Q/BJKB

北京坤标检验认证有限公司企业标准

Q/BJKB 012-2026

云服务信息安全管理体系 基本要求

Basic Requirements for Cloud Services Information Security Management System

2026-4-1 发布　　2026-4-1 实施

北京坤标检验认证有限公司　　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》起草，以 ISO/IEC 27017:2015《信息技术 安全技术 基于 ISO/IEC 27002 的云服务信息安全控制实用规则》为核心依据，融合管理体系高阶结构（HLS），形成可用于第三方认证的云服务信息安全管理体系企业标准。

本文件规定组织建立、实施、保持和持续改进云服务信息安全管理体系的强制性认证要求，适用于云服务提供商、云服务客户及相关方开展云服务全生命周期信息安全管理，可用于第三方认证、自我评价、内部审核与监管评估。

本文件由北京坤标检验认证有限公司提出并归口。

本文件主要起草人：陈刚辉、杨英者、吕晚香、李英华。

云服务信息安全管理体系 基本要求

1 范围

1.1 本文件规定云服务信息安全管理体系的组织环境、领导作用、策划、支持、运行、绩效评价与持续改进要求。
1.2 适用于云服务全场景（IaaS、PaaS、SaaS），覆盖云环境下数据、系统、网络、物理、运维、外包、业务连续性等信息安全管理活动。
1.3 本文件可作为云服务合规、监管检查、第三方评估与认证的依据，不替代国家法律法规、行业标准与强制性要求。

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
GB/T 35273 信息安全技术 个人信息安全规范
GB/T 41479-2022 信息安全技术 网络数据处理安全要求
GB/T 19011 管理体系审核指南

3 术语和定义

下列术语和定义适用于本文件。
ISO/IEC 27001:2013 信息技术 安全技术 信息安全管理体系 要求
ISO/IEC 27002:2013 信息技术 安全技术 信息安全控制实践指南
ISO/IEC 27017:2015 信息技术 安全技术 基于
ISO/IEC 27002 云服务信息安全控制实用规则
ISO/IEC 27018:2014 信息技术 安全技术 云服务中个人可识别信息（PII）保护指南
GB/T 19011 管理体系审核指南
界定的术语和定义适用于本文件。

4 组织的背景

4.1 了解组织和其背景

组织应确定与云服务信息安全相关的内外部问题：
外部：法律法规、数据跨境、监管要求、行业标准、供应链风险、云服务类型；
内部：组织战略、业务架构、云部署模式、数据分类分级、第三方接入、共享责任边界。

4.2 理解相关方的需求和期望

组织应识别并确定相关方要求：
a）监管部门对云服务安全、数据保护、个人信息保护的要求；
b）云服务客户对数据主权、访问控制、审计追溯、业务连续性的需求；

c）员工、供应商、合作伙伴在云环境中的安全责任与权限要求；
d）数据主体对个人信息保护、知情权、控制权的期望。
适当时保留成文信息，包括需求清单、合规清单、责任边界约定记录。

4.3 确定网络数据安全管理体系范围

组织应明确体系边界和适用性：
a）覆盖的云服务类型：IaaS、PaaS、SaaS；
b）覆盖的云环境：公有云、私有云、混合云、多云；
c）覆盖的安全域：物理、网络、主机、数据、应用、身份、运维、外包、应急；
d）覆盖的组织单元、系统、数据、人员、第三方供应商。
范围应形成成文信息，不适用条款应说明理由并保留记录。

4.4 网络数据安全管理体系

组织应按照本文件要求，建立、实施、保持并持续改进云服务信息安全管理体系：
a）确定体系所需过程及其在云业务中的应用；
b）确定过程顺序与相互作用，适配云共享责任模型；
c）确定过程准则与方法，确保云环境安全运行与控制；
d）确保资源与信息可获取，支持云安全过程运行与监视；
e）监视、测量、分析云安全过程绩效；
f）实施措施，实现过程改进与体系预期结果。
云外包、第三方接入、多云管理过程应被识别、控制并保留责任追溯。

5 领导作用

5.1 领导作用和承诺

最高管理者应证实对云服务信息安全体系的领导与承诺：
a）确保制定云安全方针与目标，与云服务战略一致；
b）确保将体系要求融入云服务全生命周期；
c）确保云安全资源可获得，适配云环境特性；
d）沟通云安全合规与共享责任的重要性；
e）确保体系实现预期结果，保障云服务持续安全；
f）指导、支持员工为体系有效性贡献；
g）推动持续改进；
h）明确云安全责任边界并监督落实。

5.2 方针

云服务信息安全方针应：
a）适应组织目的与云安全风险；
b）为建立云安全目标提供框架；
c）包含合规、数据保护、业务连续性、持续改进承诺；
d）形成成文信息，沟通、传达，并可为相关方获取

5.3 岗位、职责和权限

最高管理者应确保分配与沟通：
a）明确云安全责任人、云安全管理员、云运维管理员职责；

b）云服务团队、安全团队、客户团队、第三方的安全职责；
c）确保体系符合本文件要求；
d）向最高管理者报告云安全绩效、风险与改进机会。

6 策划

6.1 应对风险和机遇的措施

组织应确定云服务信息安全相关的风险与机遇：
—风险：数据泄露、越权访问、共享环境风险、身份冒用、运维失控、跨境风险、供应商失控、业务中断；
—机遇：合规提升、云安全能力成熟、客户信任增强、安全成本优化、业务可持续。
组织应策划：
a）应对风险和机遇的措施；
b）如何将措施整合并实施到云安全体系过程中；
c）如何评价措施有效性。
措施应包括：云风险评估、共享责任约定、访问控制、数据加密、审计追溯、应急处置、多云安全管控。

6.2 云服务信息安全目标及实现策划

组织应在相关职能、层次建立可测量的云安全目标：
a）云安全控制覆盖率、风险闭环率；
b）身份认证与权限合规率、最小权限落实率；
c）数据加密覆盖率、日志审计完整率；
d）云安全事件发生率、应急响应时效达标率；
e）第三方云供应商安全合规率；
f）业务连续性演练覆盖率、RTO/RPO 达标率。
目标应：与方针一致、可测量、可监视、可沟通、适时更新、形成成文信息。
策划实现目标时应确定：做什么、资源、责任人、时限、评价方法。

6.3 变更的策划

云服务、云架构、云供应商、业务流程发生变更时，应同步策划云安全调整，确保变更安全、可控、不降低安全水平，保留变更记录。

7 支持

7.1 资源

组织应提供并保障：
a）云安全人力、技术、资金、工具、场所资源；
b）云安全责任人、安全管理员、审计员、应急人员配置；
c）云安全工具：身份管理、加密、脱敏、堡垒机、日志审计、监控告警、备份恢复；
d）内部审核、管理评审、应急演练资源。

7.2 能力

组织应：

a）确定云安全岗位人员的能力要求；
b）基于教育、培训、经验确保人员胜任；
c）提供云安全、ISO/IEC 27017、共享责任、数据保护培训；
d）评价培训与能力有效性；
e）保留能力、培训、考核记录。

7.3 意识

组织应确保人员知晓：
a）云安全方针与共享责任模型；
b）个人对云安全体系有效性的贡献；
c）违规、泄露、事件的后果与责任；
d）云环境下数据保护、权限管控、操作规范。

7.4 沟通

组织应建立内外部云安全沟通机制：
沟通内容、时机、对象、方式、记录，包括：
内部：云安全要求、事件、整改、培训；
外部：监管、客户、云供应商、第三方、审计机构。

7.5 成文信息

7.5.1 组织应控制以下成文信息：
a）方针、目标、范围、共享责任矩阵；
b）云资产清单、数据分类分级清单、风险评估与处置记录；
c）云安全制度、流程、操作规程、应急预案；
d）身份权限、访问控制、加密、审计日志、备份恢复记录；
e）第三方云供应商管理、合同、评估、监督记录；
f）事件、应急、整改记录；
g）内审、管理评审、改进记录。
7.5.2 成文信息应：标识、清晰、批准、发放、更改、存储、保护、检索、处置。

8 运行

8.1 运行策划和控制

组织应策划、实施、控制云服务全生命周期安全过程，满足 ISO/IEC27017 要求：
a）云安全风险评估与控制实施；
b）共享责任模型定义与落实；
c）云环境安全配置、加固、监控；
d）数据全生命周期安全：收集、存储、使用、传输、备份、删除、匿名化；
e）其他需要建立的运行控制措施。

8.2 云环境访问控制

统一身份管理、多因素认证、最小权限、权限定期评审；
堡垒机、操作审计、会话录屏、高危操作审批；
禁止共享账号、越权访问、未授权下载与导出。

8.3 云网络与通信安全

网络分区、边界防护、流量加密、入侵检测/防御；
云防火墙、安全组、VPC 隔离、端口最小化开放；
传输加密（TLS）、接口安全、API 安全管控。

8.4 云数据安全

数据分类分级、敏感数据加密（存储＋传输）；
数据脱敏、水印、防泄露、操作审计:
数据备份与恢复、容灾、定期演练；
数据跨境合规、留存期限管控、安全销毁。

8.5 云物理与环境安全

云数据中心物理准入、安防监控、环境管控；
介质安全、设备安全、运维操作物理管控；
满足 ISO/IEC 27017 对云物理安全的要求。

8.6 云运维安全

运维权限管控、操作留痕、双人复核；
变更管理、版本管理、漏洞管理、补丁管理；
日志集中采集、存储、分析、告警、留存审计。

8.7 第三方与供应商安全

云供应商准入、安全评估、合同约定、责任明确；
持续监督、定期审计、风险评估、退出管控；
多云、混合云供应商统一安全管控。

8.8 业务连续性与灾难恢复

制定云业务连续性计划、应急预案；
RTO/RPO 目标设定、备份恢复演练；
多云/跨区域容灾、故障自动切换。

8.9 云安全事件应急处置

建立云安全事件应急机制：分级、启动、资源、流程、预案、演练；
事件发生时立即处置、止损、溯源、通报、整改、复盘改进。

9 绩效评价

9.1 监视、测量、分析和评价

组织应监视测量：
a）云安全目标完成情况；
b）云安全控制有效性、合规性；
c）权限合规、日志审计、漏洞整改闭环；
d）事件、隐患、供应商合规、相关方反馈；
e）内审、管理评审发现问题及整改情况；

f）其他需监视测量的内容。

9.2 内部审核

组织应按年度实施内审，验证：

a)符合本文件、ISO/IEC 27017、法律法规、自身要求;

b）有效实施与保持。

应制定审核方案，确保客观公正，出具报告，对不符合项整改验证。

9.3 管理评审

最高管理者应定期评审，确保体系适宜、充分、有效。

输入包括：

a）以往评审跟踪措施；

b）内外部问题与相关方需求变化；

c）目标绩效、监视测量结果；

d）内审结果、不符合与纠正措施；

e）风险评估、事件、应急、供应商情况；

f）资源充分性、改进机会。

输出包括：改进、目标调整、资源、风险措施更新。

10 改进

10.1 持续改进

组织应持续改进体系的适宜性、充分性、有效性。

10.2 不合格与纠正措施

发生不合格、事件、隐患、内审 / 评审发现问题时：

a) 处置不合格；

b) 评审原因；

c) 采取纠正措施；

d) 验证有效性；

e) 更新成文信息。

参 考 文 献

[1] GB/T19011 管理体系审核指南
[2] GB/T27011 合格评定认可机构要求
[3] GB/T27021.1 合格评定管理体系审核认证机构要求第 1 部分：要求
[4] GB/T 25069 信息安全技术 术语
[5] GB/T 35273 信息安全技术 个人信息安全规范
[6] GB/T 41479-2022 信息安全技术 网络数据处理安全要求
[7] GB/T 19011 管理体系审核指南