ICS 35.080
L 77

# 中华人民共和国国家标准

GB/T 39770—2021

# 信息技术服务　服务安全要求

**Information technology service—Service security requirements**

2021-03-09 发布　　2021-10-01 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

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由全国信息技术标准化技术委员会(SAC/TC 28)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、中国电子技术标准化研究院、北京护航科技股份有限公司、北京德信永道信息技术服务有限公司、中国电子科技网络信息安全有限公司、中国电信集团有限公司、北京银信长远科技股份有限公司、成都市人力资源社会保障信息中心、四川久远银海软件股份有限公司、成都信息化技术应用发展中心、北京伟仕佳杰信息技术服务有限公司、上海北宙企业管理咨询有限公司、上海安言信息技术有限公司、金税信息技术服务股份有限公司、成都清华永新网络科技有限公司、兴业数字金融服务(上海)股份有限公司、石家庄学院、平安科技(深圳)有限公司、南方电网广东佛山供电局、浙江大华技术股份有限公司、湖北工业职业技术学院、吉林省电子信息产品检验研究院、首都信息发展股份有限公司、江苏思特瑞信息技术有限公司、国网信通亿力科技有限责任公司。

本标准主要起草人:干露、查海平、张毅、张树玲、于浩、杨泉、董贵山、蒋涛、陈剑锋、张静、何昆、黄玉娈、陈杨、岳彩云、孙佩、付华茂、杨海涛、白璐、尹正茹、刘颋、钱伟峰、熊健淞、李霞、许志恒、李俊玲、李洋、沈勇、王晶、王晓清、干国胜、王丽明、吴芸、孙宇明、陈武。

# 信息技术服务　服务安全要求

## 1　范围

本标准提出了信息技术服务安全模型，规定了安全总则、生存周期和能力要素的安全要求。

本标准适用于信息技术服务提供方、服务需求方和第三方。

## 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　信息安全技术　术语

## 3　术语和定义

GB/T 25069 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**

服务提供方为服务需求方开发、应用信息技术的服务，以及服务提供方以信息技术为手段提供支持服务需求方业务活动的服务。

注 1：常见服务内容包括软件服务、硬件服务以及其他相关的服务。

注 2：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。

[GB/T 29264—2012，定义 2.1]

3.2

**服务需求方　service acquirer**

需要信息技术服务的组织机构或个人。

3.3

**服务提供方　service provider**

提供信息技术服务的组织机构或个人。

3.4

**服务安全　service security**

不因服务提供方相关服务要素的介入，以及供需双方的交互，导致对服务需求方的业务、资产、系统等造成损害的特性。

3.5

**服务人员　service people**

提供信息技术服务所需的人员。

3.6

**服务过程　service process**

提供信息技术服务时，合理利用必要的资源，将输入转化为输出的一组相互关联和结构化的活动。

3.7

**服务技术　service technology**

交付满足质量要求的信息技术服务应使用的技术和应具备的技术能力。

3.8

**服务资源　service resource**

提供信息技术服务所依存和产生的有形及无形资产。

## 4　服务安全模型

本标准提出的信息技术服务安全模型，是以服务安全风险评估为基础，遵循服务安全原则，对服务需求方、服务提供方、服务生存周期、服务能力要素提出安全要求，达成服务安全目标。其中服务生存周期包括需求、设计、实现、运营、退出五个阶段，服务能力要素包括服务人员（简称人员）、服务过程（简称过程）、服务技术（简称技术）、服务资源（简称资源），模型如图 1 所示。

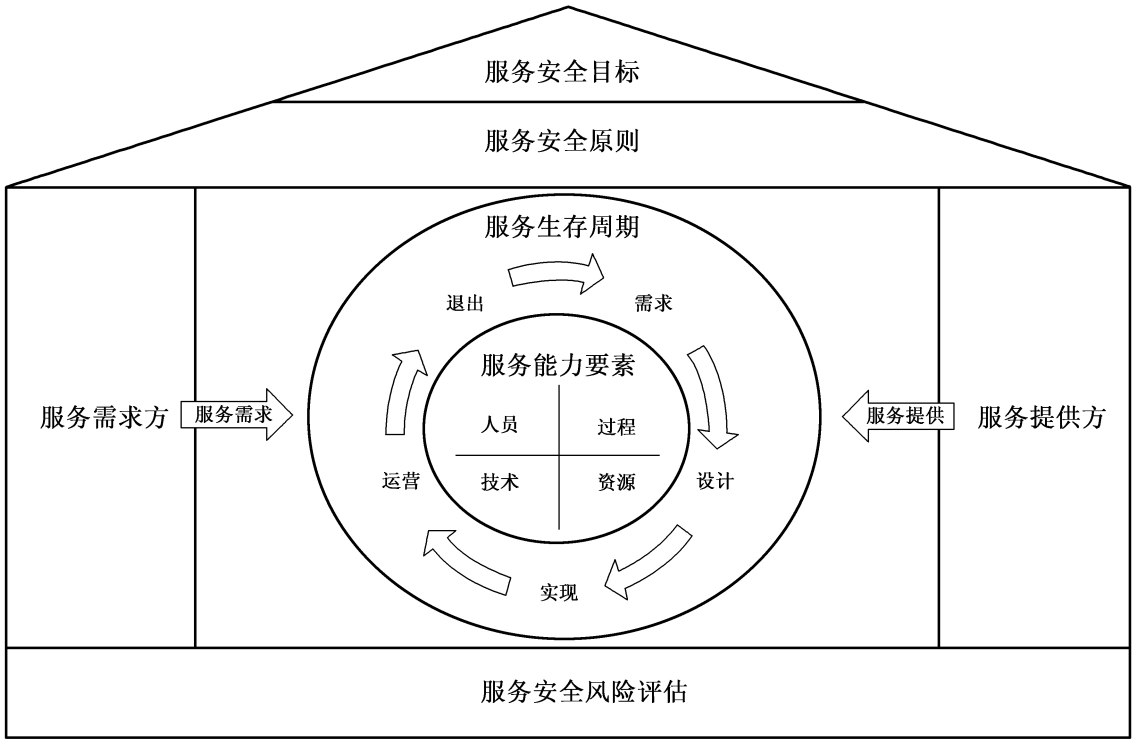


**图 1　信息技术服务安全模型**

## 5　服务安全总则

### 5.1　服务安全目标

根据信息技术服务需求和内外部环境，制定信息技术服务安全战略，通过实施技术和管理的安全控制措施，确保安全目标达成。服务安全目标包括：

a）　满足法律法规和相关标准规范要求；

b）　满足合同要求；

c）　满足服务需求方安全制度要求；

d) 满足服务过程中资产保密性、完整性和可用性要求。

### 5.2 服务安全原则

服务提供方和服务需求方在服务提供过程中应遵循以下安全原则：

a) 合规原则
以符合网络安全有关的法律、法规和标准规范为原则；

b) 关键业务原则
以优先保障服务需求方关键业务安全为原则；

c) 最小影响原则
以对服务需求方业务运行影响最小为原则；

d) 合作原则
以服务需求方和服务提供方通力合作，共同保障服务安全为原则。

### 5.3 安全风险评估

应对服务提供方、服务生存周期、服务能力要素进行安全风险评估，有针对性的落实服务安全要求，实现信息技术服务安全风险的有效控制，评估内容参见附录 A。

### 5.4 服务需求方

服务需求方从服务安全目标出发，提出服务安全需求，落实服务安全管控措施，要求包括：

a) 加强服务安全建设，完善服务安全管理制度；

b) 明确服务安全需求，将需求传达到服务提供方；

c) 为服务提供方提供必要的资源支持；

d) 开展服务安全监督，配合服务提供方不断提升服务安全水平。

### 5.5 服务提供方

#### 5.5.1 组织架构

服务提供方应建立服务安全组织机构和定义服务安全职责，要求包括：

a) 具备与信息技术服务相符合的人力资源规模，建立服务安全组织机构；

b) 定义相关服务安全岗位，明确安全职责。

注：服务安全角色和职责定义示例参见附录 B。

#### 5.5.2 管理制度

服务提供方应建立服务安全管理制度，要求包括：

a) 建立服务安全管理制度，满足所提供的信息技术服务需求；

注：建立信息安全管理制度时参见 GB/T 24405.1—2009 和 GB/T 22080—2016。

b) 保持与服务需求方的安全管理要求一致；

c) 持续开展制度执行情况的内部检查和改进；

d) 定期评审服务安全管理制度的有效性。

#### 5.5.3 供应链安全

服务提供方应确保服务供应链安全，提升服务连续性，要求包括：

a) 明确服务项目涉及的外部供应链及其支撑关系，并得到服务需求方确认；

b) 选用可替代的服务和产品，减少单一供应商依赖；

c) 将服务安全目标、原则和相关安全要求有效传递到外部供应链；
d) 与外部供应商签订服务协议或采购协议，并对协议执行情况进行有效的监督。

## 6 服务生存周期安全要求

### 6.1 需求

服务提供方通过对服务需求进行调研分析，识别和控制服务需求安全风险，要求包括：
a) 评估服务提供方的服务能力、资质、服务体系、安全管理和保障能力，选择可靠的服务提供方；
b) 分析服务安全需求，包括明确需求（如：协议要求、业务要求）和隐含需求（如：法律法规要求、服务需求方期望），形成服务需求文档；
c) 评审服务需求，确保供需双方达成共识；
d) 签订服务合同或服务协议，确保包含服务安全和保密义务条款。

### 6.2 设计

服务提供方根据服务需求方的安全需求进行服务设计，识别和控制服务设计安全风险，要求包括：
a) 编制服务设计方案，确定服务所需的组件和要素，满足服务安全需求；
b) 制定服务安全管理、评价和改进计划，保障服务所需的资源和预算，确保符合整体安全目标；
c) 评审新的或变更的服务对现有服务的风险及应对措施，并保留过程记录。

### 6.3 实现

服务提供方根据服务设计方案进行实现部署，识别和控制服务实现安全风险，要求包括：
a) 确保实现结果和服务设计保持一致并能满足安全需求；
b) 进行测试或者试运行，减少过程风险和对生产运营环境的影响，如进行压力测试、用户测试等；
c) 识别服务部署、移交过程中的风险，并制定合理的应对措施。

### 6.4 运营

服务需求方对服务提供方所提供的服务进行监控，识别和控制服务运营安全风险，要求包括：
a) 建立服务过程，确保服务过程的有效执行，并形成记录；
b) 备份并妥善保管服务过程中产生的服务数据（如方案、报告、记录等）；
c) 定期审核服务安全管控的执行情况，对异常情况及时采取处置措施；
d) 制定、更新服务安全应急预案，并组织演练和评估；
e) 动态监控服务安全风险，制定风险处置策略，及时采取风险处置措施；
f) 针对服务过程中关键业务和关键资产的变更、重大事件或重要时期等，加强对服务风险监控和预警，做好应急协同准备；
g) 对服务过程所涉及的设施、数据、事件、问题、配置等敏感信息进行保密；
h) 安全合理地使用服务过程中所产生的信息资料，确保不在服务范围以外使用。

### 6.5 退出

服务协议到期或终止时，为确保服务顺利退出，服务双方通过沟通并选择适当的退出策略，识别和控制服务退出安全风险，要求包括：
a) 制定服务终止计划，识别服务终止的风险，采取相应风险控制措施；
b) 在确保业务连续性的前提下，对服务中投入的设备设施、信息资源、人员等进行回收确认；
c) 对服务相关资料进行移交、保存或销毁；

d) 对服务授权和敏感信息进行安全审查。

## 7 服务能力要素安全要求

### 7.1 人员

#### 7.1.1 人员选择

根据服务安全需求对人员进行选择，要求包括：

a) 识别和定义服务岗位的安全要求；
b) 对重要岗位服务人员进行背景调查；
c) 为服务人员分配唯一的身份标识；
d) 基于职责分离和最小授权的原则为服务人员分配权限；
e) 对涉及敏感信息的服务人员，明确其保密义务并签订保密协议。

#### 7.1.2 人员培训

按服务安全需求对人员进行培训，要求包括：

a) 在上岗前，对人员开展服务安全培训，培训内容包括但不限于：相关法律法规、安全制度和规范、安全意识、从事服务所需的必要安全技能等；
b) 有特殊安全要求的岗位人员，应具备相关的资质认证；
c) 服务过程中，定期对人员开展服务安全培训。

#### 7.1.3 人员考核

按服务安全需求对人员进行考核，要求包括：

a) 在上岗前，对人员开展信息安全考核，考核不通过的人员不予上岗；
b) 服务过程中，定期开展信息安全考核，考核不通过的人员加强培训或进行更换；
c) 对违反安全规定的责任人员记录考核绩效，造成不利影响的责任人员应承担相应责任。

#### 7.1.4 人员变更

发生人员变更需要进行有效安全管控，要求包括：

a) 人员变更前，服务提供方提前告知服务需求方并提交变更方案，经双方确认后，在确保业务连续性的情况下实施变更；
b) 变更确认后，收回离场人员所有信息资产，撤销离场人员相关权限，并进行书面确认；
c) 变更结束后，以书面形式对离场人员重申保密义务，离场人员接受追溯审计。

### 7.2 过程

#### 7.2.1 过程定义

过程定义安全应明确服务过程定义和安全责任，要求包括：

a) 定义服务标准作业过程和服务监督管理过程；
b) 识别过程所有权，明确过程活动安全权责；
c) 明确过程及其相关文档版本控制；
d) 对服务过程进行定期评审。

#### 7.2.2 过程执行

过程执行安全应明确服务过程安全执行并持续监控安全风险，要求包括：

a) 按照过程定义，配备人员和资源，采取约定的技术执行服务；
b) 落实服务过程安全控制措施；
c) 持续进行服务安全风险监控。

#### 7.2.3 过程记录

过程记录安全应明确服务过程记录的存储和访问控制，要求包括：

a) 确保所有的服务过程和服务活动都形成记录；
b) 确保服务过程记录不被非授权访问；
c) 对服务过程记录进行存储和备份，保存期限应满足合规要求。

#### 7.2.4 过程变更

过程变更安全应明确服务过程变更需要的安全控制，要求包括：

a) 严格按照变更管理制度实施过程变更，确保变更过程获得审批；
b) 评审变更过程的合理性和正确性，充分评估变更安全风险；
c) 在受控的环境下对变更进行充分测试；
d) 记录并保留变更过程和结果。

### 7.3 技术

#### 7.3.1 技术获取

技术获取安全应确保以合理的方式获得安全合规的技术，要求包括：

a) 选择安全合规的技术提供方，并满足所提供技术的安全支持能力；
b) 确保获得的技术是完整、安全和可靠的；
c) 在技术许可协议中，明确与技术安全有关的参数；
d) 论证和审定技术获取过程的合理性和正确性；
e) 记录并保留技术获取的方法和理由。

#### 7.3.2 技术实施

技术实施安全应确保所实施技术的安全性，要求包括：

a) 提供交付清单并进行核实，如技术设备、工具、文档等；
b) 提供技术培训，如技术原理、技术使用、安全风险等；
c) 针对技术实施在受控环境下进行充分测试；
d) 论证和审定技术实施过程的合理性和正确性；
e) 记录并保留技术实施的过程和结果。

#### 7.3.3 技术维护

技术维护安全应确保技术可以持续满足服务协议，要求包括：

a) 监控技术运行状况，持续评估技术是否满足服务协议；
b) 根据服务需求和技术进步及时调整相应技术，包括技术引入、技术升级、技术退出等，并评估风险；

c) 记录并保留技术维护的过程和结果。

## 7.4 资源

### 7.4.1 资源分类分级

识别资源的安全需求和敏感程度，对资源进行分类分级管理。

### 7.4.2 资源安全责任

识别并定义资源安全的不同角色，明确每种角色的安全责任。

### 7.4.3 资源合理使用

#### 7.4.3.1 资源获取

资源获取安全应确保资源合法获取和可用，要求包括：

a) 确保服务资源的可用性；

b) 确保服务资源获取的合法性。

#### 7.4.3.2 资源利用

资源利用安全应确保服务过程中资源的合理使用，要求包括：

a) 确保服务资源仅用于服务的预定目的，防止非授权访问；

b) 制定资源利用规则和过程，避免资源滥用；

c) 保留资源使用记录和日志。

#### 7.4.3.3 资源回收

资源回收安全应确保服务结束后资源进行安全回收，要求包括：

a) 服务结束后及时释放资源，进行服务资源回收；

b) 评估资源回收的访问权限残留风险，及时回收各类访问账号和权限；

c) 评估资源回收的数据残留风险，按照要求进行有效的风险处置。

# 附 录 A
（资料性附录）
# 信息技术服务安全风险评估

信息技术服务安全风险评估对象包括服务提供方、服务生存周期和服务能力要素，评估内容见表 A.1 所示。

**表 A.1 安全风险评估对象和评估内容**

| 评估对象 | 评估内容 |
| --- | --- |
| 服务提供方 | 对服务提供方的安全风险评估内容包括：<br>1） 经营资质；<br>2） 财务状况；<br>3） 服务能力；<br>4） 服务安全保障能力；<br>5） 供应链安全等 |
| 服务生存周期 | 对服务生存周期的安全风险评估内容包括：<br>1） 服务需求阶段风险，如服务合同和服务协议；<br>2） 服务设计阶段风险，如服务变更；<br>3） 服务实现阶段风险，如服务部署；<br>4） 服务运营阶段风险，如安全事件；<br>5） 服务退出阶段风险，如资料移交 |
| 服务能力要素 | 对服务能力要素的安全风险评估内容包括：<br>1） 服务人员风险评估，如人员培训；<br>2） 服务过程风险评估，如过程变更；<br>3） 服务技术风险评估，如技术授权；<br>4） 服务资源风险评估，如资源安全责任 |

# 附 录 B
（资料性附录）
服务安全角色和职责示例

信息技术服务安全相关的角色和职责示例见表 B.1。

**表 B.1 服务安全角色和职责示例**

| 角色 | 职责的简要描述 |
| --- | --- |
| 高级管理者（例如首席安全官，或承担信息安全管理职责的其他高级管理者） | 负责愿景、战略决策和协调活动，建立信息技术服务相符合的信息安全治理架构和安全管理制度，为服务安全提供人员、资金等支持 |
| 项目组长 | 服务项目中的项目负责人。具体工作职责包括：<br>1） 根据项目情况组建服务团队；<br>2） 确定服务对象和服务范围，并指导团队进行风险评估工作；<br>3） 牵头编写服务部署计划以及规范服务过程；<br>4） 监督、协调和控制服务过程安全；<br>5） 与相关方及时进行沟通交流，针对可能发生的问题进行研讨；<br>6） 服务完成后，提请相关方进行服务验收 |
| 安全管理人员 | 负责服务过程中安全管理工作的实施人员。具体工作职责包括：<br>1） 负责服务实施过程、相关文档的把控，并参与编写服务文档；<br>2） 向相关方解答关于服务项目中涉及的管理性细节问题 |
| 信息技术服务人员 | 服务项目中的服务实施人员。具体工作职责包括：<br>1） 根据服务目标以及服务范围，参与调研，参与资产风险评估；<br>2） 参与编写《风险处置计划》和《服务部署方案》；<br>3） 遵照《服务部署方案》实施具体的技术性服务；<br>4） 对服务过程中遇到的问题及时向项目组长汇报，并提出需要协调的资源；<br>5） 将过程中的技术性服务工作成果汇总，提交服务交付物；<br>6） 解答关于服务项目中涉及的技术性细节问题 |
| 信息系统安全管理员 | 确保信息系统在整个服务过程中的安全 |

## 参 考 文 献

[1] GB/T 20984—2007 信息安全技术 信息安全风险评估规范

[2] GB/T 22080—2016 信息技术 安全技术 信息安全管理体系 要求

[3] GB/T 24405.1—2009 信息技术 服务管理 第1部分:规范

[4] GB/T 24405.2—2010 信息技术 服务管理 第2部分:实践规则

[5] GB/T 29264—2012 信息技术服务 分类与代码

[6] ISO 31000:2018 Risk Management—Guidelines

[7] NIST SP800-35:2003 Guide to Information Technology Security Services

[8] NIST SP800-39:2011 Managing Information Security Risk:Organization,Mission,and Information System View

[9] NIST SP800-53 Rev.4:2015 Security and Privacy Controls for Information Systems and Organizations