



中华人民共和国国家标准

GB/T 32926—2016

信息安全技术 政府部门信息技术服务 外包信息安全管理规范

Information security technology—Information security management specification
for government information technology service outsourcing

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

目 次

前言	III
引言	IV
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 综述	2
4.1 服务外包信息安全管理基本原则	2
4.2 服务外包信息安全管理角色和职责	2
4.3 服务外包信息安全管理模型	3
5 规划准备	3
5.1 服务外包信息安全风险评估	3
5.2 服务外包信息安全管理策略和制度	4
6 机构和人员选择	4
6.1 外包服务机构和人员风险评估	4
6.2 服务外包合同	5
6.3 服务外包信息安全管理计划	6
6.4 信息安全保密协议	6
6.5 外包服务机构备案	6
7 运行监督	7
7.1 服务过程评估审计	7
7.2 阶段成果交付验证	7
8 改进和完成	7
8.1 服务改进	7
8.2 服务退出	7
附录 A (规范性附录) 服务外包基本信息安全控制	9
参考文献	12

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。

本标准起草单位:北京信息安全测评中心、工业和信息化部电子科学技术情报研究所、信息产业信息安全测评中心、中国信息安全研究院有限公司。

本标准主要起草人:刘海峰、钱秀槟、梁博、赵章界、刘迎、霍珊珊、张晓梅、王春佳、李晨旻、张恒、张益、耿贵宁。

引 言

随着经济社会的快速发展,政府部门在打造和建设服务型政府、不断提高为人民服务能力和水平的过程中,越来越多地采用和依赖信息化手段,并为此开展了与信息化相关的信息技术咨询、信息系统集成、运行维护、安全测评等服务外包工作。大量政务信息化工作的外包,既解决了政府行政资源有限和公共服务效能要求日益提高之间的矛盾,也提高了政府部门信息化工程的质量。但政府部门在享受信息技术服务外包带来便捷的同时,也面临外包服务机构背景复杂、服务人员流动性大、内部管理不规范等问题带来的信息安全风险,如果缺乏对服务外包活动信息安全的标准化管理,将对政府部门行政办公、人民群众生产生活,乃至国家安全带来巨大损失。

本标准用于规范和指导政府部门采购和使用信息技术服务。本标准通过对政府部门服务外包过程进行梳理,建立了政府部门信息技术服务外包信息安全管理模型,在明确了服务外包信息安全管理角色和责任的同时,将管理活动划分为规划准备、机构和人员选择、运行监督、改进完成四个阶段,分别提出信息安全管理规范,为政府部门信息技术服务外包的安全管理提供参考。

政府部门在信息技术服务外包的信息安全管理过程中,还要基于本标准提出的规范要求和基本控制措施,结合自身服务外包项目实际,提出与组织机构、人员管理、数据管理、信息技术服务类型等相适应的控制措施,分阶段、有侧重地对服务外包活动实施管理,以便信息安全管理规范的要求能够切实指导不同层级政府部门实际的服务外包信息安全管理,提升其服务外包信息安全水平。

信息安全技术 政府部门信息技术服务 外包信息安全管理规范

1 范围

本标准建立了政府部门信息技术服务外包信息安全管理模型,提出了政府部门信息技术服务外包信息安全管理生命周期各阶段活动的管理要求。

本标准适用于政府部门采购和使用信息技术服务。

政府部门开展涉密信息技术服务外包工作,参照国家保密局相关保密规定和标准执行,不在本标准范围内。

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 29245—2012 信息安全技术 政府部门信息安全管理基本要求

3 术语和定义

GB/T 25069—2010 界定的以及下列术语和定义适用于本文件。

3.1

信息技术服务 **information technology service**

供方为需方提供开发、应用信息技术的服务,以及供方以信息技术为手段提供支持需方业务活动的服务。

[GB/T 29264—2012]

注:常见服务形态有信息技术咨询服务、设计与开发服务、信息系统集成实施服务、运行维护服务、数据处理和存储服务、运营服务、数字内容服务、呼叫中心服务及其他信息技术服务。

3.2

服务外包 **service outsourcing**

政府部门以签订合同的方式,委托其他机构承担信息技术服务的商业行为。

3.3

外包服务机构 **organization providing outsourced service**

服务外包中承担信息技术服务的机构。

3.4

服务分包 **service subcontraction**

外包服务机构将自身承担的部分政府部门信息技术服务再次委托给其他机构完成的商业行为和管理模式。