ICS
备案号：

DB44

广　东　省　地　方　标　准

DB44/T 1920—2016

计算机信息系统安全服务机构等级评定规范

Classified Assessment Specification
of Computer Information System Security Services

2016-09-30 发布　　2017-01-01 实施

广东省质量技术监督局发布

目 次

前　言

本标准按GB/T 1.1-2009给出的规则起草。

本标准由广东省网络空间安全协会提出。

本标准起草单位：广东省网络空间安全协会、广东新兴国家网络安全和信息化发展研究院、北京网络空间安全联盟、蓝盾信息安全技术有限公司、深圳市脉山龙信息技术股份有限公司、联奕科技股份有限公司、广东创能科技股份有限公司、佛山科讯安科技有限公司、工业和信息化部电子第五研究所、广州市信息网络安全协会、广东关键信息基础设施保护中心、北京关键信息基础设施安全保护中心、广州华南信息安全测评中心。

本标准主要起草人：黄丽玲、崔书昆、成珍苑、张 昊、刘 杰、刘志祥、刘欣荣、林勇忠、覃晓宁、陈希、刘晓林、刘彦能、李长立。

计算机信息系统安全服务机构等级评定规范

1. 范围

本标准规定了广东省内从事计算机信息系统安全服务的机构应具备的服务能力要求及评定方法。

本标准适用于第三方评审机构对在广东省内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 25069-2010　　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 25069-2010 和 GB/T 30271-2013 界定的以及下列文件中的术语和定义并适用于本文件。

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。

[GB/T 25069-2010，定义2.1.13]

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。

[GB/T 30271-2013，定义 3.1.4]

3.4

安全服务机构 security services

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

安全服务机构等级评定是衡量安全服务机构服务能力的尺度，依据安全服务机构的基本条件、基本资格、管理能力、技术服务能力等分为一级、二级、三级、四级，其中一级最高，四级最低。

5. 安全服务机构评定标准

安全服务机构等级评定要求包含基本能力要求、分级能力要求和服务能力过程要求。基本能力要求包含基本条件、基本管理能力要求、基本技术能力要求，具体要求见第6章。分级能力要求为安全服务机构各级别的能力要求，包含基本资格、管理能力要求、技术能力要求，具体要求见第7章。服务能力过程要求包含准备阶段、设计阶段、实施阶段、服务保障阶段等4个阶段，具体要求见第8章。

6. 安全服务机构基本能力要求

6.1 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) 在广东省内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。

6.2 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；
e) 建立质量管理制度，跟踪服务质量，并能对服务质量进行持续改进。

6.3 基本技术能力要求

安全服务机构应具备的基本技术能力包括：

a）具备评估系统安全威胁的能力，能够识别系统所面临的各种安全威胁及其性质和特征，以及对威胁的可能性进行评估；
b）具备评估系统脆弱性的能力，能够收集、合成系统的脆弱性数据；
c）具备评估安全对系统的影响的能力，能够识别安全对所实施的系统的影响，并对发生影响的可能性进行评估；
d）具备评估系统安全风险的能力，识别出给定环境中涉及到对某一系统有依赖关系的安全风险；
e）具备确定系统安全需求的能力，能够为客户提供安全策略、安全目标、安全需求分析报告；
f）具备确定系统的安全输入的能力，能为系统的规划者、设计者、实施者或用户提供他们所需的安全信息，包括安全体系结构、设计或实施选择以及安全指南；
g）具备安全控制管理的能力，能建立安全职责，增强所有用户和管理员的安全意识，开展安全教育培训，对所有的安全配置进行管理（如软件更新记录、安全配置修改记录等）；
h）具备监测系统安全状况的能力，能对安全风险变化、事件记录、安全防护措施进行监视，能识别安全突发事件和对安全突发事件进行响应；
i）具备检测或证实系统安全性的能力，包括检测或证实系统安全性的方法和工具；
j）具备建立系统安全的保证数据的能力，包括对保证的目标进行识别、建立保证证据数据库并对其进行分析；
k）具备对整个系统进行管理配置的能力，包括维持已标识的配置单元的数据和状况，并对系统及其配置单元的变化进行分析和控制。

7. 安全服务机构分级能力要求

7.1 基本资格分级要求

各级别必须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总额
四级	2 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。	2 年以上计算机信息系统安全服务领域工作经历；具有信息安全相关或相近专业技术资格。	具有财务系列专业从业资格。	技术团队不少于 10 人，每年按要求接受继续教育；其中 60%的技术人员具有信息安全相关或相近专业学历证书及相关机构颁发的资格（水平）证书。	无	至少完成 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。

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；具有信息安全相关或相近专业技术资格。	具有财务系列专业从业资格。	技术团队不少于 20 人，每年按要求接受继续教育；其中 60%的技术人员具有信息安全相关或相近专业学历证书及相关机构颁发的资格（水平）证书。	从事安全服务一年以上。	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；工程按合同要求质量合格，已通过验收并投入实际应用。
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；具有信息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 30 人，每年按要求接受继续教育；其中 60%的技术人员具有信息安全相关或相近专业学历证书及相关机构颁发的资格（水平）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 3 年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；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；工程按合同要求质量合格，已通过验收并投入实际应用。
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；具有信息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 50 人，每年按要求接受继续教育；其中 60%的技术人员具有信息安全相关或相近专业学历证书及相关机构颁发的资格（水平）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 3 年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；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；工程按合同要求质量合格，已通过验收并投入实际应用。

7.2 管理能力分级要求

各级别管理能力要求详见表2。

表 2 管理能力分级要求

安全服务机构等级	管理能力要求
四级	满足 6.2 所有要求。

三级	满足 6.2 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 6.2 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 6.2 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）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； c）具有项目风险预防和规避制度与措施。

7.3 技术能力分级要求

各级别技术能力要求见表3。

表 3 技术能力分级要求

安全服务机构等级	技术能力要求
四级	满足6.3所有要求。
三级	满足 6.3 所有要求外，还需满足以下条件： 服务团队核心人员熟悉相关的信息安全标准。
二级	满足 6.3 所有要求外，还需满足以下条件： 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	满足 6.3 所有要求外，还需满足以下条件： a)具备独立的测试环境及必要的软、硬件设备，用于技术培训或模拟测试； b)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； c)具有专门的人员进行信息安全标准研究。

8. 安全服务机构服务能力过程要求

安全服务机构应具备的服务能力过程要求包括：

a）制定安全服务流程；

b）制定安全服务规范，并按照规范实施；

c）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：调研客户背景信息，明确客户需求，与客户充分沟通，达成共识并编写需求分析报告。

— 服务合同签订：与客户签订服务协议，明确服务范围、目标、时间、内容、金额、质量和输出等。

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，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和实施方案进行论证，确认是否满足要求，编制项目施工手册和作业指导书。

— 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业务和技能培训。

3）实施阶段：

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

— 对项目实施监督管理，建立客户满意度调查机制，并对调查结果进行分析。

— 根据项目需求和项目范围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。

4）服务保障阶段：

— 依照项目需求和项目范围的要求，提出项目初验申请，组织客户和相关方对项目进行初步验收，并提交项目初验报告。

— 根据合同约定，配合验收组完成项目终审验收，提交项目终验报告。

9. 评定方法

9.1 评定原则

第三方评审机构应按如下原则开展评定工作：

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。

9.2 评定模式

对安全服务机构等级评定采取文档审核、现场审核、综合评定的模式进行。

9.2.1 文档审核

申请机构根据评定要求先确定需要申请的等级，提交符合相应等级要求的材料，提交的证明材料应包含但不限于：

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）质量保证制度文档材料；

j）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。

9.2.2 现场审核

申请机构的文档通过审核后，第三方评审机构组成审核组对申请机构实施现场审核，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能力过程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。

9.2.3 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 20269-2006 信息系统安全管理要求
[2] GB/T 20282-2006 信息系统安全工程管理要求
[3] GB/T 20984-2007 信息安全技术 信息安全风险评估规范
[4] GB/Z 20985-2007 信息安全技术 信息安全事件管理指南
[5] GB/T 25070-2010 信息系统等级保护安全设计技术要求
[6] GB/T 30283-2013 信息安全技术 信息安全服务 分类
[7] YD/T 2252 网络与信息安全风险评估服务能力评估方法
[8] YD/T 1799 网络与信息安全应急处理服务资质评估方法