ICS 35.040
L 80

中华人民共和国国家标准

GB/T 32914—2016

信息安全技术
信息安全服务提供方管理要求

Information security technology—
Information security service provider management requirements

2016-08-29 发布　　2017-03-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准主要起草单位:中国信息安全认证中心、上海三零卫士信息安全有限公司、中国电子技术标准化研究院等。

本标准主要起草人:翟亚红、陈晓桦、邬敏华、上官晓丽、张剑、严妍、贾雪飞、张斌、张志军、路明、张建军。

信息安全技术
信息安全服务提供方管理要求

1 范围

本标准规定了信息安全服务提供的术语和定义、信息安全服务原则、信息安全服务组织级管理和信息安全服务项目级管理的要求。

本标准适用于信息安全服务提供方对其服务要素和服务风险进行管控，对信息安全服务需求方、评价机构和监管部门具有参考意义。

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 22080—2008 信息技术 安全技术 信息安全管理体系 要求

GB/T 24405.1—2009 信息技术 服务管理 第1部分：规范

GB/T 30283—2013 信息安全技术 信息安全服务 分类

3 术语和定义

GB/T 30283—2013 界定的以及下列术语和定义适用于本文件。

3.1

信息安全服务 information security service

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一个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、产品或管理体系的，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形式进行。

3.2

信息安全服务需求方 information security service acquirer

获取外部所提供的信息安全服务，以满足信息安全需求和信息安全保障需求，实现自身业务目标的组织(或个人用户)。

3.3

信息安全服务提供方 information security service provider

按照服务协议，通过专业的信息安全人员提供信息安全服务的组织。

3.4

服务协议 service agreement

服务需求方和服务提供方在服务开始前共同签署的约定，并在服务过程中共同遵守。

注：通常包含服务原则、服务内容、服务形式、服务级别、服务价格、服务交付成果、服务安全要求等，在形式上可以是服务合同及其附属的工作说明书。

3.5

服务级别　service level

在服务协议中对服务交付成果明确约定、可测量和文档化的一系列服务指标。

3.6

服务目录　service catalogue

在服务协议中明确展示服务内容、服务形式、服务价格、服务交付成果和服务级别等的一份列表。

3.7

服务组合　service portfolio

多个服务类别或服务项目以及其他工作的集合。

3.8

供应链　supply chain

通过多个资源和过程联系在一起的一系列组织，根据由服务协议或其他采购协议建立连续的供应关系，每个组织充当一个需求方、提供方或双重角色。

3.9

可视性　visibility

系统或过程所具备的可以对系统元素和过程进行记录、监视和检查的属性。

3.10

服务要素　service factors

设计和实施服务的关键要素，包括服务人员、服务流程、服务工具、规章，以及其他服务所需的资源。

3.11

服务方案　service plans

基于服务目标，对服务各阶段中所需执行的过程、任务、活动以及相关服务要素、服务级别进行详细描述的文档。

3.12

服务工具　service tools

为达成服务目标或提高服务质量和效率所需要的设备、软件、模板、知识库等。

3.13

服务变更　service change

任何可能对服务产生影响的新增、修改或解除的活动。

注：服务变更可能涉及服务的范围、人员、内容、形式、价格、时间、方案、流程、工具、服务级别等。

4　信息安全服务原则

4.1　合规性

遵循国家和行业关于信息安全服务的要求，基于明确的信息安全保障需求和信息安全服务目标。具体原则如下：

a）　应符合国家信息安全法律法规和政策、国家和行业相关信息安全标准的要求；

b）　应遵循服务要素可视性、服务行为预先告知、服务和产品中立、资产保护等信息安全服务原则；

c）　应根据信息安全服务类别，通过需求调研、风险评估等手段，提取信息安全保障需求；

d）　应根据信息安全保障需求，结合服务对象业务、系统或设备的实际情况，确定信息安全服务目标；

e）　应按照服务协议所规定的关键节点、交付成果和服务级别要求，记录、监视、检查和评审服务目标的完成情况及差异程度。

4.2 数据和业务保护

在信息安全服务实施过程中，对信息安全服务需求方的数据和业务进行保护。具体原则如下：

a) 在服务实施之前，应与需求方签订数据保护协议，明确规定身份数据、业务数据、系统数据等保护内容，明确规定最小数据范围、最小特权访问、最小服务用途等保护要求；

b) 应对在服务实施过程中所获得或产生的信息资料，只在服务范围内进行数据合理利用，并采用必要的安全措施进行妥善保管；

c) 应采取相应的措施防止因信息安全服务的实施，影响需求方的系统正常使用和业务正常开展，或造成对 IT 资产的损害；

d) 针对直接作用于信息系统的信息安全实施服务，应事先对服务意外中断或终止的影响进行确认，并制定应对措施；

e) 在服务实施完成之后，应按需求方和服务协议的要求，进行资料、账号、证件等清理工作（例如：移交、注销、销毁等）。

5 信息安全服务组织级管理

5.1 制度和体系

建立并施行满足信息安全服务所需的管理制度或管理体系。具体要求如下：

a) 应确定一名高层管理者全面负责信息安全服务相关管理制度或管理体系的建立、实施、运行、监视、评审、保持和改进；

b) 应按照 GB/T 24405.1—2009 和 GB/T 22080—2008 要求建立管理制度或管理体系，并保证与所提供的信息安全服务类别相适宜且有效；

c) 应将服务项目纳入与管理制度或管理体系相符合的管理流程或管理工具中，并定期对制度执行情况进行内部检查，保证服务质量的持续改进；

d) 应对组织内部所有相关人员进行管理制度或管理体系的教育、培训和考核；

e) 应遵循需求方相关的管理制度和业务流程。

5.2 人力资源

建立并执行满足信息安全服务所需的人力资源管理制度。具体要求如下：

a) 应具有与信息安全服务类别相符合的人力资源规模和结构，建立相应的人员安全管理制度；

b) 应在员工任用前、任用中、任用终止具有不同的措施，保证员工正确理解信息安全服务原则，并能够在工作中切实予以贯彻；

c) 应具有独立设置的专业技术部门或团队，稳定地开展信息安全服务；

d) 应确保具有信息安全相关资格的技术人员数量（例如：持证上岗等），并保证这些人员具备足够的专业工作经验；

e) 应保证组织内部与信息安全服务有关的其他人员具有基本的信息安全知识；

f) 宜建立服务实施人员完整的工作履历表，包含人员基本信息、专业能力证明和曾经参与服务的所有记录。

5.3 保密

建立并执行满足信息安全服务所需的保密管理制度。具体要求如下：

a) 应建立并执行满足服务所需的保密管理制度，保证组织内部员工对组织和需求方履行保密义务；

b) 应与信息安全服务相关人员签订保密协议，并定期进行保密教育和保密检查；
c) 应具备安全保密的工作环境和工作流程（例如：指派专人负责将服务的资料进行单独保管、采用安全的措施存放各类介质资料、准备独立且不联网的计算机以存放有保密要求的电子文档等）；
d) 应遵循需求方相关的保密管理制度和工作流程；
e) 凡涉及国家秘密的信息安全服务，应按照国家相关的保密法律法规、政策和标准执行。

5.4 技术能力

具备满足信息安全服务所需的技术能力、服务工具和服务环境。具体要求如下：
a) 应持续关注并及时掌握国家信息安全相关法律法规、政策和标准中对技术的要求；
b) 应持续跟踪国内外信息技术动向，研究与之相关的信息安全技术，并熟悉国内外主流的信息安全产品和服务，不断提升自身的技术能力；
c) 应关注国内外权威机构发布的态势报告及漏洞公告，对安全威胁和安全脆弱点有全面的了解；
d) 应具备与信息安全服务类别相关的服务工具（例如：设备、软件、模板、知识库等）；
e) 应针对信息安全实施服务，具备服务所必需的开发、测试和管理环境（例如：平台和设备）。

5.5 服务协议

与信息安全服务需求方以服务协议的方式对信息安全服务进行约定并执行。具体要求如下：
a) 应在服务协议中，根据行业或需求方认可的规范模版，明确规定信息安全服务的范围、目标和验收等条款，并采用服务目录的方式确定服务内容和服务形式；
b) 应在服务目录中，确定每项服务的价格、成本，并在服务实施过程中进行有效的财务管理；
c) 应在服务目录中，确定每项服务的交付成果、服务级别，并在服务实施过程中进行有效的质量管理（例如：监视、检查、评审和报告等）；
d) 在服务协议签订前，应共同评审协议，就服务协议各项条款及其条件和要求与需求方达成一致；
e) 在服务协议签订后，应严格按照服务协议和服务目录实施信息安全服务，对于服务协议执行过程中所产生的双方不能解决的争议，宜提交专业机构仲裁；
f) 未经需求方许可，不得将信息安全服务进行转包、分包；
g) 针对信息安全实施服务，应按行业或需求方的要求，接受安全监理、安全审计等方式来监督和确认服务协议的执行。

5.6 服务组合

建立并落实对多个信息安全服务类别或服务项目的组合管理。具体要求如下：
a) 应从组织战略层面，建立并落实对多个服务类别或服务项目的组合管理，改善项目负责人和组织管理者之间的沟通关系；
b) 应建立服务组合管理流程，确定服务项目之间相互关联或依赖关系，并提出服务保障承诺，提高服务项目的成功率；
c) 应基于不同服务项目的服务目标和服务级别，保证在组织范围内进行服务要素的分配和管理，取得项目之间的平衡，保证服务资源的配置最优化；
d) 应为所有服务项目制定预算并进行财务管理（例如：授权和监控），有效分配服务的间接费用和直接成本；
e) 对于服务的新增或变更，应保证所有项目的服务交付和服务级别控制在组织的资金和资源能力之内，并应评估由此对组织、技术和商业产生的影响；

f) 应定期根据服务组合情况，识别服务项目运营风险，评估组织的信息安全服务能力，改进服务保障能力，提高对环境变化的快速响应能力。

5.7 供应链

具备并保障信息安全服务所需的供应链资源。具体要求如下：

a) 作为供应链下游获取方，与每个供应链上游提供方明确规定管理规范、过程接口，签订服务协议或采购协议，并对其进行有效的监视和评审；

b) 应保持与信息安全服务类别相关的产品提供商、服务提供商、专业机构等外部供应链的良好合作关系，并履行服务和产品中立原则；

c) 应主动与需求方进行事先说明服务项目涉及的外部供应链及其支撑关系，并得到其确认；

d) 应将信息安全服务的原则和目标，服务目录相关要求有效传递到服务项目涉及的外部供应链，并通过合同或协议的方式进行有效管理。

6 信息安全服务项目级管理

6.1 服务方案

以服务方案的方式对信息安全服务项目的目标实现进行详细描述。具体要求如下：

a) 应根据信息安全服务目标，参照相关标准、规范，制定信息安全服务的各类方案（包括：设计方案、实施方案、验证方案等）；

b) 应保证各类服务方案与服务协议中所约定的各项条款要求相一致，并明确需求方在服务过程中所需具备的条件；

c) 应在服务实施方案中明确规定每一个具体的服务过程、任务、活动，对应的服务要素，以及服务成果或服务级别；

d) 应与需求方就服务方案进行充分沟通，并得到其确认；

e) 宜采用第三方评审的方式来确定服务方案。

6.2 服务人员

具备并保障满足信息安全服务项目所需的人员和团队。具体要求如下：

a) 应建立相关机制保障服务人员及相关工作人员仅限于中国公民；

b) 应对服务项目确定信息安全第一责任人；

c) 应对服务项目清晰定义服务实施团队中所有服务人员的角色和职责，并对其进行身份和权限管理；

d) 应确保服务实施人员具备能满足服务项目所需的专业知识、技能和经验，具备相关的信息安全专业资质；

e) 应保证服务实施团队的整体稳定和可用，定期开展与信息安全服务相关的各类教育培训，宜建立层次化的服务组织结构（例如：多线支持、专家团队等）。

6.3 服务过程

明确在信息安全服务项目服务过程中的日常管理和应急管理。具体要求如下：

a) 应保证服务过程遵循相关的标准、规范或最佳实践（例如：系统安全工程能力成熟度模型、信息系统安全等级保护基本要求、信息安全管理体系要求等），并主动告知需求方；

b) 应对需要进行服务交接或服务导入的信息安全服务，做好服务实施前的准备工作（例如：资产识别、信息分类、技术交底、业务培训等），并在通过需求方确认后，才能正式实施服务；

c) 应落实并保证该服务项目所需的所有服务要素(例如:人员、流程、工具和资源等)在服务实施过程中,符合服务协议和服务方案中的约定;
d) 应建立并执行项目管理制度,保证在每一个具体的服务过程、任务、活动,均严格按照服务方案和管理制度进行,形成记录,定期检查和评审,并采取改进措施;
e) 应及时响应并妥善解决在服务实施过程中产生的事件,并对其潜在的原因进行问题管理(例如:识别和消除);
f) 针对信息安全实施服务,应建立与该服务项目相关的应急预案,并保障应急处置所需的相关资源。

6.4 服务工具和平台

具备并保障满足信息安全服务项目所需的工具和平台。具体要求如下:
a) 应具备能满足服务项目所需的服务工具或服务平台,保证其合法版权,并充分考虑其适用性;
b) 应保证服务工具或服务平台仅用于达成该服务项目的服务目标,不会因引入新的安全隐患或因不当操作对业务造成影响或损害;
c) 应保证服务工具或服务平台在多个服务项目之间的共享环境安全(例如:信息传输和处理的隔离等);
d) 应主动就服务所使用的服务工具或服务平台,与需求方进行事先说明、技术培训和必要的功能性能测试,并得到其确认;
e) 服务工具或服务平台宜通过国家认可的第三方机构的安全测评或认证。

6.5 服务风险

对信息安全服务项目服务过程中的各类风险(不仅是信息安全风险)进行评估和控制。具体要求如下:
a) 在服务实施之前,应从服务要素(例如:人员、流程、工具和资源等)各方面,识别服务实施过程中可能产生的各类风险;
b) 对已识别的风险进行评估,应采取适当的风险控制措施,并对实际效果进行跟踪确认;
c) 应与需求方就风险及其控制措施进行充分的沟通,并取得必要的确认(例如:授权、现场监督等);
d) 应针对服务实施过程中的重大业务变更、IT 资产变更、服务要素变更,以及服务实施的重要时期和关键节点等,加强对风险的监控和预警,并及时提供风险提示报告。

6.6 服务变更

制定信息安全服务项目变更管理流程,确保变更受控。具体要求如下:
a) 应保证服务变更(例如:范围、人员、内容、形式、价格、时间、方案、服务级别等)不能影响既定的服务原则和服务目标;
b) 应制定服务项目变更管理流程,与需求方就服务变更进行主动沟通,确保服务变更以受控的方式得到评估、批准、实施和评审;
c) 应跟踪变更后对服务原则、服务目标、服务质量和效率、需求方信息系统和业务造成的影响,并进行针对性的改进、补救或恢复;
d) 应确保未经需求方许可,不得进行超出服务协议范围的操作,不得擅自对系统或数据进行变更。

6.7 服务沟通

建立并施行满足信息安全服务项目所需的沟通机制。具体要求如下:

a) 应与需求方共同确定各自的项目负责人和沟通接口人，建立项目沟通机制；
b) 在服务准备、计划、实施、终止各阶段，应与需求方、其他利益相关方，均保持畅通和良好的沟通；
c) 应主动将管理制度或管理体系、保密管理制度等告知需求方；
d) 应通过通知、会议、报告等多种形式进行正式沟通，并就沟通内容和结论进行记录；
e) 针对服务实施过程中产生的客户投诉或争议，应事先与需求方确定处理流程并形成过程记录，在实际处理中应有明确的沟通结论和解决方案，并得到需求方的确认。

6.8 服务交付

以服务交付的方式对信息安全服务项目进行确认和验收。具体要求如下：

a) 应按服务协议中所规定的关键节点，正式提交服务交付成果（例如：服务方案、服务过程记录、服务阶段报告、服务验收总结等），并得到需求方的确认；
b) 应保证所有服务交付成果的完整性和详实性，均能清晰阐明其目的、依据、组成、结论、措施、数据来源及支撑材料等内容；
c) 针对信息安全实施服务，应按行业或需求方的要求，接受安全监理、风险评估等方式对服务交付成果进行检查、评审和验收；
d) 在服务阶段交付之后，宜进行服务管理的改进，在服务完全交付之后，宜进行服务满意度调查；
e) 应对所有服务交付成果建立服务档案，按相关规定的期限和要求进行妥善保管。

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 28827.1—2012 信息技术服务 运行维护 第1部分:通用要求
[3] GB/T 24405.2—2010 信息技术 服务管理 第2部分:实践规则
[4] GB/T 22081—2008 信息技术 安全技术 信息安全管理实用规则
[5] YD/T 1621—2007 网络与信息安全服务资质评估准则
[6] ISO/IEC DIS 27036-1 信息技术 安全技术 供应链关系信息安全 第1部分:概述和概念
[7] ISO/IEC DIS 27036-2 信息技术 安全技术 供应链关系信息安全 第2部分:通用要求
[8] NIST SP800-35 信息技术安全服务指南
[9] CMU/SEI OMSS(Outsourcing Managed Security Services) 可管理安全服务外包