ICS 35.040
L 80

中华人民共和国国家标准

GB/T 30283—2013

信息安全技术
信息安全服务　分类

Information security technology—
Information security service—Category

2013-12-31 发布　　2014-07-15 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

本标准按照 GB/T 1.1—2009 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:上海三零卫士信息安全有限公司、中国信息安全测评中心、中国信息安全认证中心、中国电子技术标准化研究院。

本标准主要起草人:邬敏华、张建军、陈晓桦、李斌、胡啸、杨建军、陈长松、闵京华、曹雅斌、张晓菲、翟亚红、王琰、沈传宁。

信息安全技术
信息安全服务　分类

1　范围

本标准规定了信息安全服务分类，包括信息安全咨询类、信息安全实施类、信息安全培训类及其他类四个方面。

本标准适用于信息安全行业对信息安全服务概念的理解和分类管理，适用于信息安全服务的开发、提供、选用和采购。

本标准不适用于仅依附于某一信息安全产品的服务（如信息安全产品的使用、维保等服务）。

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 5271.8—2001　信息技术　词汇　第8部分：安全

GB/T 22080—2008　信息技术　安全技术　信息安全管理体系　要求

GB/T 22239—2008　信息安全技术　信息系统安全等级保护基本要求

GB/T 25058—2010　信息安全技术　信息系统安全等级保护实施指南

3　术语和定义

GB/T 5271.8—2001 中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：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。

3.2

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

有偿采购（或免费使用）外部所提供的信息安全服务，以满足信息安全保障需求，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各类组织机构。

注：信息安全服务提供方在每项具体的服务中承担相应的服务角色和服务职责。如果服务内容仅涉及供需双方的，则服务提供方为乙方角色；在上述服务的基础上，就所涉及的问题，独立于有关各方提供评估、证明等服务并承担相关社会责任的，则服务提供方为第三方角色。服务角色与服务提供方的组织机构类型无关。

3.4

服务协议　service contract

服务需求方和服务提供方在服务开始前共同达成的约定，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、服务级别协议、服务价格、服务交付物、服务安全要求等，在形成上可以是服务合同及其附属的工作说明书。

3.5

服务类别　service category

一组具有共同目标对象和服务特征的、但侧重点可能不同的服务组件的集合。

3.6

服务组件　service component

可包含在服务协议中的最小可选服务。

3.7

服务实例　service instance

为满足某一确定的安全保障目的而组合在一起的，一组可重用的服务组件。

3.8

信息安全咨询服务　information security consulting service

面向组织的信息安全服务，围绕组织信息系统所支持的业务和管理，通过知识传递、工作辅导和系统规划等形式提供信息安全服务。

3.9

信息安全实施服务　information security implementation service

面向组织或个人用户的信息安全服务，围绕组织信息系统或个人信息设备，及其基础设施、业务应用和信息数据的安全和可用，通过人力派遣、设施租用、流程外包等形式提供信息安全服务。

3.10

信息安全培训服务　information security training service

面向组织内人员或个人的信息安全服务，围绕信息安全意识、技术、管理等方面，通过授课、实操、考核等形成提供信息安全服务。

4　信息安全服务分类

本标准采用“服务类别—服务组件”这种层次结构来描述服务分类，见表1。信息安全服务分类的原则是：将相对独立的服务尽量细分为服务组件，将具有相同或相近服务界面（服务目标对象、服务供需关系、服务特征和服务质量要素等）的服务组件归并为同一服务类别。

本标准采用层次代码结构，共分二层，第一层采用一位字母表示信息安全服务类别；第二层采用两位数字表示信息安全服务组件，第二层中数字为“99”均表示收容类目。代码的表示形式如下：

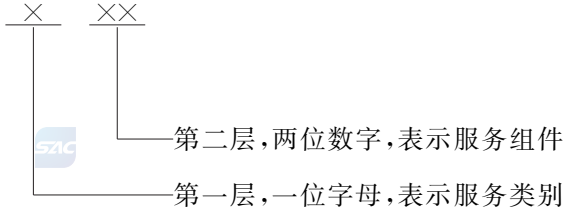

表 1　信息安全服务分类

服务类别		服务组件		目标对象
代码	名　称	代码	名　称	
A	信息安全咨询服务	A01	信息安全规划	组织的信息系统及其所支持的业务和管理
		A02	信息安全管理体系咨询	
		A03	信息安全风险评估	
		A04	信息安全应急管理咨询	
		A05	业务连续性管理咨询	
		A99	其他信息安全咨询服务	
B	信息安全实施服务	B01	信息安全设计	组织的信息系统； 个人的信息设备
		B02	信息安全产品部署	
		B03	信息安全开发	
		B04	信息安全加固和优化	
		B05	信息安全检查和测试	
		B06	信息安全监控	
		B07	信息安全应急处理	
		B08	信息安全通告	
		B09	备份和恢复	
		B10	数据修复	
		B11	电子认证服务	
		B12	信息安全监理	
		B13	信息安全审计	
		B99	其他信息安全实施服务	
C	信息安全培训服务	C01	信息安全培训	信息安全相关人员
Z	其他信息安全服务			

基于这种分类，信息安全服务均可以服务实例的形式，由一个或多个服务类别或者（及其）服务组件所构成，某些还可能包含本标准不涉及的其他扩展服务。典型的信息安全服务实例有以下十种类型：安全咨询、风险评估、安全集成、安全运维、应急处理、灾难恢复、安全培训、安全测评、安全监理、安全审计。典型的信息安全服务实例与其可能包含的服务组件之间的关系见附录 A。

信息安全服务与信息安全法律、政策密切相关。例如：根据我国计算机信息系统实行安全等级保护的要求，按上述分类，可开展等级保护咨询、等级保护建设（整改）、等级保护测评、等级保护培训等信息安全服务。

5　信息安全咨询服务

5.1　概述

信息安全咨询服务的服务界面为：

a） 服务对象

面向组织的信息系统及其支持的业务和管理。

b） 服务供需

服务提供方提供信息安全领域的知识传递、工作辅导、系统规划等服务内容，以满足组织对外部“专业知识”的需求，从而提高自身的信息安全管理、规划、分析和决策能力。

c） 服务特征

基于组织整体的使命和业务，以人力的方式提供相关咨询，服务交付物通常是一些文档。

d） 服务质量

首先取决于服务人员的专业知识、经验的丰富程度，其次取决于服务人员的理解、分析和沟通等综合能力。服务人员与组织内有关人员（尤其是信息安全责任部门人员）的有效交互过程是咨询服务成败的关键。

e） 服务组件

包括：信息安全规划、信息安全管理体系咨询、信息安全风险评估、信息安全应急管理咨询、业务连续性管理咨询、其他信息安全咨询服务。

5.2 信息安全规划

信息安全规划主要是从组织核心业务、核心价值出发，根据组织的发展战略，通过风险评估等方式提取组织的安全需求，对相应的安全保障目标、任务、措施和步骤进行规划。信息安全规划站在组织整体的角度，从策略、组织、管理、技术、资源等多方面进行综合考虑，涉及综合管理、技术规范、工程建设、运行维护等多个层面。信息安全规划的成果，是组织在一段时间内开展信息安全保障工作的依据。

5.3 信息安全管理体系咨询

信息安全管理体系咨询主要是依照国际或国家信息安全管理体系相关标准，基于业务风险方法，通过定义范围和方针、业务分析、风险评估、设计、实施等步骤，面向组织建立、实施、运行、监视、评审、保持和改进信息安全的体系。信息安全管理体系是一个组织整个管理体系的一部分，包括组织结构、方针策略、规划活动、职责、实践、规程、过程和资源等多个方面。常见的信息安全管理体系有 GB/T 22080—2008、GB/T 22239—2008 中的管理要求等。

5.4 信息安全风险评估

信息安全风险评估主要是依据有关信息安全技术与管理标准，从风险管理角度，对信息系统及由其处理、传输和存储的信息的保密性、完整性和可用性等安全属性进行评价的过程，通过评估资产面临的威胁以及威胁利用脆弱性导致安全事件的可能性，结合安全事件所涉及的资产价值来判断安全事件一旦发生对组织造成的影响，并提出有针对性的抵御威胁的防护对策和整改措施。信息安全风险评估贯穿于信息系统的规划、设计、实施、运行维护以及废弃各个阶段。

5.5 信息安全应急管理咨询

信息安全应急管理咨询主要是针对各类各级信息安全事件，从应急管理角度，通过编制应急预案和指导应急演练，面向组织建立信息安全应急管理体系，不断进行改进和提高，应急预案的内容包括：建立组织的应急响应小组，制定应急响应流程，建立监测和预警机制，落实应急保障资源，制定子预案及相关支持文档，以及指导实施应急处理（见 6.8）等。

5.6 业务连续性管理咨询

业务连续性管理咨询主要是为保护组织的核心业务、核心价值，从保障组织的业务持续开展出发，

通过识别组织业务的连续性指标要求，识别潜在的威胁和相关影响，制订业务连续性计划和灾难恢复计划，最终帮助组织建立一套综合管理流程，形成组织的业务保持和恢复能力，提高组织的风险防范能力，有效地响应非计划的业务破坏并降低不良影响。

6 信息安全实施服务

6.1 概述

信息安全实施服务的服务界面为：

a） 服务对象

面向具体的（组织）信息系统或（个人）信息设备。

b） 服务供需

服务提供方提供与信息安全相关的技术保障、管理保障等直接支撑，以满足组织（或个人）对专业技能、专业人员、专业工具的需求，从而保障信息系统整体或各层面的安全性。

c） 服务特征

基于对信息系统全生命周期的信息安全保障，为系统的建设和运行提供相关的实现，具有较高的重复性。

d） 服务质量

取决于服务提供方的整体专业能力和服务成熟度，主要包括：组织管理、专业知识、技术能力、人员素质、工具平台、服务经验、外部资源等方面。服务需求方的积极参与可以提高实施服务成效。

e） 服务组件

包括：信息安全设计、信息安全产品部署、信息安全开发、信息安全加固和优化、信息安全检查和测试、信息安全监控、信息安全应急处理、信息安全通告、备份和恢复、数据修复、电子认证服务、信息安全监理、信息安全审计、其他信息安全实施服务。

6.2 信息安全设计

信息安全设计主要是针对信息系统的安全保障需求，对组织的安全规划进行落实，设计总体安全策略、制定信息安全建设方案和实施方案，并在此基础上形成安全架构、技术体系和管理体系的设计。信息安全设计一般可分为顶层设计、初步设计和详细设计等不同的服务交付物。信息安全设计还可以包含对信息安全产品的功能和性能设计，以及选型建议。

6.3 信息安全产品部署

信息安全产品部署主要是根据信息系统安全设计方案，对已采购、租用或开发的信息安全产品进行安装配置、功能调试和性能测试，以及对相关人员的必要培训等，以达到预期的安全要求。一般包括各类信息安全产品的独立部署、各自部署或者组合部署（集成部署）。

信息安全产品部署还可以包含对信息安全产品的采购，即按照设计方案中的要求，依据相关主管部门的管理要求，以产品性价比为原则，完成产品及其后续服务的采购。

6.4 信息安全开发

信息安全开发主要是按照信息安全设计方案的安全目标和安全功能，对于一些不能通过采购现有信息安全产品来满足的安全需求，通过定制开发而予以满足。信息安全开发也可以基于已有的信息安全产品进行二次开发。

6.5 信息安全加固和优化

信息安全加固主要是针对组织在实施风险评估、安全检查和测试过程中发现的各种安全风险、系统漏洞和不符合项，依据既定的信息安全策略，采取措施予以弥补，消除已暴露的问题和可能的隐患。信息安全优化主要是基于风险评估等方法，对现有网络和系统架构进行调整和优化，或对现有设备的安全策略进行设置和调整。在实际服务中，信息安全加固和信息安全优化往往同时进行。

6.6 信息安全检查和测试

信息安全检查主要是针对组织部署的信息安全技术措施及其运行记录进行检查或审查，验证安全措施的完整性和有效性，并及时发现异常活动和潜在风险。一般包括对信息系统各层面的运行状态检查、配置项检查、日志分析等，也包括借助专门的安全审计设备来实施检查。信息安全检查还可以包含对信息安全管理措施和相关人员的检查。

信息安全测试主要是针对信息系统及其产品的安全属性，采取动态的手段进行问题发现、符合性和有效性验证。一般包括信息系统测试、漏洞扫描和渗透性测试等。信息系统测试是指将已经确认的信息系统组成元素结合在一起，进行各种组装测试和确认测试，发现所开发的系统与安全需求不符或矛盾的地方，从而提出安全整改方案。漏洞扫描服务是指借助一些专业的漏洞扫描工具，发现信息系统各层面存在的安全漏洞，为信息安全加固提供支持信息。渗透性测试是指信息安全服务提供者的专业人员模拟攻击行为，对目标系统实施渗透，意图找到“非法”进入目标系统并取得相关权限的途径，从而测试目标系统安全控制措施的有效性。

6.7 信息安全监控

信息安全监控主要是通过监控工具或平台，对信息系统的环境、网络、主机、系统和应用等进行实时监控，查看各个系统组件的功能、性能、运行状况等，检查设备、系统和应用的日志，一旦发现异常情况，可以采取措施解决，或者启动应急响应等服务。信息安全监控还可以包含对信息安全事件的预警功能。

信息安全监控一般可以分为现场监控和远程监控两种方式。现场监控是由服务提供方的驻场人员为组织承担系统维护和管理的任务，对组织的信息系统实施监控。远程监控是由服务提供方在远程的安全运行中心(SOC)中进行，一般需要有加密的网络连接，并在组织的信息系统上安装一些监控软件。

6.8 信息安全应急处理

信息安全应急处理主要是根据组织信息安全应急管理体系，针对各类突发信息安全事件，提供实施层面的应急响应和应急演练。应急响应是对已发生的各类信息安全事件作出快速响应，及时而有效进行事件处理，最大程度上减少损失和该事件造成的消极影响，响应的方式可以按事件特点和级别分为现场和远程两种。应急演练是根据组织已有的应急预案，在设备、系统、业务、组织等不同层面进行测试和演练，从而提高组织的应对各类突发信息安全事件的能力，演练的方式可分为桌面演练、模拟演练和实战演练。

6.9 信息安全通告

信息安全通告主要是在通告服务提供方与服务需求方之间，建立一种紧密的信息发布和沟通渠道，以便最新的信息安全信息能够被组织或个人获知，并及时采取控制措施来预防自身信息安全事件的发生。信息安全通告的服务提供方可以是权威专业组织、IT 产品厂商或信息安全厂商等。安全通告服务的内容主要包括：漏洞信息、威胁信息、病毒信息、预警消息、重大事件和问题通告等，以及相应的解决方案。

6.10 备份和恢复

备份和恢复是为了防止信息系统及其应用和数据等，因信息安全事件或灾难而造成的丢失或损坏。从而在原文中独立出来单独存储的程序或文件副本，并在系统出现故障或瘫痪时，能够及时恢复系统及其应用和数据，将信息系统从故障或瘫痪状态恢复到可正常运行状态、并将其支持的业务功能从不正常状态恢复到可接受状态。备份和恢复还包括对备份介质和链路的定期测试、恢复的定期演练。

6.11 数据修复

数据修复服务主要指对由有害程序、系统故障、误操作、升级或安装软件错误、人为故意破坏等安全事件造成的逻辑损坏或数据丢失，或由电击、水淹、火烧、震荡、撞击、机械故障等意外事故造成物理损坏或数据丢失，而进行数据抢救和修复的专业服务。

6.12 电子认证服务

电子认证服务主要指为电子签名的真实性和可靠性提供证明的活动，包括签名人身份的真实性认证，电子签名过程的可靠性认证和数据电文的完整性认证三个部分，涉及数据电文的生成、传递、接收、保存、提取、鉴定各环节，涵盖电子认证专有设备提供、基础设施运营、技术产品研发、系统检测评估、专业队伍建设等各方面的专业服务。

6.13 信息安全监理

信息安全监理主要是指信息安全工程监理，即具有相关资质的监理单位受信息安全工程建设单位的委托，依据国家批准的信息化工程项目建设文件、有关工程建设的法律法规和工程建设监理合同及其他工程建设合同，尤其是依据信息安全方面的标准和要求，在工程建设各阶段向建设单位提供相关咨询，并协助建设单位对承建单位在工程建设中的信息安全实施服务，实施控制和管理的一种专业化服务活动。信息安全监理还可以包括对信息系统运维阶段的其他信息安全实施服务进行监理。

6.14 信息安全审计

信息安全审计主要是针对与信息安全有关的活动，从外部独立进行相关信息的识别、记录、存储和分析，确保各项活动符合组织已建立的安全策略和操作过程，并评估它们的有效性和准确性，发现安全违规，掌握安全状态，提出改进建议。信息安全审计的具体对象是在组织的信息安全层面上，技术和管理、物理和逻辑等方面的控制措施，包括对数据中心物理安全、信息系统脆弱性、应用系统安全、数据库逻辑安全，以及组织的信息安全合规性等进行审核。

7 信息安全培训服务

信息安全培训服务的服务界面为：

a） 服务对象

面向信息安全相关人员。

b） 服务供需

服务提供方提供信息安全意识、技术、管理、体系、工程、法律、政策和标准等方面的培训内容，以满足提高信息安全意识、完善信息安全知识、掌握信息安全技能的需求，从而提高相关人员的信息安全能力水平。

c） 服务特征

基于培训目的，结合培训规模、人员基础知识、培训时间、培训条件等情况，对培训内容、培训方式、

考核方式等作出针对性的培训计划，并通过授课、实操、考核等方式予以实施。

d） 服务质量

取决于培训的针对性、科学性和实效性。对面向组织的统一培训，培训服务提供方可在培训结束后，提供培训效果分析报告，以便组织掌握培训情况并对培训工作持续改进。

e） 服务组件

包括：针对信息安全专业人员的资质培训、针对服务需求方特定要求的定制培训等。

8 信息安全服务特点

本标准涉及的信息安全服务除了信息技术服务所具有的共同特点之外，还具有如下特点：

——不依附于某一单独的、具体的、批量生产的信息安全产品；

——就某项具体的服务而言，信息安全服务提供方只能以乙方或第三方的一种角色出现；

——针对不同的信息安全保障需求，信息安全服务提供方可提供不同服务内容的组合；

——信息安全服务的形式可以分为现场服务、远程联机服务、远程非联机服务等；

——信息安全服务提供方应保证其服务人员、过程和工具的可信和可控；

——信息安全服务需求方的信息安全责任部门（或个人自身）应承担对服务的采购、管理等责任；

——信息安全服务提供方应符合国家信息安全基本政策的相关规定（如等级保护），并接受国家信息安全管理部门的行业管理。

附 录 A
（规范性附录）
信息安全服务的采购

A.1 信息安全服务采购要素

A.1.1 采购时机

信息安全工作是组织信息化工作的重要组成部分，贯穿组织信息系统整个生命周期，因此在整个信息系统的生命周期中，组织都会根据信息安全保障需求采购信息安全服务，参见附录 B。

根据业界实践，在信息系统规划、设计和运行阶段，采购咨询类服务较多；在信息系统建设、运行阶段，采购实施类服务较多；在每个阶段都有可能采购信息安全风险评估和信息安全培训服务。

A.1.2 采购目录

由于信息安全服务对服务质量、服务可信和服务可控的高要求，预算和采购政策的管理部门，需及时制定并发布相关的信息安全服务采购目录（采购目录的服务分类可按照本标准执行），以便于组织正确采购相关的服务。

A.1.3 服务资质

信息安全服务资质是服务提供方服务能力的一种体现形式。对同一类服务的不同服务商，如果分别拥有不同能力级别的服务资质，则会在服务质量和服务成本上有所差异。服务需求方可根据自身的信息安全需求，结合信息安全管理部门的相关要求，确定服务提供方的资质准入或认证要求。

A.1.4 服务价格

可以根据组织级别规模、信息系统规模、信息安全保护级别，信息安全保障需求和现有水平，根据不同信息安全服务的服务界面和服务特点，综合采用定额法和比率法，分别确定面向组织和面向信息系统的信息安全服务价格（结合计价单位，确定基准价格和浮动因素）。

A.1.5 招投标规范

采购部门可根据本标准的分类，针对不同服务类别，制定相关的采购招投标规范，至少对如下内容作出规定：

a） 服务资质（准入资质）的要求；
b） 服务级别协议的承诺形式和度量方法；
c） 服务的质量要求；
d） 服务的保障措施（人员、过程、工具、资源等）；
e） 服务自身的安全要求；
f） 服务项目评标规则。

A.1.6 服务协议（采购合同）

信息安全服务的服务协议至少包括：

a） 服务原则：对服务提供方的原则性要求；

b） 服务内容：服务提供方提供的服务组件，可参照本标准二级分类；

c） 服务形式：服务提供方所提供服务的方式，如：现场、远程等；

d） 服务级别协议：评价服务效果关键指标；

e） 服务价格：服务提供方所提供服务的价格，含总价和分项计算依据等；

f） 服务交付物：服务过程中、服务结束后，服务提供方需要提供的文档、记录、数据、成果等；

g） 服务安全要求：对服务人员、服务过程、服务工具、服务数据保护等作出明确要求。

A.2 信息安全服务实例

作为最常见的信息安全服务采购，信息安全服务实例是由信息安全服务类别及其服务组件所构成的，典型的信息安全服务实例与其可能包含的服务组件之间的关系如表 A.1 所示。

表 A.1 典型的信息安全服务实例

服务实例	对应的服务组件（代码）
安全咨询	A02、C01
风险评估	A03
安全集成	B01、B02、B03、B04、B05、B09
安全运维	B04、B05、B06、B07、B08、B09
应急处理	A04、B07、C01
灾难恢复	A05、B09、C01
安全培训	C01
安全测评	B05
安全监理	B12
安全审计	B13

服务提供方会根据服务需求方的信息化现状和信息安全保障需求、结合自身的服务能力和服务特点，对服务组件进行组合（即形成各个服务提供方的信息安全服务实例），供需求方采购，最常见的组合方式是“安全集成”和“安全运维”。

安全集成是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。典型的安全集成包括：

a） 信息安全设计；

b） 信息安全产品部署；

c） 信息安全检查和测试。

安全运维是为满足信息系统运行的安全需求，综合采用检查、测试、监控、应急等手段，维持信息系统安全保障水平的行为或活动。典型的安全运维包括：

a） 信息安全检查和测试；

b） 信息安全监控；

c） 信息安全应急处理。

有时在安全集成和安全运维服务过程中，还会涉及一些咨询类服务和第三方角色的服务。但由于这些服务与乙方角色的实施类服务的服务界面不同，服务需求方需尽可能将其分开采购，才可保证相关的服务质量。

附 录 B
（资料性附录）
信息安全服务与信息系统生命周期的对应关系

信息安全服务与信息系统生命周期(参照 GB/T 25058—2010)的对应关系见表 B.1。

表 B.1 信息安全服务与信息系统生命周期的对应关系

信息安全服务		信息系统生命周期			
服务类别	服务组件	规划	设计	建设	运行
信息安全咨询服务	信息安全规划	√			
	信息安全管理体系咨询	√			√
	信息安全风险评估	√	√	√	√
	信息安全应急管理咨询	√			√
	业务连续性管理咨询	√			√
信息安全实施服务	信息安全设计		√		
	信息安全产品部署			√	√
	信息安全开发			√	√
	信息安全加固和优化			√	√
	信息安全检查和测试			√	√
	信息安全监控				√
	信息安全应急处理				√
	信息安全通告				√
	备份和恢复			√	√
	数据修复				√
	电子认证服务			√	√
	信息安全监理			√	√
	信息安全审计				√
信息安全培训服务	信息安全培训	√	√	√	√

注：本标准在服务类别中统一采用信息安全实施服务，而不直接使用“安全集成服务”“安全运维服务”等服务实例名称，原因是安全集成服务、安全运维服务的服务内容在不同的服务场景下差异较大。例如，安全集成服务可能包含信息安全设计、信息安全产品部署、信息安全开发等多项信息安全实施服务，也可能只包含信息安全产品部署；安全运维服务可能包含信息安全检查和测试、信息安全监控、信息安全应急处理等多项信息安全实施服务，也可能只包含信息安全应急处理服务。

参 考 文 献

[1] GB/T 18336—2008 信息技术 安全技术 信息技术安全性评估准则

[2] ISO/IEC TR 15443-1:2005 信息技术 安全技术 信息技术安全保障框架 第1部分:总揽和框架

[3] NIST SP800-35 信息技术安全服务指南

[4] CMU/SEI OMSS 可管理安全服务外包

[5] CMU/SEI SSE-CMM 系统安全工程能力成熟度模型

中 华 人 民 共 和 国
国 家 标 准
信息安全技术
信息安全服务 分类
GB/T 30283—2013
*
中 国 标 准 出 版 社 出 版 发 行
北京市朝阳区和平里西街甲 2 号(100029)
北京市西城区三里河北街 16 号(100045)
网址:www.gb168.cn
服务热线:400-168-0010
010-68522006
2014 年 5 月第一版
*
书号:155066·1-48878

GB/T 30283-2013