云服务信息安全管理体系

认证技术规范

文件编号：CTS TBGL142-2026

版本号：B/2

受控状态： （ 受控 ）

编写：技术部

审核：张辉根

批准：周春阳

首次发布：2022-12-20 **首次实施：2022-12-20** **修订实施日期：20260423**

江西腾标认证有限公司

目录

前言

本文件旨在为组织（以下简称"组织"）建立、实施、维护和持续改进云服务信息安全管理体系（CSMS）提供要求和指南。本文件采用PDCA（策划-实施-检查-改进）循环模式，与 **ISO/IEC 27001:2022《信息安全、网络安全和隐私保护 — 信息安全管理体系 — 要求》** 的高阶结构保持一致，并充分融合了 **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施规范》** 的特定行业控制要求。

本文件旨在为组织在基于ISO/IEC 27001:2022建立和实施信息安全管理体系的过程中，提供一套专门的云服务信息安全控制选择和实施指南。本文件的核心架构与ISO/IEC 27001:2022完全一致，组织可通过实施本文件，建立一个同时满足ISO/IEC 27001和ISO/IEC 27017:2015要求的整合性管理体系。组织应首先建立满足ISO/IEC 27001要求的信息安全管理体系（ISMS），并在此基础上扩展云服务信息安全管理要求。

1. 范围

本文件规定了组织建立、实施、保持和持续改进 云服务信息安全管理体系认证技术规范 的要求。本文件适用于

1） 组织建立、实施、保持和改进 云服务信息安全管理体系认证技术规范 管理方针和目标；

2） 认证机构对组织进行云服务信息安全管理体系认证技术规范认证。

2. 规范性引用文件

下列文件对于本文件的应用必不可少。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。

- ISO/IEC 27000 信息技术 — 安全技术 — 信息安全管理体系 — 概述和词汇
- ISO/IEC 27001:2022 信息安全、网络安全和隐私保护 — 信息安全管理体系 — 要求
- ISO/IEC 27002:2022 信息安全、网络安全和隐私保护 — 信息安全控制
- 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施规范

注：认证审核时引用文件的有效性以审核实施时现行有效的最新版本为准。

3. 术语和定义

ISO/IEC 27000、ISO/IEC 27001:2022界定的以及下列术语和定义适用于本文件。ISO和IEC在以下地址维护用于标准化的术语数据库：

- ISO在线浏览平台：https://www.iso.org/obp
- IEC电子百科：https://www.electropedia.org/

3.1 云服务

通过网络提供可扩展和弹性的、可测量的、按需自服务的资源（如网络、服务器、存储、应用和服务）的一种模式。

[来源：ISO/IEC 17788:2014, 3.2.8]

3.2 云服务客户

为使用云服务而与云服务提供商建立业务关系的参与方。

[来源：ISO/IEC 17788:2014, 3.2.10]

3.3 云服务提供商

提供云服务的参与方。

[来源：ISO/IEC 17788:2014, 3.2.11]

3.4 云服务用户

使用云服务的个人或实体。

[来源：ISO/IEC 17788:2014, 3.2.12]

3.5 云服务客户数据

云服务客户在云服务中存储、处理或传输的数据。

3.6 云服务衍生数据

云服务提供商在提供云服务过程中生成的、与云服务客户相关的数据（如日志、元数据）。

3.7 多租户环境

一种云服务部署模式，其中单个云服务实例同时服务于多个云服务客户，这些客户共享计算、存储和网络资源，但彼此隔离。

3.8 虚拟网络

在物理网络基础设施之上通过虚拟化技术创建的逻辑网络。

4. 组织环境

4.1 理解组织及其环境

组织应确定与其意图相关的，且影响其实现CSMS预期结果能力的外部和内部事项。

- **外部因素**：适用的信息安全法律和法规（如《网络安全法》、《数据安全法》、《个人信息保护法》等）、监管机构要求（如网信办、工信部、数据局等）、行业标准与最佳实践、云服务特有的威胁（如多租户风险、供应链攻击、数据跨境传输）、云服务提供商的安全能力、客户对云服务安全的期望等。
- **内部因素**：组织的规模、治理结构、作为云服务客户或提供者的角色、云服务的使用模式（IaaS/PaaS/SaaS）、云服务客户数据的敏感度、人员云安全技能与意识、以往云安全事件记录等。

4.2 理解相关方的需求和期望

组织应确定：

a) 与CSMS有关的相关方；

b) 这些相关方的有关要求；

c) 哪些要求将通过CSMS予以解决。

相关方包括但不限于：云服务客户、云服务提供商、云服务用户、监管机构、员工、合作伙伴、供应商、认证机构、公众。

组织应建立、实施并保持程序，以识别相关方，并促其参与到与CSMS相关的已识别的议题中。与相关方的沟通应为一个**持续的过程**。**组织应将促进相关方参与所产生的输出形成文件**。

4.3 确定CSMS的范围

组织应确定CSMS的边界及其适用性，以建立其范围。在确定范围时，组织应考虑：

a) 4.1中提到的外部和内部事项；

b) 4.2中提到的要求；

c) 组织实施的活动与其他组织实施的活动之间的接口和依赖关系（特别是与云服务提供商、云服务客户之间的接口）。

范围应形成文件化信息并可用。

4.4 云服务信息安全管理体系（CSMS）

4.4.1 组织应按照本标准的要求，建立、实施、保持和持续改进云服务信息安全管理体系，包括所需过程及其相互作用。

组织应确定云服务信息安全管理体系所需的过程及其在整个组织中的应用，且应：

a) 确定这些过程所需的输入和期望的输出；

b) 确定这些过程的顺序和相互作用；

c) 确定和应用所需的准则和方法（包括监视、测量和相关绩效指标），以确保这些过程的有效运行和控制；

d) 确定这些过程所需的资源并确保其可获得；

e) 分配这些过程的职责和权限；

f) 按照 6.1 的要求应对风险和机遇；

g) 评价这些过程，实施所需的变更，以确保实现这些过程的预期结果；

h) 改进过程和云服务信息安全管理体系。

4.4.2 在必要的范围和程度上，组织应：

a) 保持成文信息以支持过程运行；

b) 保留成文信息以确信其过程按策划进行。

5. 领导作用

5.1 领导作用和承诺

最高管理者应通过以下活动，证实其在对CSMS的领导作用和承诺：

a) 确保建立云服务信息安全方针和目标，并与组织战略方向一致；

b) 确保将CSMS要求融入组织的业务过程；

c) 确保CSMS所需的资源可获得；

d) 沟通有效的云服务信息安全管理的重要性；

e) 确保CSMS达成其预期结果（如云服务安全、合规、客户信任）；

f) 指导并支持相关人员为CSMS的有效性做出贡献；

g) 促进持续改进；

h) 支持其他相关管理角色在其职责范围内发挥领导作用。

5.2 方针

最高管理者应建立云服务信息安全方针，该方针应：

a) 与组织的宗旨相适宜；

b) 包括信息安全目标（见6.2）或为设定信息安全目标提供框架；

c) 包括对满足适用信息安全与云服务安全相关要求的承诺；

d) 包括对持续改进CSMS的承诺；

e) **特别应包括对保护云服务客户数据、遵守云服务相关法律法规以及明确与云服务提供商/客户之间职责分配的承诺**。

信息安全方针应：

f) 形成文件化信息并可获取；

g) 在组织内得到沟通；

h) 适当时，可被相关方获取（如云服务客户、监管机构）。

5.3 组织的岗位、职责和权限

最高管理者应确保与云服务信息安全相关岗位、职责和权限在组织内得到分配和沟通。

最高管理者应**指定一名或多名管理者**（如云安全负责人、信息安全负责人），不论其是否负有其他职责，应使其具有以下方面的岗位、职责和权限：

a) 确保CSMS符合本文件的要求；

b) 向最高管理者报告CSMS绩效，供其评审并作为持续改进的依据；

c) 确保在整个组织内提高对云服务信息安全重要性的意识；

d) 协调与CSMS有关的内部和外部沟通（特别是与云服务客户和云服务提供商）。

同时，最高管理者应明确**指定一个联络点**，供云服务客户或云服务提供商使用，以处理与云服务信息安全相关的事宜（根据ISO/IEC 27017:2015第6.1.1条）。

6. 策划

6.1 应对风险和机会的措施

6.1.1 总则

当策划CSMS时，组织应考虑4.1中提到的事项和4.2中提到的要求，并确定需要应对的风险和机会，以：

a) 确保CSMS可达到预期结果；

b) 预防或减少不良影响（如云服务数据泄露、合规处罚、客户流失、服务中断）；

c) 达到持续改进。

组织应策划：

d) 应对这些风险和机会的措施；

e) 如何将此措施整合到CSMS过程中并予以实现及评价其有效性。

6.1.2 云服务信息安全风险评估

组织应定义并应用风险评估过程，以建立并维护风险准则（包括风险接受准则和评估实施准则）；识别与云服务相关的信息安全风险（如多租户隔离失效、云服务提供商锁定、数据跨境传输风险、供应链风险、未授权访问云管理接口）；分析并评价风险。风险评估应特别考虑云服务特有的威胁和脆弱性。组织应保留有关风险评估过程的文件化信息。

6.1.3 云服务信息安全风险处置

组织应定义并应用风险处置过程，以选择适当的处置方案（通过 **ISO/IEC 27001:2022附录A** 及 **ISO/IEC 27017:2015** 中的控制措施）。组织应**制定并维护一个《适用性声明》**，包含所选控制措施及删减的合理性说明，并制定正式的风险处置计划。组织应保留有关风险处置过程的文件化信息。

注： 组织应**建立并保持合规义务登记册**，以识别和跟踪与云服务信息安全相关的法律法规、标准及其他要求。

6.2 云服务信息安全目标及其实现的策划

组织应在相关职能和层级上建立云服务信息安全目标。目标应：

a) 与云服务信息安全方针一致；

b) 可测量（如云服务安全事件数、云服务客户投诉率、培训完成率、审计发现项关闭率、服务可用性指标）；

c) 考虑适用的要求；

d) 予以监视；

e) 予以沟通；

f) 视情况予以更新。

策划如何实现这些目标时，组织应确定要做什么、需要什么资源、由谁负责、何时完成、如何评价结果。

6.3 针对变更的规划

当组织确定需要对CSMS进行变更时（如引入新的云服务、切换云服务提供商、法律法规重大变更、云服务架构重大调整），变更应系统地予以策划和实施。

7. 支持

7.1 资源

组织应确定并提供建立、实施、维护和持续改进CSMS所需的资源。资源包括：具备相应能力的人员（云安全架构师、云运维工程师等）、技术基础设施（云安全工具、加密工具、访问控制系统、日志审计系统、入侵检测系统等）、财务资源、技术资源等。

7.2 能力

组织应：确定从事会影响组织云服务信息安全绩效的工作人员的必要能力（如云安全技术、云服务管理、风险评估方法）；基于适当的教育、培训或经验确保其胜任；适用时采取措施获得必要能力（如云安全培训、认证），并评估有效性；保留适当的文件化信息作为能力的证据（如培训记录、认证证书）。

注：**能够访问云服务客户数据的人员应承担保密义务**（根据ISO/IEC 27017:2015附录A.10.1）。

7.3 意识

在组织控制下工作的人员应了解：

a) 云服务信息安全方针；

b) 其对CSMS有效性的贡献；

c) 不符合CSMS要求的潜在影响（尤其是对云服务客户和组织的风险）。

7.4 沟通

组织应确定与CSMS相关的内部和外部沟通的需求，包括：沟通什么（如云服务安全策略、安全事件通知、职责分配变更）、何时沟通、与谁沟通、谁来沟通、怎么沟通。特别地，应建立与云服务客户和云服务提供商关于信息安全的沟通机制。

7.5 文件化信息

7.5.1 总则

组织的CSMS应包括：本文件要求的文件化信息（如CSMS手册、风险评估报告、风险处置计划、适用性声明、云服务安全策略等）；组织为CSMS有效性所确定的必要的文件化信息（如云服务配置清单、安全操作流程、事件响应计划）。

7.5.2 创建和更新

创建和更新文件化信息时，组织应确保适当的标识和说明、形式、载体以及评审和批准。

7.5.3 文件化信息的控制

CSMS及本文件所要求的文件化信息应得到控制，以确保：在需要的场合和时机可获得并适用；予以妥善保护（避免泄密、不当使用或缺失）。为控制文件化信息，适用时，组织应分发、访问、检索和使用；存储和防护；更改控制；保留和处置。

8. 运行

8.1 运行的策划和控制

组织应策划、实施和控制为满足要求和实施第6章所确定的措施所需的过程，包括建立过程准则，并按照准则实施控制。组织应控制计划内和计划外的变更，确保外部提供的过程、产品和服务受控。

8.2 云服务信息安全风险评估

组织应考虑6.1.2a) 所建立的准则，按计划的时间间隔或当重大变更发生时（如新云服务上线、云服务提供商变更），执行云服务信息安全风险评估。应保留风险评估结果的文件化信息。

8.3 云服务信息安全风险处置

组织应实现云服务信息安全风险处置计划。应保留风险处置结果的文件化信息。

8.4 云服务信息安全特定控制措施（依据ISO/IEC 27017:2015）

组织应按本章节要求实施和运行特定的云服务信息安全控制措施，这些措施补充和细化了ISO/IEC 27001:2022附录A中的相关控制。

8.4.1 云服务信息安全策略（依据ISO/IEC 27017:2015第5章）

控制

应制定和维护云服务信息安全策略，以管理组织的云服务信息安全。

实施要求：

a) 制定并维护文件化的《云服务信息安全策略》，该策略应由最高管理层批准。

b) 该策略应涵盖：云服务使用原则；云服务客户数据保护；职责分配（云服务客户与提供商

之间）；访问控制原则；加密要求；事件响应要求；合规要求。

c) 该策略应定期评审和更新（至少每年一次）。

8.4.2 云服务中的职责分配（依据ISO/IEC 27017:2015第6.1.1条）

控制

应明确并记录云服务客户与云服务提供商之间的信息安全角色和职责。

实施要求：

a) 组织（作为云服务客户或提供商）应与对方就信息安全角色和职责的适当分配达成一致，并记录在案。

b) 组织应确认其能够履行其分配的职责。

c) 组织应识别和管理其与对方客户支持与维护职能的关系。

8.4.3 云服务中的资产责任（依据ISO/IEC 27017:2015第6.1.5条）

控制

应明确云服务客户数据及相关资产的所有权和责任。

实施要求：

a) 应定义并记录所有云服务客户数据资产的所有权。

b) 应明确对与这些资产相关的操作（如备份和恢复操作）负有责任的各方。

8.4.4 云服务中的意识、教育和培训（依据ISO/IEC 27017:2015第7.2.2条）

控制

应为云服务相关角色提供针对性的意识、教育和培训。

实施要求：

a) 组织应在意识、教育和培训计划中添加以下项目：

- 云服务使用标准和程序；
- 与云服务相关的信息安全风险以及如何管理这些风险；
- 使用云服务带来的系统和网络环境风险；
- 适用的法律和法规考虑。

b) 应向管理和上级经理（包括业务部门经理）提供有关云服务的信息安全意识、教育和培训计划。

8.4.5 云服务中的用户注册和注销（依据ISO/IEC 27017:2015第9.2.1条）

控制

应管理云服务用户的注册和注销。

实施要求：

a) **（云服务提供商）** 应提供用户注册和注销功能，以及使用这些功能的规范给云服务客户。

b) **（云服务客户）** 应使用云服务提供商提供的功能来管理其用户的访问。

8.4.6 云服务中的用户访问供给（依据ISO/IEC 27017:2015第9.2.2条）

控制

应确保云服务中的访问控制得以实现。

实施要求：

a) **（云服务客户）** 应确保能够根据其访问控制策略限制对云服务中信息的访问，并确保实现此类限制。

b) **（云服务提供商）** 应提供访问控制，允许云服务客户限制对其云服务、云服务功能和服务中维护的云服务客户数据的访问。

8.4.7 云服务中的加密与密钥管理（依据ISO/IEC 27017:2015第10.1.1条）

控制

应使用加密技术保护云服务客户数据。

实施要求：

a) **（云服务客户）** 如果风险分析证明合理，应为其使用云服务实施加密控制。

b) **（云服务提供商）** 应向云服务客户提供关于其使用加密技术保护云服务客户数据的情况的信息。

8.4.8 云服务中的事件日志记录（依据ISO/IEC 27017:2015第12.4.1条）

控制

应记录云服务中的安全事件日志。

实施要求：

a) **（云服务客户）** 应定义其事件日志记录要求，并验证云服务是否满足这些要求。

b) **（云服务提供商）** 应向云服务客户提供日志记录功能。

8.4.9 云服务中的技术脆弱性管理（依据ISO/IEC 27017:2015第12.6.1条）

控制

应管理可能影响云服务的技术脆弱性。

实施要求：

a) **（云服务客户）** 应向云服务提供商请求有关管理可能影响所提供云服务的技术脆弱性的信息。

b) **（云服务提供商）** 应向云服务客户提供有关管理可能影响所提供云服务的技术脆弱性的信息。

8.4.10 云服务中的信息安全事件管理（依据ISO/IEC 27017:2015第16.1.1条）

控制

应明确云服务中的信息安全事件管理职责。

实施要求：

a) **（云服务客户）** 应验证信息安全事件管理职责的分配，并确保其满足要求。

b) **（云服务提供商）** 作为服务规范的一部分，应定义云服务客户和云服务提供商之间的信息安全事件管理职责和程序。

8.4.11 云服务中的合规（依据ISO/IEC 27017:2015第18.1.1条）

控制

应确保云服务符合适用的法律、法规和合同要求。

实施要求：

a) **（云服务客户）** 应考虑相关法律法规可以是管辖云服务提供商的司法管辖区的法律法规，也可以是管辖云服务客户的法律法规。

b) **（云服务提供商）** 应向云服务客户告知管理云服务的法律管辖区。

c) **（云服务提供商）** 应确定其自身的相关法律要求（例如，关于保护个人身份信息的加密），并在要求时提供给云服务客户。

d) **（云服务提供商）** 应向云服务客户提供其当前符合适用立法和合同要求的证据。

8.4.12 云服务扩展控制集（依据ISO/IEC 27017:2015附录A）（修订）

控制

应实施云服务扩展控制集，以应对云服务特有的风险。

实施要求：

a) **云服务客户数据隔离（CLD.8.1.1）：** 云服务提供商应实施云服务客户数据、虚拟化应用程序、操作系统、存储和网络的适当逻辑隔离，包括多租户环境下的资源分离和云服务提供商内部管理与客户资源的分离。

b) **虚拟网络配置（CLD.13.1.1）：** 云服务提供商应根据物理网络的信息安全策略为虚拟网络的配置定义和记录信息安全策略。云服务提供商应确保虚拟网络配置与信息安全策略匹配，而不管创建配置的方式如何。

c) **虚拟机强化与安全（CLD.9.1.5 / CLD.12.1.5）：** 在配置虚拟机时，应确保适当的方面得到加强（如仅开放必要的端口、协议和服务），并确保为所使用的每个虚拟机制定适当的技术措施（如反恶意软件、日志记录）。云服务客户应记录关键操作的过程（如安装、变更和删除虚拟设备；云服务使用终止程序；备份和恢复），并指定一个主管监视这些操作。云服务提供商应向需要关键操作和程序的云服务客户提供相关文档。

d) **服务监控（CLD.12.1.5）：** 云服务提供商应提供使云服务客户能够监控与云服务客户有关的云服务操作特定方面的功能（例如，监控和检测云服务是否被用作攻击他人的平台，或敏感数据是否从云服务中泄漏）。云服务提供商应提供这些监控功能的文档。

9. 绩效评价

9.1 监视、测量、分析和评价

组织应确定：需要被监视和测量的内容（包括云服务安全事件、云服务可用性、云服务客户投诉、合规性偏差等）；适用的方法；何时执行；谁应执行；何时分析和评价结果。组织应评价云服务信息安全绩效以及CSMS的有效性。**确保用于监视与测量的资源（如云安全监控平台、日志分析系统）的准确性**。

9.1.2 合规性评价

组织应建立、实施并保持程序，以定期评价其对适用法律法规（特别是云服务相关法律）、标准及自身CSMS要求的遵守情况。**合规性评价应至少每年进行一次**，并**保留合规性评价报告作为成文信息**。

9.2 内部审核

组织应按策划的时间间隔进行内部审核，以提供有关CSMS符合性及有效性的信息。审核员应确保客观性和公正性。审核结果应报告给相关管理层。

9.3 管理评审

最高管理者应按计划的时间间隔评审CSMS，以确保其持续的适宜性、充分性和有效性。管理评审应考虑：

a) 以往管理评审措施的状态；

b) 内外部的变化（如新的云服务法规、云服务技术发展、云服务提供商变更）；

c) 绩效信息（包括：云服务安全事件趋势、云服务客户投诉率、**外部供方（如云服务提供商、云服务分包商）的绩效**、合规性偏差、风险评估与处置状态、改进机会等）；

d) 持续改进的机会。

评审输出应包括与持续改进机会及CSMS变更需求相关的决定。

10. 改进

10.1 持续改进

组织应持续改进CSMS的适宜性、充分性和有效性。

10.2 不符合与纠正措施

当发生不符合时，组织应：做出应对、控制并纠正，处置后果；评价是否需要采取措施消除原因；实施所需的措施并评审有效性；必要时对CSMS进行更改。应保留文件化信息作为不符合性质及后续采取措施的证据。**推荐预防措施**以防范潜在不符合的发生（例如，通过定期云服务安全评估，预防新云服务带来的安全风险）。

————————————————