文件编码：CCRC-ISV-C01:2025

信息安全服务规范

2025-8-27 发布　　2025-8-27 实施

中国网络安全审查认证和市场监管大数据中心发布

目录

1. 适用范围

本规范规定了信息安全服务提供者（以下简称服务提供者）在提供服务时应具备的服务安全通用要求和专业服务能力要求。

本规范可作为第三方认证机构对服务提供者的评价依据，也可作为服务提供者开展自我评价的依据，同时,可为政府及有关社会组织选择服务提供者提供参考。

2. 规范性引用文件

GB/T 25069-2022《信息安全技术　术语》

3. 术语与定义

3.1. 信息安全服务

面向组织或个人的各类信息安全需求和信息安全保障需求,由服务提供方按照服务协议所执行的信息安全过程或任务。

注1:信息安全服务通常是基于信息安全技术、产品或管理体系,通过外包的形式,由专业信息安全人员所提供的支持和帮助。

注2:信息安全服务通常以信息安全服务提供方和信息安全服务需求方之间的服务项目方式进行。

3.2. 信息安全风险评估

对特定威胁利用单个或一组资产脆弱性的可能性以及由此可能给组织带来的损害进行识别、分析和评价的过程。

3.3. 信息安全应急处理

为应对信息系统运行过程中突发/重大信息安全事件的发生所做的准备，在事件发生时，按照既定的程序对事件进行处理，以及在事件发生后所采取措施的过程。

3.4. 信息系统安全集成

按照信息系统建设的安全需求，采用信息系统安全工程的方法和理论，将安全单元、产品部件进行集成的行为或活动。

3.5. 信息系统灾难备份与恢复

将信息系统的数据、数据处理系统、网络系统、基础设施、专业技术支持能力和运行管理能力进行备份，并在灾难发生时，将信息系统从灾难造成的故障或瘫痪状态恢复到可正常运行状态、将其支持的业务功能从灾难造成的不正常状态恢复到可接受状态的过程。

注：信息系统灾难备份与恢复分为资源服务类（A 类）、技术服务类（B 类）两个类别。

资源服务类（A 类），指灾难备份资源服务提供方需具备灾备中心场地资源、基础设施、运维管理等能力。

技术服务类（B 类），指灾难备份技术服务提供方实施灾备技术服务时具备灾备方案设计、系统建设与管理、预案制定与演练等能力。

3.6. 软件安全开发

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。

3.7. 信息系统安全运维

从面向业务的运维服务出发，依据安全需求对信息系统进行安全运维准备、安全运维实施，并对实施安全运维服务的有效性进行评审，从而进行持续性改进，全过程、全生命周期地为信息系统运行提供安全保障的过程。

3.8. 网络安全审计

网络安全审计是指网络安全审计服务机构对被审计方所属的计算机信息系统的安全性、可靠性和经济性进行检查、监督，通过获取审计证据并对其进行客观评价所开展的系统的、独立的、形成文件的活动。

4. 通用评价要求

通用评价要求适用于风险评估、安全集成、应急处理、灾难备份与恢复、软件安全开发、安全运维、网络安全审计等类别的信息安全服务认证评价，均分为三个级别，其中一级最高。

4.1. 三级评价要求

4.1.1. 办公场所要求

拥有长期固定办公场所和相适应的办公条件，能够满足机构设置及其业务需要。

4.1.2. 人员能力要求

技术负责人应具备与申报类别一致的信息安全服务管理能力；项目负责人、项目工程师应具备与申报类别一致的信息安全服务技术能力。能力评价要求参考附录 H。

4.1.3. 业绩要求

a) 从事信息安全服务（与申报类别一致）6个月以上。

b) 近3年内签订并完成至少1个信息安全服务（与申报类别一致）项目。

4.1.4. 服务管理要求

a) 建立并运行文档管理程序，包括组织管理、服务过程管理、质量管理等内容，明确项目产生、发布、保存、传输、使用（包括交付和内部使用）、废弃等环节的文档控制。

b) 建立并运行项目管理程序，明确服务项目的组织、计划、实施、风险控制、交付等环节的操作规程，提供项目风险管理记录。

c) 建立并运行保密管理程序，明确岗位保密责任，签订保密协议，并能够适时对相关人员进行保密教育。

d) 建立与运行供应商管理程序，确保其供应商满足服务安全要求（仅适用于安全集成、安全运维、灾难备份与恢复方向）。

4.1.5. 技术工具要求

应配备承担信息安全服务（与申报类别一致）所需的安全、可信的软硬件工具和设备。

4.1.6. 服务技术要求

建立和制定信息安全服务（与申报类别一致）所需的流程和规范，并遵照实施。

4.2. 二级评价要求

4.2.1. 办公场所要求

拥有长期固定办公场所和相适应的办公条件，能够满足机构设置及其业务需要。

4.2.2. 人员能力要求

技术负责人应具备与申报类别一致的信息安全服务管理能力；项目负责人、项目工程师应具备与申报类别一致的信息安全服务技术能力。能力评价要求参考附录 H。

4.2.3. 业绩要求

a) 从事信息安全服务（与申报类别一致）3年以上，或取得信息安全服务（与申报类别一致）三级1年以上。

b) 近3年内签订并完成至少6个信息安全服务（与申报类别一致）项目。

4.2.4. 服务管理要求

a) 建立并运行文档管理程序，包括组织管理、服务过程管理、质量管理等内容，明确项目产生、发布、保存、传输、使用（包括交付和内部使用）、废弃等环节的文档控制。

b) 建立并运行项目管理程序，明确服务项目的组织、计划、实施、风险控制、交付等环节的操作规程，提供项目风险管理记录。

c) 建立并运行保密管理程序，明确岗位保密责任，签订保密协议，并能够适时对相关人员进行保密教育。

d) 建立与运行供应商管理程序，确保其供应商满足服务安全要求（仅适用于安全集成、安全运维、灾难备份与恢复方向）。

4.2.5. 技术工具要求

应配备承担信息安全服务（与申报类别一致）所需的安全、可信的软硬件工具和设备。

4.2.6. 服务技术要求

建立和制定信息安全服务（与申报类别一致）所需的流程和规范，并遵照实施。

4.3. 一级评价要求

4.3.1. 办公场所要求

拥有长期固定办公场所和相适应的办公条件，能够满足机构设置及其业务需要。

4.3.2. 人员能力与要求

技术负责人应具备与申报类别一致的信息安全服务管理能力；项目负责人、项目工程师应具备与申报类别一致的信息安全服务技术能力。能力评价要求参考附录 H。

4.3.3. 业绩要求

a) 从事信息安全服务（与申报类别一致）5年以上，或取得信息安全服务（与申报类别一致）二级1年以上。

b) 近3年内签订并完成至少10个信息安全服务（与申报类别一致）项目。

4.3.4. 服务管理要求

c) 建立并运行文档管理程序，包括组织管理、服务过程管理、质量管理等内容，明确项目产生、发布、保存、传输、使用（包括交付和内部使用）、废弃等环节的文档控制。

d) 建立并运行项目管理程序，明确服务项目的组织、计划、实施、风险控制、交付等环节的操作规程，提供项目风险管理记录。

e) 建立并运行保密管理程序，明确岗位保密责任，签订保密协议，并能够适时对相关人员进行保密教育。

f) 建立与运行供应商管理程序，确保其供应商满足服务安全要求（仅适用于安全集成、安全运维、灾难备份与恢复方向）。

4.3.5. 技术工具要求

应配备承担信息安全服务（与申报类别一致）所需的安全、可信的软硬件工具和设备。关键软硬件工具和设备的安全性应获得第三方评价或者证明。

4.3.6. 服务技术要求

建立和制定信息安全服务（与申报类别一致）所需的流程和规范，并遵照实施。

5. 专业评价要求

5.1. 风险评估服务专业评价要求

风险评估服务专业评价要求参见附录A。

5.2. 安全集成服务专业评价要求

安全集成服务专业评价要求参见附录B。

5.3. 应急处理服务专业评价要求

应急处理服务专业评价要求参见附录C。

5.4. 灾难备份与恢复服务专业评价要求

灾难备份与恢复服务专业评价要求参见附录D。

5.5. 软件安全开发服务专业评价要求

软件安全开发服务专业评价要求参见附录E。

5.6. 安全运维服务专业评价要求

安全运维服务专业评价要求参见附录F。

5.7. 网络安全审计服务专业评价要求

网络安全审计服务专业评价要求参见附录G。

附录 I：参考文献

[1] GB/T 20261-2020 信息安全技术 系统安全工程 能力成熟度模型

[2] YD/T 1621-2007 网络与信息安全服务资质评价准则

[3] YD/T 2252-2011 网络与信息安全风险评估服务能力评价方法

[4] RB/T 201-2013 信息系统安全集成服务资质认证评价要求