团体标准《网络安全服务机构等级评定规范》

编制说明

1. 工作简况

1.1任务来源

《网络安全服务机构等级评定规范》由广东省网络空间安全协会作为提出单位。该标准由广东省网络空间安全协会和北京网络空间安全协会归口管理。

1.2主要起草单位和工作组成员

本标准由成都信息网络安全协会、陕西省信息网络安全协会、广东省网络空间安全协会等多家单位共同参与编制。

1.3主要工作过程

（1）2020年12月，组织参与本标准编写的相关单位召开项目启动会，成立规范编制小组，确立各自分工，开展标准修订工作。

（2）2021年1月15日，编制组召开组内研讨会并结合充分的调研结果，参考各类国家标准和相关政策文件，形成标准草案初稿，

（3）2021年1月29日，经内部多次讨论研究，形成标准内容修改稿。

（4）2021年3月18日，编制组召开组内研讨会，基于前期成果，经多次内部讨论研究，组织完善草案内容，形成终稿。

二、标准编制原则和标准编制详细说明及解决的主要问题

2.1编制原则

本标准的研究与编制工作遵循以下原则：

（1）符合性原则

遵循国家现有资费相关标准，符合国家有关法律法规和已编制标准规范的相关要求，符合国家资费管理主管部门的要求。

（2）实用性原则

本标准规范是对实际工作成果的总结与提升，保持整体结果合理且维持原意和功能不变，针对不同的用户群体，做到可操作、可用与实用。

2.2文档结构

网络安全服务机构等级评定规范文档分为前言、引言、范围、规范性引用文件、术语和定义、网络安全服务类型、评定原则与流程、基本能力要求、参考文献、附录等十部分。

2.3整体格式

整体格式根据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》的相关要求，对本标准的各要素进行编写和排版。

在标准内容汇总过程中，对各编写组成员提交过来的部分，根据GB/T 1.1的编写要求进行了必要的增删改，以确保符合一致性、协调性、易用性等文件的表述原则及相关规定。

2.4标准名称英文翻译

标准的名称“网络安全服务机构等级评定规范”翻译为Grade assessment specification of cyber security service institutions。

2.5术语和定义

术语和定义中所列的术语的英文翻译，根据各部分编写成员提供的术语，如有类似术语的标准，参考了其翻译，没有类似术语标准翻译的，通过百度翻译和谷歌翻译后进行对比，并参考网络相关翻译后进行确定。

2.6网络安全服务类型

网络安全服务类型主要包括安全咨询服务、信息系统安全集成服务、信息系统安全运维服务、监测预警服务、应急响应服务、软件安全服务、工业控制系统安全服务、数据安全服务、信息安全风险评估服务、云计算安全服务、信息系统安全审计服务、渗透测试服务。

2.7结构与内容

2.7.1安全咨询服务

《安全咨询服务机构评价要求》规定了一级、二级、三级和四级服务机构的服务过程能力要求，本部分共分为四小节。

第一级要求：包括准备阶段、实施阶段、改进阶段要求；

第二级要求：在第一级要求基础上还需要满足的准备阶段、实施阶段、改进阶段要求；

第三级要求：在第二级要求基础上还需要满足的准备阶段、实施阶段、改进阶段要求；

第四级要求：在第三级云要求基础上还需要满足的准备阶段、实施阶段、改进阶段要求。

2.7.2信息系统安全集成服务

《信息系统安全集成服务机构评价要求》规定了一级、二级、三级和四级服务机构的服务过程能力要求，本部分共分为四小节。

第一级要求：包括准备阶段、设计阶段、实施阶段、保障阶段、验收阶段要求；

第二级要求：在第一级要求基础上还需要满足的准备阶段、设计阶段、实施阶段、保障阶段；

第三级要求：在第二级要求基础上还需要满足的准备阶段、设计阶段、实施阶段、保障阶段、验收阶段要求；

第四级要求：在第三级云要求基础上还需要满足的准备阶段、设计阶段、实施阶段、保障阶段、验收阶段要求。

2.7.3信息系统安全运维服务

《信息系统安全运维服务机构评价要求》规定了一级、二级、三级和四级服务机构的服务过程能力要求，本部分共分为四小节。

第一级要求：包括准备阶段、实施阶段、评审阶段、改进阶段要求；

第二级要求：在第一级要求基础上还需要满足的准备阶段、实施阶段、评审阶段、改进阶段要求；

第三级要求：在第二级要求基础上还需要满足的准备阶段、实施阶段、评审阶段、改进阶段要求；

第四级要求：在第三级云要求基础上还需要满足的准备阶段、实施阶段、评审阶段、改进阶段要求。

2.7.4监测预警服务

《监测预警服务机构评价要求》规定了一级、二级、三级和四级服务机构的服务过程能力要求，本部分共分为四小节。

第一级要求：包括准备阶段、实施阶段、总结阶段要求；

第二级要求：在第一级要求基础上还需要满足的准备阶段、实施阶段、总结阶段要求；

第三级要求：在第二级要求基础上还需要满足的准备阶段、实施阶段、总结阶段要求；

第四级要求：在第三级云要求基础上还需要满足的准备阶段、实施阶段、总结阶段要求。

2.7.5应急响应服务

《应急响应服务机构评价要求》规定了一级、二级、三级和四级服务机构的服务过程能力要求，本部分共分为四小节。

第一级要求：包括准备阶段、检测阶段、抑制阶段、根除阶段、恢复阶段、总结阶段要求；

第二级要求：在第一级要求基础上还需要满足的准备阶段、检测阶段、抑制阶段、根除阶段、恢复阶段、总结阶段要求；

第三级要求：在第二级要求基础上还需要满足的准备阶段、检测阶段、抑制阶段、根除阶段、恢复阶段、总结阶段要求；

第四级要求：在第三级云要求基础上还需要满足的准备阶段、检测阶段、抑制阶段、根除阶段、恢复阶段、总结阶段要求。

2.7.6软件安全服务

《软件安全服务机构评价要求》规定了一级、二级、三级和四级服务机构的服务过程能力要求，本部分共分为四小节。

第一级要求：包括准备阶段、需求阶段、设计阶段、编码阶段、测试阶段、验收阶段、维保阶段要求；

第二级要求：在第一级要求基础上还需要满足的准备阶段、需求阶段、设计阶段、编码阶段、测试阶段、验收阶段、维保阶段要求；

第三级要求：在第二级要求基础上还需要满足的准备阶段、需求阶段、设计阶段、编码阶段、测试阶段、验收阶段、维保阶段要求；

第四级要求：在第三级云要求基础上还需要满足的准备阶段、需求阶段、设计阶段、编码阶段、测试阶段、验收阶段、维保阶段要求。

2.7.7工业控制系统安全服务

《工业控制系统安全服务机构评价要求》规定了一级、二级、三级和四级服务机构的服务过程能力要求，本部分共分为四小节。

第一级要求：包括基本要求、能力要求；

第二级要求：在第一级要求基础上还需要满足的基本要求、能力要求；

第三级要求：在第二级要求基础上还需要满足的基本要求、能力要求；

第四级要求：在第三级云要求基础上还需要满足的基本要求、能力要求。

2.7.8数据安全服务

《数据安全服务机构评价要求》规定了一级、二级、三级和四级服务机构的服务过程能力要求，本部分共分为四小节。

第一级要求：包括基本要求、能力要求；

第二级要求：在第一级要求基础上还需要满足的基本要求、能力要求；

第三级要求：在第二级要求基础上还需要满足的基本要求、能力要求；

第四级要求：在第三级云要求基础上还需要满足的基本要求、能力要求。

2.7.9信息安全风险评估服务

《信息安全风险评估服务机构评价要求》规定了一级、二级、三级和四级服务机构的服务过程能力要求，本部分共分为四小节。

第一级要求：包括准备阶段、风险识别阶段、风险分析阶段要求；

第二级要求：在第一级要求基础上还需要满足的准备阶段、风险识别阶段、风险分析阶段、风险处置阶段要求；

第三级要求：在第二级要求基础上还需要满足的准备阶段、风险识别阶段、风险分析阶段、风险处置阶段要求；

第四级要求：满足三级能力全部要求。

2.7.10云计算安全服务

《云计算安全服务机构评价要求》规定了一级、二级、三级和四级服务机构的服务过程能力要求，本部分共分为四小节。

第一级要求：包括基础能力要求、云计算安全技术要求、云计算安全管理要求；

第二级要求：在第一级要求基础上还需要满足的基础能力要求、云计算安全技术要求、云计算安全管理要求；

第三级要求：在第二级要求基础上还需要满足的基础能力要求、云计算安全技术要求、云计算安全管理要求；

第四级要求：在第三级要求基础上还需要满足的基础能力要求、云计算安全技术要求、云计算安全管理要求。

2.7.11信息系统安全审计服务

《信息系统安全审计服务机构评价要求》规定了一级、二级、三级和四级服务机构的服务过程能力要求，本部分共分为四小节。

第一级要求：包括基本要求、审计过程要求；

第二级要求：在第一级要求基础上还需要满足的基本要求、审计过程要求；

第三级要求：在第二级要求基础上还需要满足的基本要求、审计过程要求；

第四级要求：在第三级云要求基础上还需要满足的基本要求、审计过程要求。

2.7.12渗透测试服务

《渗透测试服务机构评价要求》规定了一级、二级、三级和四级服务机构的服务过程能力要求，本部分共分为四小节。

第一级要求：包括准备阶段、实施阶段、报告阶段、复测阶段、总结阶段要求；

第二级要求：在第一级要求基础上还需要满足的准备阶段、实施阶段、报告阶段、复测阶段、总结阶段要求；

第三级要求：在第二级要求基础上还需要满足的准备阶段、实施阶段、报告阶段、复测阶段、总结阶段要求；

第四级要求：在第三级云要求基础上还需要满足的准备阶段、实施阶段、报告阶段、复测阶段、总结阶段要求。

2.8参考文献

本部分列出了在本标准编写过程中所参考的主要文献名称。

2.9解决问题

通过对本标准的制定，主要解决了现行标准的实用性问题，具体内容包括：

（1）行业内网络安全服务机构的技术能力、工作规范及管理水平不足；

（2）缺乏从业企业能力的统一方法，从业企业的服务质量良莠不齐，由于网络安全服务机构等级评定规范涉及服务机构的资格和服务能力的评价、市场秩序的规范、避免恶性竞争、杜绝不良企业涉足网络安全行业等问题。

三、知识产权情况说明

本标准不涉及专利。

四、采用国际标准和国外先进标准情况

无。

五、与现行相关法律、法规、规章及相关标准的协调性

建议本标准推荐信实施。本标准不触犯国家现行法律法规，不与其他强制性国标相冲突。

六、重大分歧意见的处理经过和依据

《网络安全服务机构等级评定规范》编制过程中未出现重大分歧。

七、标准性质的建议

建议《网络安全服务机构等级评定规范》作为推荐性团体标准发布实施。

八、贯彻标准的要求和措施建议

鉴于本标准是网络安全服务机构等级评定规范的标准，建议在标准贯彻执行过程中，各单位应当起到协调以及推广的作用，召开研讨会、协调会，网络安全服务机构等级评定活动首先使用本标准中的方法进行评估。

九、替代或废止现行相关标准的建议

无替代或废止。

十、其他应予说明的事项

无。

《网络安全服务机构等级评定规范》标准编制组

2021年4月