要求。根据项目需求组织客户及相关技术专家对技术方案或实施方案进行论证，确认是否满足要求。

——人员和工具准备：组建服务团队，服务团队应由管理层、相关业务骨干、技术人员等组成。应对服务团队及第三方配合人员进行安全意识、技能等培训。

3） 实施阶段：

——项目实施人员依照实施方案，按时提交记录文档，及时向项目经理汇报项目进度。

——对整个系统的安全配置进行管理、分析安全状况（如软件更新记录、安全配置记录等）。

4） 服务保障阶段：

——依照项目需求和项目范围的要求，提出项目验收申请，组织客户和相关方对项目进行验收，并提交项目验收报告。

——调研客户对服务团队的满意度，并对调查结果进行分析。

8 评定方法

8.1 评定原则

原则开展评定工作：

a） 公开、公正、公平原则；

b） 定性与定量相结合原则；

c） 实行统一标准、统一程序、统一管理。

8.2 评定模式

8.2.1 采取文档审核、现场审核的模式进行。

8.2.1.1 文档审核

审查机构对申请机构进行文档审核，应提交以下证明材料：

a） 独立法人资格证明；

b） 固定办公场所的证明材料；

c） 人员构成与素质证明材料；

d） 财务制度及反映财务状况的材料；

e） 人员管理制度和培训制度材料；

f） 文档管理制度文档材料；

g） 项目管理制度文档材料；

h） 保密管理制度文档材料；

i） 项目业绩证明材料；

技术能力及服务能力过程证明材料。第三方评审机构审查申请机构提交的申请材料，并判断所提交的证明材料是否满足相应等级要求。如果满足则文档审核为通过，否则为不通过。

8.2.1.2 现场审核

申请机构的文档通过审核后，应对申请机构进行现场审核，通过检查、观察、访谈等方式，对申请机构的基本能力要求、分级能力要求和服务实施能力要求等进行审核验证，并提交现场审核报告。

审核验证结果满足相应等级要求的，其结论为通过；审核验证结果不满足相应等级要求的，其结论为不通过。

8.2.2 综合评定

第三方评审机构根据文档审核和现场审核的结果进行综合评价，作出最终是否符合等级要求的结论并提交综合评价报告。对综合评定结果为不通过的申请机构，第三方评审机构应提出整改建议，申请机构在能力达到相应等级要求后重新申请评定。

参 考 文 献

[1] GB/T 30271—2013 信息安全技术 信息安全服务能力评估准则
[2] GB/T 30283—2022 信息安全技术 信息安全服务 分类与代码
[3] RB/T 201—2013 信息系统安全集成服务资质认证评价要求
[4] YD/T 1621—2007 网络与信息安全服务资质评估准则
[5] CNCA/CTS0052-2007 信息安全服务资质认证技术规范
[6] ISO 27001:2005 Information technology-Security techniques-Information security management systems-Requirements
[7] ISO 27002:2005 Information technology-Security techniques-Code of practice for information security controls
[8] ISO 27005:2008 Information technology-Security techniques－Information security risk management