ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 30283—2022
代替 GB/T 30283—2013

信息安全技术　信息安全服务 分类与代码

Information security technology—Information security service—Classification and code

2022-04-15 发布　　2022-11-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本文件按照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》的规定起草。

本文件代替GB/T 30283—2013《信息安全技术　信息安全服务　分类》，与GB/T 30283—2013相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 更改了若干信息安全服务类别、代码、名称及内容（见第6章、第7章、第8章、第9章、第10章、第11章、第12章、第13章，2013年版的第4章、第5章、第6章、第7章）；

b) 增加了信息安全设计与开发服务、信息安全集成服务、信息安全运营服务、信息的安全处理和存储服务、信息安全测评与认证服务类别（见第8章、第9章、第10章、第11章、第12章）；

c) 删除了信息安全实施服务、信息安全培训服务（见2013年版的第6章、第7章）；

d) 更改了要素“规范性引用文件”（见第2章，2013年版的第2章）；

e) 增加了术语和定义，新增、改写和引用部分术语和定义（见第3章，2013年版的第3章）；

f) 增加了缩略语，对本文件涉及的缩略语进行解释说明（见第4章）；

g) 更改了要素“信息安全服务特点”的编写，对部分内容进行了调整（见第5章，2013年版的第8章）；

h) 更改了要素“信息安全服务分类”的编写，调整了服务分类的层次结构和编码方法（见第6章，2013年版的第4章）；

i) 增加了“其他信息安全服务”章节，说明其他信息安全服务的扩展原则和类型（见第13章）。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国信息安全标准化技术委员会（SAC/TC 260）提出并归口。

本文件起草单位：中国电子科技网络信息安全有限公司、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、中电长城网际系统应用有限公司、中国信息安全测评中心、中国网络安全审查技术与认证中心、公安部第三研究所、国家计算机网络应急技术处理协调中心、毕马威企业咨询（中国）有限公司、安天科技集团股份有限公司、北京天融信网络安全技术有限公司、中国科学院信息工程研究所（信息安全国家重点实验室）、陕西省网络与信息安全测评中心、北京东方通网信科技有限公司、陕西省信息化工程研究院、国网区块链科技（北京）有限公司、山谷网安科技股份有限公司、北京北信源软件股份有限公司、烽台科技（北京）有限公司、成都卫士通信息安全技术有限公司、工业互联网创新中心（上海）有限公司、北京知道创宇信息技术股份有限公司、北京红戎信安技术有限公司、网神信息技术（北京）股份有限公司、远江盛邦（北京）网络安全科技股份有限公司、北京奇虎科技有限公司、西安西电捷通无线网络通信股份有限公司、北京百度网讯科技有限公司。

本文件主要起草人：张焱、刘慧晶、干露、杨建军、闵京华、王惠莅、孙明亮、翟亚红、陈晓桦、陈长松、张剑、李斌、邬敏华、张静、王媛、陈亮、王伟、李柏松、赵焕菊、陈驰、马红霞、白峻、王龑、崔婷婷、杨向东、张屹、陈洪波、潘正泰、李丹、杨珂、王栋、左洪强、李洪典、龚亮华、李瑞、张晓菲、王朝栋、徐春蕾、何志明、杜志强、訾立强、张雪帆、唐佳伟、王晶、权晓文、刘大海、杨德川、王庆磊、陈乔、刘阳、高强、徐峰。

本文件及其所代替文件的历次版本发布情况为：

——2013年首次发布为GB/T 30283—2013；

——本次为第一次修订。

信息安全技术　信息安全服务分类与代码

1　范围

本文件描述了信息安全服务的分类与代码，主要包括信息安全咨询类、信息安全设计与开发类、信息安全集成类、信息安全运营类、信息的安全处理和存储类、信息安全测评与认证类及其他类七个方面。

本文件适用于信息安全服务提供方和信息安全服务需求方使用，也可供其他相关方参考。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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　信息安全技术　术语

GB/T 32914—2016　信息安全技术　信息安全服务提供方管理要求

GB/T 38674—2020　信息安全技术　应用软件安全编程指南

3　术语和定义

GB/T 25069、GB/T 32914—2016 和 GB/T 38674—2020 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，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或机构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。

[来源：GB/T 32914—2016，3.1，有修改]

3.2

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

需方

获取外部所提供的信息安全服务，以满足信息安全需求，实现自身业务目标的组织。

[来源：GB/T 32914—2016，3.2，有修改]

3.3

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

供方

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。

[来源：GB/T 32914—2016，3.3]

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、服务级别协议、服务价格、服务交付物、服务安全要求等，在形式上是服务合同及其附属的工作说明书。

[来源：GB/T 32914—2016，3.4]

3.5

服务分类　service classification

根据信息安全服务的属性或特征将其进行区分和归类的过程。

3.6

服务实例　service instance

为满足某一确定的信息安全需求而组合在一起的，一组可重用的信息安全服务。

3.7

信息安全咨询服务　information security consulting service

面向组织或个人，围绕组织信息系统所支持业务相关人员、技术和管理，通过知识传递、工作辅导和系统规划等方法和资源提出解决信息安全问题的建议和方案等形式提供的信息安全服务。

3.8

信息安全设计与开发服务　information security design and development service

面向组织或个人，围绕信息安全开发需求，通过需求分析、安全设计、安全开发、安全测试等过程向需方提供，并协助其实施控制和管理的信息安全服务。

3.9

信息安全集成服务　information security integration service

面向组织或个人，围绕信息安全建设需求，通过结构化的综合布缆系统、计算机网络技术和软件技术，将各个分离的设备、功能和信息等集成到相互关联的、统一和协调的系统之中，以及为信息系统的正常运行而提供的信息安全服务。

3.10

信息安全运营服务　information security operation service

面向组织或个人，围绕实现组织的业务持续、稳定运行的安全目标，通过提出安全解决构想、分析问题、诊断问题、协调资源、解决问题、验证效果并持续迭代优化的统筹管理过程，满足组织信息安全的动态性、持续性和整体性需求的信息安全服务。

3.11

信息的安全处理和存储服务　information securityprocessing and storage service

面向组织，围绕信息和数据的分析、整理、计算、编辑、存储等加工处理业务，以及应用软件、信息系统基础设施等租用业务的信息安全需求而提供的信息安全服务。

3.12

信息安全测评与认证服务　information security evaluation and certification service

面向组织或个人，由信息安全测评与认证机构围绕产品、系统、服务、人员、管理体系证明其符合相关技术规范、相关技术规范的强制性要求或者标准合格评定活动而提供的信息安全服务。

4　缩略语

下列缩略语适用于本文件。

AI：人工智能（Artificial Intelligence）
APT：高级持续性威胁（Advanced Persistent Threat）
APP：应用软件（Application Software）
CDN：内容分发网络（Content Delivery Network）
IT：信息技术（Information Technology）

5 信息安全服务特点

本文件所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：

a） 不依附于某一单独的、具体的、批量生产的信息安全产品；
b） 针对不同的信息安全需求，供方提供不同服务内容的组合；
c） 信息安全服务具有敏感的动态性要求和突出的个性化要求；
d） 信息安全服务的形式多样，分为现场服务、远程联机服务、远程非联机服务等；
e） 供方的服务人员、过程和工具保证可信和可控；
f） 供方符合国家和行业相关信息安全标准的要求。

6 信息安全服务分类与代码

6.1 编码方法

本文件采用“服务大类—服务中类—服务小类”层次结构来描述服务分类，从左到右：

a） 服务大类由1位大写英文字母表示，信息安全咨询服务、信息安全设计与开发服务、信息安全集成服务、信息安全运营服务、信息的安全处理和存储服务、信息安全测评与认证服务、其他信息安全服务分别用A、B、C、D、E、F、Z表示；
b） 服务中类由1位大写英文字母和2位阿拉伯数字表示，第1位是大类代码，后两位是中类顺序代码，如“A01”表示信息安全规划咨询，数字为“99”表示收容类目，如“A99”表示其他信息安全咨询服务；
c） 服务小类由1位大写英文字母和4位阿拉伯数字表示，前三位为中类代码，后两位为小类顺序代码，如“A0601”表示信息安全意识培训，后两位数字为“99”表示收容类目，如“A0699”表示其他信息安全培训服务。

信息安全服务的分类代码结构见图1。

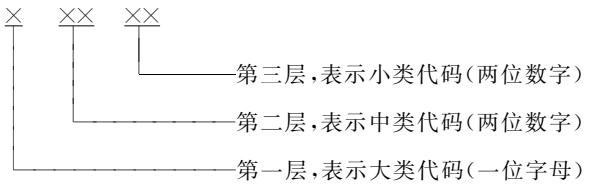

图1 信息安全服务的分类代码结构

6.2 分类与代码

信息安全服务分类与代码见表1。

表 1　信息安全服务分类与代码

代码	类别名称	目标对象
A	信息安全咨询服务	需方的信息系统及其所支持的业务和管理
A01	信息安全规划咨询	
A02	信息安全设计咨询	
A03	信息安全管理体系咨询	
A04	信息安全工程监理	
A05	信息安全测试评估	
A0501	信息安全测试	
A0502	信息安全风险评估	
A0599	其他信息安全测试评估服务	
A06	信息安全培训	
A0601	信息安全意识培训	
A0602	信息安全基础培训	
A0603	信息安全专业培训	
A0699	其他信息安全培训服务	
A99	其他信息安全咨询服务	
B	信息安全设计与开发服务	需方的业务和安全需求
B01	信息安全系统设计	
B02	信息安全开发	
B99	其他信息安全设计与开发服务	
C	信息安全集成服务	需方的信息安全系统及软硬件基础设施
C01	信息安全硬件集成	
C02	信息安全软件集成	
C99	其他信息安全集成服务	
D	信息安全运营服务	需方的信息系统及其所支持的业务和管理
D01	信息安全监测	
D02	信息安全检查	
D03	威胁信息共享	
D04	信息安全分析	
D05	信息安全报送	
D06	恶意代码防范和处理	
D07	信息安全应急响应	
D08	信息安全演练	
D09	信息安全调查取证	
D10	信息安全加固	

表 1　信息安全服务分类与代码（续）

代码	类别名称	目标对象
D11	信息安全运维规范管理	需方的信息系统及其所支持的业务和管理
D12	信息安全审计	
D13	身份管理	
D14	备份和恢复	
D99	其他信息安全运营服务	
E	信息的安全处理和存储服务	信息系统及设备所涉及的安全信息和数据
E01	数据安全保护	
E02	信息安全租赁	
E03	网络信息内容审核	
E99	其他信息的安全处理和存储服务	
F	信息安全测评与认证服务	需方的信息安全系统、服务资质、管理体系、人员等
F01	信息安全测评	
F0101	信息安全产品测评	
F0102	信息安全服务资质测评	
F0103	信息安全人员测评	
F0104	等级保护测评	
F0105	分级保护测评	
F0106	密码测评	
F0199	其他信息安全测评服务	
F02	信息安全认证	
F0201	信息安全产品认证	
F0202	信息安全管理体系认证	
F0203	信息安全服务资质认证	
F0204	信息安全人员认证	
F0299	其他信息安全认证服务	
F99	其他信息安全测评与认证服务	
Z	其他信息安全服务	

基于如上分类，需方根据自身的信息化现状和信息安全需求，对服务中类或小类进行组合，形成信息安全服务实例。因此，信息安全服务可以服务实例的形式，由一个或多个服务中类或者服务小类构成，某些还可能包含本文件不涉及的其他扩展的服务。通常信息安全服务实例有以下几种类型：安全咨询、风险评估、安全集成、安全运维、应急响应、灾难恢复、安全培训、安全测评、安全监理、安全审计、安全运营。信息安全服务分类新旧结构对照见附录 A，信息安全服务分类新旧类目对照见附录 B，典型的信息安全服务实例及其对应服务类别见附录 C。

信息安全服务贯穿信息系统的规划、设计、实施、运行、终止等阶段，信息安全服务与信息系统生命周期的对应关系见附录 D。

信息安全服务分类的其他形式与本文件的服务类别的对应关系见附录 E。

7 信息安全咨询服务

7.1 信息安全规划咨询

信息安全规划咨询主要是针对需方信息系统及其支持的业务和管理的安全需求，由供方结合需方投资预算、信息安全现状以及发展趋势，基于人员利用资源、技术，通过规定的过程提出需方安全规划目标，从管理、技术两个维度设计规划内容以形成一套指导性文件，系统指导需方信息安全建设，满足其可持续发展的需要。信息安全规划咨询通常涉及多学科知识、工程实践经验、现代科学和管理技术，为信息安全资源开发利用、工程建设、人员培训、管理体系建设、技术支撑等方面提供支持。

任何提供的主要服务内容与以上描述相符的服务，均可归入本类。

7.2 信息安全设计咨询

信息安全设计咨询主要是针对信息系统的安全防护需求，由供方落实需方的安全规划，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策略、安全技术体系结构、安全管理体系结构等的设计，指导需方信息安全防护具体实现。信息安全设计一般可分为顶层设计、概要设计和详细设计等不同的服务交付物。

任何提供的主要服务内容与以上描述相符的服务，均可归入本类。

7.3 信息安全管理体系咨询

信息安全管理体系咨询主要是针对需方信息安全管理体系需求，由供方结合需方的需要和目标、安全要求、所采用的过程、规模和结构，通过确定信息安全管理体系范围和方针、明确责任、权限和角色，采用风险评估的方法规划管理体系建设任务并落实，实施内部审核与管理评审等过程，协助需方建立、实现、维护、并持续改进信息安全管理体系。信息安全管理体系是组织的过程和整体管理结构的一部分并集成在其中，涵盖相关标准要求的文件化信息，应阐述被保护的资产、风险管理的方法、控制目标及控制方式和需要的保证程度。

任何提供的主要服务内容与以上描述相符的服务，均可归入本类。

7.4 信息安全工程监理

信息安全工程监理主要是针对需方各类信息系统工程中涉及信息安全的工程活动，由具有相关资质的监理单位(供方)根据需方委托，在工程建设的规划设计、部署实施(招标、设计、实施、验收)各阶段实施控制和管理，提供相关建议和意见，确保实现各阶段的监理目标和完成监理内容。信息安全工程监理还可以包括对信息系统运行维护阶段的信息安全服务进行监理。

任何提供的主要服务内容与以上描述相符的服务，均可归入本类。

7.5 信息安全测试评估

7.5.1 信息安全测试

信息安全测试主要是针对信息系统、软硬件产品等被测对象的安全属性，由供方在特定的测试环境下，根据需方授权，按照测试准备、测试实施、测试分析、测试结果反馈等工作流程，选择适用的方法/工具，动态分析测试数据，发现被测对象存在的安全隐患，验证被测对象安全保障措施的符合性及有效性，提出安全整改建议。信息安全测试通常包括信息系统安全测试、APP 安全测试、漏洞安全扫描、基线配置核查、渗透测试、源代码审计等。信息安全测试工具应符合相关国家标准要求，确保可靠性和安全性。

任何提供的主要服务内容与以上描述相符的服务，均可归入本类。

7.5.2 信息安全风险评估

信息安全风险评估主要是针对业务、信息系统、基础网络和平台、数据资源等被评估对象，由供方确定风险评估的工作形式，按照风险评估流程，覆盖风险评估准备、资产识别、威胁识别、脆弱性识别、已有安全措施确认、风险分析、风险处理等环节，对所面临的风险进行识别、分析和评价，制定和提出抵御风险的安全策略和整改措施。信息安全风险评估通常贯穿被评估对象的规划、设计、实施、运行、废弃各生命周期阶段。

7.5.3 其他信息安全测试评估服务

不属于以上服务小类的其他信息安全测试评估服务。

7.6 信息安全培训

7.6.1 信息安全意识培训

信息安全意识培训主要是针对需方的全体人员，结合组织的信息安全管理制度，采用宣传资料（如简报、短片等）、宣传周、网络媒介等多种方式，传递有关信息安全方面的基本常识，并对培训效果进行评价，确保培训人员树立信息安全观念，提高信息安全风险意识，增强信息安全责任感。信息安全意识培训通常提供的是一种较为初级的培训服务。

任何提供的主要服务内容与以上描述相符的服务，均可归入本类。

7.6.2 信息安全基础培训

信息安全基础培训主要是针对需方与信息系统设计、开发、实现和运维等相关的技术人员和管理人员，采取案例教学、课堂讲授等方式，传授有关信息安全的基础知识，并对培训效果进行评价，确保培训对象掌握与自身工作相关的信息安全理论知识和基本技能，履行信息安全职责。信息安全基础培训通常提供的是一种基于角色和职责的定制服务。

任何提供的主要服务内容与以上描述相符的服务，均可归入本类。

7.6.3 信息安全专业培训

信息安全专业培训主要是针对需方的信息安全专业人员、专职人员和高级管理人员，根据信息安全人才培养计划，采取在职培训、岗位培训、技能考核、多学科专题研讨等方式，传授有关信息安全的专业知识，并对培训效果进行评价，确保培训对象全面了解信息安全知识体系，掌握信息安全专业知识和专业技能，提高信息安全专业素养。

任何提供的主要服务内容与以上描述相符的服务，均可归入本类。

7.6.4 其他信息安全培训服务

不属于以上服务小类的其他信息安全培训服务。

7.7 其他信息安全咨询服务

不属于以上服务中类的其他信息安全咨询服务。

8 信息安全设计与开发服务

8.1 信息安全系统设计

信息安全系统设计主要是针对需方不能通过采购现有信息安全系统或产品予以满足的安全需求，

由供方按照需求分析、概要设计、详细设计等流程设计信息安全系统，可按照 GB/T 38674—2020 提出的应用软件安全编程的通用框架的要求，并结合需方应用环境的特性，提出安全防护设计要求，以指导后续的信息安全开发(见 8.2)。信息安全系统设计一般包括安全实现技术框架设计、安全功能设计、性能要求设计等。

任何提供的主要服务内容与以上描述相符的服务，均可归入本类。

8.2 信息安全开发

信息安全开发主要针对需方不能通过采购现有信息安全系统或产品予以满足的安全需求，由供方在信息安全系统设计(见 8.1)的基础上，按照安全要求确认、安全基线要求确定、设计要求确认、安全策略制定、威胁建模、安全编码规范设计、事件响应计划制定、最终安全评析等软件安全开发流程开发信息安全系统或产品，并可按照 GB/T 38674—2020 提出的应用软件安全编程通用框架的要求，采取相应的措施保障信息安全系统或产品的安全性，以满足需方特定的安全需求并最大程度地减少信息安全系统或产品的安全缺陷。信息安全开发也可以基于已有的信息安全系统或产品进行二次开发。

任何提供的主要服务内容与以上描述相符的服务，均可归入本类。

8.3 其他信息安全设计与开发服务

不属于以上服务中类的其他信息安全设计与开发服务。

9 信息安全集成服务

9.1 信息安全硬件集成

信息安全硬件集成主要是针对需方采购或租赁的信息安全硬件设备，由供方根据已制定的系统集成方案(包含设计方案和实施方案等)，明确集成部署方式，按照部署环境搭建、安装配置、功能调试、性能测试等工作流程规范开展集成部署工作，确保各个子系统实现安全互联互通。信息安全硬件集成通常覆盖信息安全需求分析、规划设计、设备采购、集成部署、交付验收等过程，其中，集成部署环境一般有以下几种：部署在需方本地机房，部署在托管数据中心，部署在云平台的虚拟资源上，或者以前面几种形式混合部署等。

任何提供的主要服务内容与以上描述相符的服务，均可归入本类。

9.2 信息安全软件集成

信息安全软件集成主要是针对需方采购或租赁的信息安全软件、系统(包括软件构件)，由供方根据已制定的软件集成方案(包含设计方案和实施方案等)，明确部署安装方式，按照部署环境搭建、软件集成实施(包括现场系统开发)、现场部署、评测改进等工作流程规范开展集成部署工作，确保信息安全软件、系统实现安全、高效应用。信息安全软件集成通常覆盖信息安全需求分析、设计、实施与运行、测试与改进和验收等过程。

任何提供的主要服务内容与以上描述相符的服务，均可归入本类。

9.3 其他信息安全集成服务

不属于以上服务中类的其他信息安全集成服务。

10 信息安全运营服务

10.1 信息安全监测

信息安全监测主要是针对信息系统的环境、网络、设备、系统、应用、不同区域间流动信息等被监测

对象，由供方采用监测类工具、平台或感知节点设备现场或远程对被监测对象的信息安全事件、运行状态、脆弱性与威胁进行监测和感知，以及时发现威胁、告警、事件等异常情况或行为。信息安全监测可与信息安全报送（见 10.5）、应急响应（见 10.7）和调查取证（见 10.9）协同实施。信息安全监测通常还应实现或完善对新型网络攻击行为（如 APT 攻击）的监测。

任何提供的主要服务内容与以上描述相符的服务，均可归入本类。

10.2 信息安全检查

信息安全检查主要是针对需方的信息安全自检查需求，由供方根据需方委托，结合检查对象安全特性，明确具体的检查依据、范围、对象和内容，按照检查准备、检查实施、检查结果分析、检查报告编制、检查结果反馈等工作流程，通过人员访谈、文档查阅、技术验证、测试等手段，以协助需方发现可能存在的信息安全问题。信息安全检查通常与信息安全测试评估（见 7.5）和信息安全监测（见 10.1）协同实施，并确保不引入额外的风险。

任何提供的主要服务内容与以上描述相符的服务，均可归入本类。

注 1：信息安全检查分为监督检查、自检查和委托检查。监督检查是指上级管理部门组织的或国家有关职能部门依法开展的检查。自检查是指信息系统所有者、运营或使用单位发起的对本单位信息安全状况进行的检查。委托检查是指受检单位或监督检查的组织部门不具备检查能力的，委托经相关主管部门认可的机构开展的检查。

注 2：本服务中的信息安全检查主要适用于由供方协助需方开展的信息安全自检查场景。

10.3 威胁信息共享

威胁信息共享主要是针对需要和使用网络安全威胁信息的需方，由供方采用多种技术手段，通过采集大规模、多渠道的网络安全威胁数据，集中进行深度融合、归并和分析，形成网络安全威胁信息，经人工或自动化处理为结构化信息，采用通用模型来实现对网络安全威胁信息的统一描述，批量传递给需方，以实现跨组织的海量网络安全威胁信息的快速传递，进而支持对复杂网络安全威胁的应对。网络安全威胁信息的描述通常由可观测数据、攻击指标、安全事件、攻击活动、威胁主体、攻击目标、攻击方法和应对措施等要素组成。

任何提供的主要服务内容与以上描述相符的服务，均可归入本类。

10.4 信息安全分析

信息安全分析主要是针对需方的信息系统，由供方采集并处理日志、流量、性能、漏洞等多类数据，采用多类专业智能化分析引擎、AI 检测模型和信息资源库，识别网络攻击、恶意软件、信息泄露等安全威胁，并提出建议采取的解决方案或措施。信息安全分析可与信息安全报送（见 10.5）、应急响应（见 10.7）和调查取证（见 10.9）协同实施。信息安全分析通常采用大数据技术以实现对海量数据的快速、高效、及时的分析与计算。信息安全分析包括现场分析和远程分析两种方式。其中，远程分析通常由供方在远程的安全运行或运营中心进行，一般应有加密的网络连接，并在需方的信息系统上安装数据采集软件或工具。

任何提供的主要服务内容与以上描述相符的服务，均可归入本类。

10.5 信息安全报送

信息安全报送主要是针对需要及时掌握信息安全事件或威胁信息的需方，由供方协助建立信息报送的工作机制，明确信息报送范围、渠道及信息格式，在即将发生或正在发生信息安全事件或威胁时，提前或及时报送需方，以便需方及时采取措施。信息安全报送内容通常包括信息安全事件或威胁的发生时间、基本情况描述、可能产生的危害及程度、可能影响的用户及范围、宜采取的应对措施等。

任何提供的主要服务内容与以上描述相符的服务，均可归入本类。

10.6 恶意代码防范和处理

恶意代码防范和处理主要针对危害需方信息资产的人为故意编制或设置的代码或数据，由供方协助建立和实施恶意代码防范机制，安装防恶意代码软件或配置具有相应功能的软件，实时监测并定期扫描，对恶意代码采取阻断、清除、分析、报警及其他遏制措施，恢复受影响的功能和数据，并定期升级和更新防恶意代码库，以增强需方对恶意代码事件的防范和处理能力。恶意代码防范和处理通常与信息安全监测（见 10.1）、分析（见 10.4）和应急响应（见 10.7）协同实施。

任何提供的主要服务内容与以上描述相符的服务，均可归入本类。

10.7 信息安全应急响应

信息安全应急响应主要是针对影响网络与信息系统安全的各类各级信息安全事件，由供方结合需方的信息安全应急管理体系，快速进行标识、记录、分类和处理，最大程度上减少损失和降低该事件造成的消极影响。在实践中，通常会采取编写应急预案制定应急计划，指导需方开展应急演练等方式提高应急能力，以在信息安全事件发生后能够及时、有效地实施应急响应。

任何提供的主要服务内容与以上描述相符的服务，均可归入本类。

10.8 信息安全演练

信息安全演练主要是针对有信息安全演练需求的需方，由供方协助明确演练的组织架构，编制演练规划，包括演练频次、规模、形式、时间、地点、预算等，制定演练的工作方案、保障方案、评估方案等，按照演练规划和方案执行安全演练（必要时可安排一次或多次预演），监视、评价安全演练过程，并就演练过程中存在的问题、取得的经验教训等加以改进，使安全演练符合预期设定目标，确保演练规划得到有效执行。信息安全演练根据组织形式、内容、目的和作用的不同，通常体现不同的演练形式。如根据组织形式，可分为桌面推演、模拟演练、实操演练；根据演练内容，可分为专项演练、综合演练；根据演练目的和作用，可分为检验性演练、示范性演练和研究性演练。

任何提供的主要服务内容与以上描述相符的服务，均可归入本类。

10.9 信息安全调查取证

信息安全调查取证主要是针对信息安全相关的网络违法犯罪活动，由供方根据需方委托，使用符合相关技术标准和规范的取证设备和方法，通过技术手段收集、保全和记录电子证据，形成证据链以支持信息安全调查、分析、识别等工作。信息安全调查取证过程通常包括确定调查依据，制定调查取证实施步骤，获取和保存电子证据，分析和验证证据链以及编写调查取证报告等。

任何提供的主要服务内容与以上描述相符的服务，均可归入本类。

10.10 信息安全加固

信息安全加固主要是针对需方的网络设备、操作系统、数据库和应用系统等被加固对象，由供方在获得需方允许的前提下，按照已制定的安全加固方案，采取补丁升级、关闭不必要的端口和服务、优化访问控制策略、增加安全机制等措施对被加固对象存在的安全缺陷和漏洞进行弥补和修复，以增强被加固对象的安全性，提高其安全保护能力。信息安全加固通常与信息安全测试评估（见 7.5）、分析（见 10.4）协同实施。

任何提供的主要服务内容与以上描述相符的服务，均可归入本类。

10.11 信息安全运维规范管理

信息安全运维规范管理主要是针对信息安全运维相关的活动，由供方协助需方制定安全运维基线，

采取运维行为审批、运维操作过程记录、运维工具审核及监视、运维人员适度授权等必要手段和措施，规范安全运维活动，以降低可能带来的风险。信息安全运维规范管理通常贯穿安全运维策略、安全运维组织、安全运维支撑体系、安全运维规程各个方面。

任何提供的主要服务内容与以上描述相符的服务，均可归入本类。

10.12 信息安全审计

信息安全审计主要是针对需方的信息安全相关活动，由供方通过文件审核、记录检查、技术测试、现场访谈等手段，获得审计证据，并对其进行客观的评价，形成审计报告，确定被审计对象满足审计依据的程度，帮助需方全面了解和掌握其信息安全工作的有效性、充分性和适宜性。信息安全审计的范围通常包括信息安全管理目标、方针和策略，信息安全管理组织的建立，信息安全管理制度和流程，信息安全信息分类和保护体系，信息安全事件管理，信息安全教育和培训，物理安全，系统开发安全，信息安全，设备安全，操作系统安全，应用系统安全，数据安全，业务连续性管理以及供应商管理等。

任何提供的主要服务内容与以上描述相符的服务，均可归入本类。

10.13 身份管理

身份管理主要针对网络用户、网络设备等各类网络中的实体，由供方通过对网络实体身份的发布和使用涉及的身份标识定义、身份验证与证明、身份鉴别、授权管理，以及涵盖开发与应用、互操作、接口与协议、身份管理框架等在内的集成应用与身份管理等环节进行可信管理，构建网络信任体系的基础，解决其身份管理问题。目前广泛应用的身份管理关键技术包括在线身份管理、多因素身份鉴别等。

任何提供的主要服务内容与以上描述相符的服务，均可归入本类。

10.14 备份和恢复

备份和恢复主要是针对需方的信息系统故障及灾难恢复相关活动，由供方围绕物理环境、网络、设备、工具、组织及人员等方面，确定备份和恢复范围、恢复等级、恢复目标及策略，采取数据备份系统、备用数据处理系统、备用网络系统、灾难恢复服务及工具等手段和措施，将信息系统从灾难造成的故障和瘫痪状态恢复到可正常运行状态。备份和恢复通常贯穿规划设计、建设实施和运行维护管理各个环节。

任何提供的主要服务内容与以上描述相符的服务，均可归入本类。

10.15 其他信息安全运营服务

不属于以上服务中类的其他信息安全运营服务。

11 信息的安全处理和存储服务

11.1 数据安全保护

数据安全保护主要是针对需方生产经营活动中所涉及的业务数据以及其他重要数据、个人信息等，由供方对数据收集、传输、存储、处理、使用以及销毁等数据生命周期中的相关行为以及数据的交易、公开等活动，实施分类分级、标识、风险评估、应急处置、防泄漏、审计、隐藏（如水印、脱敏）、访问控制、加密、备份恢复、数据抢救和修复等一系列的数据安全保护措施，协助需方保证数据的机密性、完整性和可用性并保障数据得到有效保护和合法利用，持续处于安全状态。数据安全保护通常还应与信息安全风险评估（见 7.5.2）协同实施，针对个人信息和重要数据出境情形，按照国家相关要求，协助需方进行安全评估。

任何提供的主要服务内容与以上描述相符的服务，均可归入本类。

11.2 信息安全租赁

信息安全租赁主要是针对需方租赁的信息安全软件、硬件、云安全虚拟资源等，由供方（即出租人），按照租赁申请、受理及调查、审核、合同签订和履行、租后管理等阶段向需方（承租人）提供产品或服务，确保在规定的时间内（通常称之为租期）满足相应的信息安全需求。信息安全租赁通常包括安全设备租赁、安全系统租赁以及安全虚拟资源（池）租赁等。

任何提供的主要服务内容与以上描述相符的服务，均可归入本类。

注：出租人以在法律上拥有租赁设备所有权为前提，在租期内将该项产品的使用权出租给承租人；承租人则对租赁产品在经济上拥有使用权，在租期内有权占有，并正常使用该项租赁产品。租期结束后，由承租人和出租人按照服务合同或协商确定租赁设备的所有权。

11.3 网络信息内容审核

网络信息内容审核主要是针对需方的文本、图像、音频、视频等载体，由供方对其内容中可能包含的淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪、政治敏感、低俗辱骂、恶意推广等违法和不良信息进行检测和识别，并协助需方开展防范和处置工作，以降低内容违规风险。网络信息内容审核对象通常包括视频网站、直播平台、社交平台、媒体平台、垂直社区/论坛、电商网站、存储平台、CDN 平台等。

任何提供的主要服务内容与以上描述相符的服务，均可归入本类。

11.4 其他信息的安全处理和存储服务

不属于以上服务中类的其他信息的安全处理和存储服务。

12 信息安全测评与认证服务

12.1 信息安全测评

12.1.1 信息安全产品测评

信息安全产品测评是针对保障信息安全的软件、硬件、固件或其组合体，由具有国家认可资格的测评机构，依据相关测评标准和相关技术要求，按照一定的测评方法论，对信息安全产品的自主性、安全性和可控性等进行验证、测试和评估，以验证产品是否达到相关要求或存在潜在的安全风险，并出具相应的测试评估报告。信息安全产品测评类型包括但不限于信息安全产品分级测评、自主原创测评、选型对比测评、定制测评等。

任何提供的主要服务内容与以上描述相符的服务，均可归入本类。

12.1.2 信息安全服务资质测评

信息安全服务资质测评主要是针对需方提出的信息安全服务资质测评需求，由具有相关服务资质的测评方（供方）根据需方委托，依据相关标准和技术规范，结合测评对象服务形式的特点，明确具体的测评依据、范围、对象和内容，按照测评准备、测评实施、测评结果分析、测评结果反馈等过程开展信息安全服务能力测评。整个测评工作主要根据需求方的基本资格与基本能力、质量管理与项目管理能力、技术服务过程能力等进行展开，测评结束后，由供方出具相关的测评报告并结合相应级别的测评证书作为最终的测评结果。信息安全服务资质测评工作主要依据国际通用的能力成熟度模型五级架构展开，测评类型包括安全工程、信息安全风险评估、安全开发、灾难恢复、信息系统审计、大数据安全、云计算安全、安全运营等。

任何提供的主要服务内容与以上描述相符的服务，均可归入本类。

12.1.3 信息安全人员测评

信息安全人员测评主要是针对需方(可以是组织或者个人)提出的信息安全人员测评需求,由具有相关服务资质的测评方(供方)根据需方委托,依据相关标准、准则和规定,结合人员测评对象委托测评类型的特点,明确具体的测评依据、范围、对象和内容,按照规定测评工作流程展开人员测评。信息安全人员测评主要对信息安全从业人员的相应能力进行测评,测评通过者发放相应测评资质证书。信息安全人员测评是对信息安全从业人员具备相应专业能力测评的系列活动。信息安全人员测评通常包括注册信息安全工程师、注册信息安全管理员、注册信息系统审计师、注册信息安全开发人员、注册渗透工程师、注册渗透测试专家、注册应急响应工程师、注册应急响应专家、注册工业控制系统安全工程师、注册云安全工程师、注册大数据安全分析师、注册电子数据取证专业人员、注册信息安全专业人员—密码技术专家、注册个人信息保护专业人员、注册数据安全治理专业人员等。

任何提供的主要服务内容与以上描述相符的服务,均可归入本类。

12.1.4 等级保护测评

等级保护测评主要是针对需方的网络安全等级测评需求,由具有服务资质的测评机构(供方)根据需方委托,依据国家网络安全等级保护制度规定,按照有关管理规范和技术标准,采用相关测评手段,遵从一定的测评规程,结合等级保护对象的安全级别,对非涉及国家秘密的网络安全等级保护对象进行检测评估,并出具等级保护测评报告,协助需方评判是否达到特定级别安全保护能力。等级保护测评包括单向测评和整体测评,其中单向测评包括物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、安全策略和管理制度、安全管理机构和人员、安全建设管理和安全运维管理等方面。

任何提供的主要服务内容与以上描述相符的服务,均可归入本类。

12.1.5 分级保护测评

分级保护测评主要是针对需方的涉密信息系统测评需求,由具有相关资质的供方根据需方委托,依据国家相关保密规定和标准,从风险管理角度,分析涉密信息系统所面临的威胁及其存在的脆弱性,提出有针对性的防护对策和整改措施,并出具测评报告,防范和化解涉密信息系统安全保密风险,为涉密信息系统安全保密提供科学依据。

任何提供的主要服务内容与以上描述相符的服务,均可归入本类。

12.1.6 密码测评

密码测评即商用密码应用安全性评估主要是针对需方使用密码的信息系统,包括相关配套密码产品、通用设备、人员、制度文档等,由具有相关资质的供方根据需方委托,根据已通过评审的密码应用方案、有关管理规范和技术标准,按照测评准备、方案编制、现场测评、分析与报告编制等过程开展测评,对密码应用的合规性、正确性和有效性等进行评估,以规范密码应用和管理。密码测评通常包括物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、管理制度、人员管理、建设运行和应急处置等方面。

任何提供的主要服务内容与以上描述相符的服务,均可归入本类。

12.1.7 其他信息安全测评服务

不属于以上服务小类的其他信息安全测评服务。

12.2 信息安全认证

12.2.1 信息安全产品认证

信息安全产品认证主要是针对需方信息安全产品的申请、维持换证等需求,由信息安全认证机构依

据相关标准和其他补充技术要求与技术规范，采取审核、验证、考核、访谈、体验等手段，实施信息安全产品认证，并向通过认证的信息安全产品颁发相应证书。信息安全产品认证是对信息安全产品符合规范及安全标准要求的一种确认活动，其证明方式是获得认证证书和或认证标志。信息安全产品认证通常包括网络关键设备和网络安全专用产品安全认证、国家信息安全产品认证、IT 产品信息安全认证等。

任何提供的主要服务内容与以上描述相符的服务，均可归入本类。

12.2.2 信息安全管理体系认证

信息安全管理体系认证主要是针对需方信息安全管理体系认证证书的申请、维持换证等需求，由信息安全认证机构依据相关标准和其他补充技术要求与技术规范，采取审核、验证、考核、访谈、体验等手段，实施信息安全管理体系认证，并在其通过认证后颁发相应证书。信息安全管理体系认证是对需方的信息安全管理体系符合规范及安全标准要求的一种确认活动，其证明方式是获得认证证书和或认证标志。

任何提供的主要服务内容与以上描述相符的服务，均可归入本类。

12.2.3 信息安全服务资质认证

信息安全服务资质认证主要是针对需方信息安全服务资质的申请、维持换证等需求，由信息安全认证机构依据相关标准和其他补充技术要求与技术规范，采取审核、验证、考核、访谈、体验等手段，衡量供方的基本资格、服务管理能力、服务技术能力和服务过程等，并颁发不同级别的资质证书。网络安全服务资质认证是对供方提供相应服务能力符合规范及安全标准要求的一种确认活动。信息安全服务资质认证类型通常包括信息安全集成、安全运维、风险评估、应急处理、软件安全开发、灾难备份与恢复、工业控制安全、信息系统审计、大数据安全、云计算安全等服务。

任何提供的主要服务内容与以上描述相符的服务，均可归入本类。

12.2.4 信息安全人员认证

信息安全人员认证主要是针对信息安全从业人员的申请、维持换证等需求，由信息安全认证机构依据相关准则、大纲等，按照专业认证方向和级别要求，对信息安全从业人员的相应能力进行考核、评估和认定，并颁发相应的能力证书。信息安全人员认证是对信息安全从业人员具备某方面的专业能力的一种确认活动。信息安全人员认证通常包括注册信息安全专业人员、注册信息安全员、信息安全保障人员认证、等级测评师认证、重要信息系统保护人员认证、注册信息安全开发人员、注册软件安全专业人员、注册信息内容安全分析师、网络安全应急响应工程师认证等。

任何提供的主要服务内容与以上描述相符的服务，均可归入本类。

12.2.5 其他信息安全认证

不属于以上服务小类的其他信息安全认证服务。

12.3 其他信息安全测评与认证服务

不属于以上服务中类的其他信息安全测评与认证服务。

13 其他信息安全服务

13.1 概述

不属于以上类别的其他信息安全服务。

13.2 扩展原则

扩展原则如下：

a) 在能满足信息安全服务需求时，优先使用已有的信息安全服务，而不必扩展新的信息安全服务；

b) 允许对现有信息安全服务施加比本文件更加详细的解释说明；

c) 扩展的信息安全服务原则上不改变本文件中现有信息安全服务的分类、名称等；

d) 扩展的信息安全服务的分类与代码符合第6章的规定。

13.3 扩展类型

扩展类型包括：

a) 增加新的服务大类；

b) 增加新的服务中类；

c) 增加新的服务小类。

附 录 A
（资料性）
信息安全服务分类新旧结构对照

信息安全服务分类新旧结构对照表见表 A.1。

表 A.1 信息安全服务分类新旧结构对照表

GB/T 30283—2022		GB/T 30283—2013	
服务类别	服务中类	服务类别	服务组件
A 信息安全咨询服务	6	A 信息安全咨询服务	5
B 信息安全设计与开发服务	2	B 信息安全实施服务	13
C 信息安全集成服务	2	C 信息安全培训服务	1
D 信息安全运营服务	14	Z 其他信息安全服务	—
E 信息的安全处理和存储服务	3	—	—
F 信息安全测评与认证服务	2	—	—
Z 其他信息安全服务	—	—	—
（合计）	29	（合计）	19

附 录 B
（资料性）
信息安全服务分类新旧类目对照

信息安全服务分类新旧类目对照表见表 B.1。

表 B.1 信息安全服务分类新旧类目对照表

GB/T 30283—2022			GB/T 30283—2013		说明
A	**信息安全咨询服务**		**A**	**信息安全咨询服务**	内容变更
A01	信息安全规划咨询		A01	信息安全规划	内容变更
A02	信息安全设计咨询		B01	信息安全设计	类别、名称、代码和内容变更
A03	信息安全管理体系咨询		A02	信息安全管理体系咨询	代码和内容变更，原 A05 部分内容调到此处
A04	信息安全工程监理		B12	信息安全监理	类别、名称、代码和内容变更
A05	信息安全测试评估	A0501 信息安全测试	B05 A03	信息安全风险评估 信息安全检查和测试	新的类别，原 A03 B05 部分内容调到此处
		A0502 信息安全风险评估			
A06	信息安全培训	A0601 信息安全意识培训	C01	信息安全培训	类别、代码和内容变更
		A0602 信息安全基础培训			
		A0603 信息安全专业培训			
A99	其他信息安全咨询服务		A99	其他信息安全咨询服务	—
B	**信息安全设计与开发服务**		—	**新的大类**	新增
B01	信息安全系统设计		—	—	新的中类
B02	信息安全开发		B03	信息安全开发	类别、代码和内容变更
B99	其他信息安全设计与开发服务		—	—	预留中类
C	**信息安全集成服务**		—	**新的大类**	—
C01	信息安全硬件集成		—	—	新的中类，原 B02 部分内容调到此处
C02	信息安全软件集成		—	—	新的中类
C99	其他信息安全集成服务		—	—	预留中类
D	**信息安全运营服务**		—	**新的大类**	—
D01	信息安全监测		B06	信息安全监控	类别、名称、代码和内容变更
D02	信息安全检查		B05	信息安全检查和测试	更名，类别、代码和内容变更
D03	威胁信息共享		—	—	新的中类
D04	信息安全分析		—	—	新的中类
D05	信息安全报送		B08	信息安全通告	类别、名称、代码和内容变更
D06	恶意代码防范和处理		—	—	新的中类

表 B.1　信息安全服务分类新旧类目对照表（续）

GB/T 30283—2022			GB/T 30283—2013		说明
D07	信息安全应急响应		A04 B07	信息安全应急管理咨询 信息安全应急处理	类别、名称、代码和内容变更。原 A04 B07 部分内容调到此处
D08	信息安全演练		—	—	新的中类
D09	信息安全调查取证		—	—	新的中类
D10	信息安全加固		B04	信息安全加固和优化	类别、名称、代码和内容变更
D11	信息安全运维规范管理		—	—	新的中类
D12	信息安全审计		B13	信息安全审计	类别、代码和内容变更
D13	身份管理		B11	电子认证服务	类别、名称、代码和内容变更
D14	备份和恢复		B09	备份和恢复	类别、代码和内容变更
D99	其他信息安全运营服务		—	—	预留中类
E	**信息的安全处理和存储服务**		—	**新的大类**	—
E01	数据安全保护		B10	数据修复	类别、名称、代码和内容变更
E02	信息安全租赁		—	—	新的中类
E03	网络信息内容审核		—	—	新的中类
E99	其他信息的安全处理和存储服务		—	—	预留中类
F	**信息安全测评与认证服务**		—	**新的大类**	—
F01	信息安全测评	F0101 信息安全产品测评	—	—	新的小类
		F0102 信息安全服务资质测评	—	—	新的小类
		F0103 信息安全人员测评	—	—	新的小类
		F0104 等级保护测评	—	—	新的小类
		F0105 分级保护测评	—	—	新的小类
		F0106 密码测评	—	—	新的小类
		F0199 其他信息安全测评服务	—	—	预留中类
F02	信息安全认证	F0201 信息安全产品认证	—	—	新的小类
		F0202 信息安全管理体系认证	—	—	新的小类
		F0203 信息安全服务资质认证	—	—	新的小类
		F0204 信息安全人员认证	—	—	新的小类
		F0299 其他信息安全测评与认证服务	—	—	预留中类
Z	**其他信息安全服务**		**Z**	**其他信息安全服务**	新增内容

附 录 C
（资料性）
信息安全服务实例及其对应服务类别

典型的信息安全服务实例与其可能包含的服务类别之间的关系如表 C.1 所示。

表 C.1 典型的信息安全服务实例

服务实例	对应的服务类别(代码)
安全咨询	A01 A02 A03
风险评估	A0502
安全集成	A01 A02 A06 B01 B02 C01 C02
安全运维	A06 D01 D02 D06 D07 D08 D10 D12
应急响应	D07
灾难恢复	A06 D14
安全培训	A06
安全测评	F01
安全监理	A04
安全审计	B12
安全运营	D01 D02 D03 D04 D05 D06 D07 D08 D09 D10 D11 D12 E01 E02 E03

附 录 D
（资料性）
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（见 GB/T 25058—2019）的对应关系，见表 D.1。

表 D.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				
服务大类	服务中类（部分含小类）		规划	设计	建设	运行	终止
信息安全咨询服务	信息安全规划咨询		√	—	—	—	√
	信息安全设计咨询		√	√	—	√	—
	信息安全管理体系咨询		√	—	—	√	—
	信息安全工程监理		√	√	√	√	—
	信息安全测试评估	信息安全测试	—	—	—	√	√
		信息安全风险评估	√	√	√	√	√
	信息安全培训	信息安全意识培训	√	√	√	√	√
		信息安全基础培训	√	√	√	√	√
		信息安全专业培训	√	√	√	√	√
信息安全设计与开发服务	信息安全系统设计		√	√	—	—	—
	信息安全开发		—	√	√	—	—
信息安全集成服务	信息安全硬件集成		—	—	√	—	—
	信息安全软件集成		—	—	√	—	—
信息安全运营服务	信息安全监测		—	—	—	√	—
	信息安全检查		√	√	√	√	√
	威胁信息共享		—	—	—	√	—
	信息安全分析		—	—	—	√	—
	信息安全报送		—	—	—	√	—
	恶意代码防范和处理		—	—	—	√	—
	信息安全应急响应		√	—	—	√	√
	信息安全演练		—	—	—	√	—
	信息安全调查取证		—	—	—	√	—
	信息安全加固		—	—	√	√	—
	信息安全运维规范管理		—	—	—	√	—
	信息安全审计		—	—	—	√	—
	身份管理		—	—	√	√	—
	备份和恢复		—	—	√	√	√

表 D.1　信息安全服务与信息系统生命周期的对应关系（续）

信息安全服务			信息系统生命周期				
服务大类	服务中类(部分含小类)		规划	设计	建设	运行	终止
信息的安全处理和存储服务	数据安全保护		√	√	√	√	√
	信息安全租赁		—	—	√	√	—
	网络信息内容审核		—	—	—	√	—
信息安全测评与认证服务	信息安全测评	信息安全产品测评	—	—	√	—	—
		信息安全服务资质测评	√	√	√	√	√
		信息安全人员测评	—	—	—	—	—
		等级保护测评	—	—	—	√	—
信息安全测评与认证服务	信息安全测评	分级保护测评	—	—	—	√	—
		密码测评	—	—	—	√	—
	信息安全认证	信息安全产品认证	—	—	√	√	—
		信息安全管理体系认证	√	√	√	√	√
		信息安全服务资质认证	√	√	√	√	√
		信息安全人员认证	—	—	—	—	—
注：“√”表示通常情况下，该项信息安全服务涉及的信息系统生命周期阶段。“—”表示通常情况下，该项信息安全服务不涉及的信息系统生命周期阶段。							

附 录 E
（资料性）
信息安全服务分类的其他形式与本文件服务类别的对应关系

信息安全服务还可分为信息安全咨询服务、信息安全工程服务、信息安全培训服务和信息安全运行服务（见 YD/T 1621—2007），见表 E.1。

表 E.1 信息安全服务分类的其他形式与本文件服务类别的对应关系

服务类型	服务类型	对应的服务类别（代码）
信息安全咨询服务	安全管理咨询	A03
	安全架构咨询	A02
	安全通告服务	D05
信息安全工程服务	安全实施方案设计	A02
	安全集成服务	C01 C02
	安全监理服务	A04
信息安全培训服务	安全培训服务	A06
信息安全运行支持服务	安全评估服务	A05
	安全加固/增强服务	D10
	安全应急响应服务	D07 A06
	安全监控服务	D01
	安全定制开发服务	B01 B02

在整个信息系统生命周期中，根据信息安全过程中各活动，可定义多种信息安全服务类型，主要包括安全集成、风险评估、灾难恢复、应急响应、安全审计、安全管理、安全运维和安全培训等（见 GB/T 30271—2013），见表 E.2。

表 E.2 信息安全服务分类的其他形式与本文件服务类别的对应关系

服务类型	对应的服务类别（代码）
安全集成	A02 B01 B02 C01 C02
风险评估	A05
灾难恢复	A06 D14
应急响应	D07 A06
安全审计	D12
安全管理	A03
安全运维	D01 D02 D03 D04 D05 D06 D07 D08 D09 D10 D11 D12 D13 D14 E01 E02 E03
安全培训	A06

信息安全服务还可分为风险评估服务、安全集成服务、应急处理服务、灾难备份与恢复服务、软件安全开发服务、安全运维服务、网络安全审计服务、工业控制安全服务（见 CCRC-ISV-C01:2018），见表 E.3。

表 E.3　信息安全服务分类的其他形式与本文件服务类别的对应关系

服务类型	对应的服务类别(代码)
风险评估	A05
安全集成	A02 A06 B01 B02 C01 C02
应急处理	A06 D07
灾难备份与恢复	A06 D14
软件安全开发	B01 B02
安全运维	D01 D02 D03 D04 D05 D06 D07 D08 D09 D10 D11 D12 D13 D14
网络安全审计	B12
工业控制安全	—

根据我国实行网络安全等级保护制度的要求,信息安全服务还可分为等级保护咨询、等级保护定级备案、等级保护建设、等级保护测评、等级保护整改自查、等级保护培训等服务,见表 E.4。

表 E.4　信息安全服务分类的其他形式与本文件服务类别的对应关系

服务类型	对应的服务类别(代码)
等级保护咨询	A01 A02
等级保护定级备案	—
等级保护建设	A04 B01 B02 C01 C02 E01 E02
等级保护测评	F0104
等级保护整改自查	A05 D01 D02 D06 D10 D11 D14
等级保护培训	A06

参 考 文 献

[1] GB/T 4754—2017 国民经济行业分类
[2] GB/T 19668.4—2017 信息技术服务 监理 第4部分:信息安全监理规范
[3] GB/T 25058—2019 信息安全技术 网络安全等级保护实施指南
[4] GB/T 25066—2020 信息安全技术 信息安全产品类别与代码
[5] GB/T 28448—2019 信息安全技术 网络安全等级保护测评要求
[6] GB/T 28827.3—2012 信息技术服务 运行维护 第3部分:应急响应规范
[7] GB/T 29264—2012 信息技术服务 分类与代码
[8] GB/T 30146—2013 公共安全 业务连续性管理体系 要求
[9] GB/T 30271—2013 信息安全技术 信息安全服务能力评估准则
[10] GB/T 32316—2015 金融租赁服务流程规范
[11] GB/T 32924—2016 信息安全技术 网络安全预警指南
[12] GB/T 35273—2020 信息安全技术 个人信息安全规范
[13] GB/T 36463.1—2018 信息技术服务 咨询设计 第1部分:通用要求
[14] GB/T 36463.2—2019 信息技术服务 咨询设计 第2部分:规划设计指南
[15] GB/T 36635—2018 信息安全技术 网络安全监测基本要求与实施指南
[16] GB/T 36643—2018 信息安全技术 网络安全威胁信息格式规范
[17] GB/T 36957—2018 信息安全技术 灾难恢复服务要求
[18] GB/T 37046—2018 信息安全技术 灾难恢复服务能力评估准则
[19] GB/T 37685—2019 物联网 应用信息服务分类
[20] GB/T 37919—2019 电子商务产品执法查处取证规则
[21] GB/T 37961—2019 信息技术服务 服务基本要求
[22] GB/T 38645—2020 信息安全技术 网络安全事件应急演练指南
[23] GB/T 39786—2021 信息安全技术 信息系统密码应用基本要求
[24] GA/T 1393—2017 信息安全技术 主机安全加固系统安全技术要求
[25] RB/T 201—2013 信息系统安全集成服务资质认证评价要求
[26] YD/T 1621—2007 网络与信息安全服务资质评估准则
[27] YD/T 1799—2008 网络与信息安全应急处理服务资质评估方法
[28] CCRC-ISV-C01:2018 信息安全服务规范
[29] 中华人民共和国数据安全法