

认 证 技 术 规 范

CTS QAC/IT03—2026

基于 ISO/IEC27017 控制的云服务信息安全 全管理体系 要求

Requirements for Cloud Service Information Security Management System based
on controls in ISO/IEC 27017

2026 -08 -27 发布

2026 - 08 - 27 实施

中质协质量保证中心 发 布

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。

本文件由中质协质量保证中心提出并归口。

本文件起草单位：中质协质量保证中心。

本文件主要起草人：徐强、谭虎、曹红玲、王雪静、刘俊伟。

引言

随着数字化转型深入推进与数据要素价值释放，云服务环境下的业务数据已成为组织重要战略资产与关键生产要素。云环境中业务数据贯穿收集、使用、留存、披露、销毁等完整生命周期，其安全管控直接关系到组织资产安全、合规履约能力以及业务稳定运行。当前，云服务环境下业务数据面临数据泄露、恶意攻击等各类安全威胁持续加剧，加之云环境数据跨境流动、信息安全相关监管规则不断完善，组织在云服务场景开展数据安全保护工作，同时面临管理、技术与合规层面的多重现实挑战。

为规范云服务场景下组织数据安全管理工作，依据国家网络安全、数据安全相关法律法规，对接 GB/T 22080-2025/ISO/IEC 27001:2022《网络安全技术 信息安全管理体系 要求》、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的实施规范》等标准，结合云服务环境数据全生命周期安全管理实践，制定本认证技术规范。

本文件聚焦云服务场景数据安全核心管控需求，构建覆盖组织环境、领导责任、规划、支持、运行、绩效评价、改进的全流程管理体系，明确云服务下数据安全的管理原则、控制目标、实施要求与实践指南，涵盖云环境数据资产管控、信息分类、访问控制、多租户隔离、物理与环境安全、运行安全、通信安全、密码保护、介质处置、测试数据防护、云服务供应商安全、信息安全事件管理、业务连续性、安全合规性等关键领域，适用于各类使用或提供云服务的组织建立、实施、运行、监视、评审、维护和改进云服务场景数据安全管理体系。

本文件整合两项标准的核心内容，进一步细化云服务场景数据安全管理体系相关要求，提升实施的明确性与可操作性：

- GB/T 22080-2025/ISO/IEC 27001:2022 网络安全技术 信息安全管理体系 要求
- 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的实施规范

本文件旨在引导组织建立系统化、标准化、可落地的云服务数据安全治理机制，平衡云业务场景下数据应用效率与安全保障水平，识别、防范并处置云环境数据处理全流程中的各类安全风险，保障业务数据的保密性、完整性、可用性，满足监管合规与业务发展双重需要，促进云环境下数据要素安全有序流通与价值释放，为组织云化数字化高质量发展提供坚实安全支撑。

目 录

前 言	3
引 言	4
1 范围	1
2 规范性引用文件.....	1
3 术语和定义	1
4 组织环境	1
4.1 理解组织及其环境	1
4.2 理解相关方的需求和期望	1
4.3 确定云服务信息安全管理体范围	2
4.4 云服务信息安全管理体	2
5 领导	2
5.1 领导和承诺	2
5.2 方针	2
5.3 组织的角色、责任和权限	2
6 规划	3
6.1 应对风险和机会的措施	3
6.2 信息安全目标及其实现规划	4
6.3 针对变更的规划	4
7 支持	4
7.1 资源	4
7.2 能力	5
7.3 意识	5
7.4 沟通	5
7.5 文件化信息	5
8 运行	6
8.1 运行规划和控制	6
8.2 信息安全风险评估	6
8.3 信息安全风险处置	6
9 绩效评价	6
9.1 监视、测量、分析和评价	6
9.2 内部审核	6
9.3 管理评审	7
10 改进	7
10.1 持续改进	8
10.2 不符合与纠正措施	8

附 录 A （规范性） 信息安全控制	1
附录 B（规范性附录） 云服务信息安全 控制集	6
1 范围	6
2 规范性引用文件	6
3 术语和缩略语	6
4 云领域特定概念	7
5 信息安全方针	8
6 信息安全组织	9
7 人力资源安全	11
8 资产管理	12
9 访问控制	13
10 密码学	15
11 物理和环境安全	16
12 运行安全	18
13 通信安全	21
14 系统获取、开发和维护	22
15 供应商关系	24
16 信息安全事件管理	25
17 业务连续性管理的信息安全方面	26
18 符合性	27
CLD. 6. 3 云服务客户与云服务提供商的关系	30
CLD. 8. 1 资产责任	30
CLD. 9. 5 共享虚拟环境中云服务客户数据的访问控制	30
CLD. 12. 1 运行流程与职责	31
CLD. 12. 4 日志与监控	32
CLD. 13. 1 网络安全管理	32
参考文献	33

基于 ISO/IEC27017 控制的云服务信息安全管理 体系 要求

1 范围

本文件规定了在组织环境下建立、实现、维护和持续改进云服务信息安全管理的要求。本文件还包括了根据组织需求所剪裁的信息安全风险评和处置的要求。本文件规定的要求是通用的，适用于各种类型、规模或性质的组织。当组织声称符合本文件时，不接受排除第4章到第10章中规定的任何要求。

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 22080-2025/ISO/IEC 27001:2022 网络安全技术 信息安全管理 体系 要求
ISO/IEC 29151:2017 信息技术 安全技术 个人可识别信息保护实施规范

3 术语和定义

ISO/IEC 27000界定的术语和定义适用于本文件。

下列文件界定的术语和定义适用于本文件：

ISO/IEC 29151:2017 信息技术 安全技术 个人可识别信息保护实施规范

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，且影响其达到云服务信息安全管理预期结果能力的外部 and 内部事项。

组织应确定气候变化¹是否是一个相关事项。

||

注：对这些事项的确定，见GB/T 24353-2022中5.4.1建立外部和内部环境。

4.2 理解相关方的需求和期望

组织应确定：

a) 云服务信息安全管理的相关方；

¹ 有关气候变化的更多信息，可参见 ISO 和 IAF（国际认可论坛）关于管理体系标准中增加气候变化因素的联合公报。

- b) 这些相关方的有关要求；
- c) 哪些要求将通过云服务信息安全管理体系予以解决。

注1：相关方的要求包括法律、法规和合同义务。

注2：相关方可能提出与气候变化相关的要求。

||

4.3 确定云服务信息安全管理体系范围

组织应确定云服务信息安全管理体系的边界及其适用性，以建立其范围。

组织应根据以下内容确定云服务信息安全管理体系范围：

- 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。

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

组织应按照本文件的要求，建立、实现、维护和持续改进云服务信息安全管理体系，包括所需的过程及其相互作用。

5 领导

5.1 领导和承诺

最高管理层应通过以下活动，证实其对云服务信息安全管理体系的领导和承诺：

- a) 确保建立了信息安全方针和信息安全目标，并与组织战略方向一致；
- b) 确保将云服务信息安全管理体系要求整合到组织的业务过程中；
- c) 确保云服务信息安全管理体系所需资源可用；
- d) 沟通有效个人可识别信息保护管理的重要性和符合云服务信息安全管理体系要求的重要性；
- e) 确保云服务信息安全管理体系达到预期结果；
- f) 指导并支持相关人员为云服务信息安全管理体系的有效性做出贡献；
- g) 促进持续改进；
- h) 支持其他相关管理角色在职责范围内证实其领导作用。

注：本文件中提到的“业务”能广义地解释为对组织的意图具有核心意义的活动。

5.2 方针

最高管理层应建立信息安全方针，该方针应：

- a) 与组织的意图相适宜；
- 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) 包括对满足适用的信息安全相关要求的承诺；
- d) 包括对持续改进云服务信息安全管理体系的承诺。

信息安全方针应：

- e) 形成文件化信息并可用；
- f) 在组织内得到沟通；
- g) 适当时，对相关方可用。

5.3 组织的角色、责任和权限

最高管理层应确保与信息安全相关角色的责任和权限在组织内得到分配和沟通。

最高管理层应分配责任和权限，以便：

- a) 确保云服务信息安全管理符合本文件的要求；
- b) 向其报告云服务信息安全管理绩效。

注：最高管理层也能在组织内分配报告云服务信息安全管理绩效的责任和权限。

6 规划

6.1 应对风险和机会的措施

6.1.1 总则

当规划云服务信息安全管理时，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，以便：

- a) 确保云服务信息安全管理能达到预期结果；
- b) 预防或减少不良影响；
- c) 达到持续改进。

组织应规划：

- d) 应对这些风险和机会的措施；
- e) 如何：
 - 1) 将这些措施整合到云服务信息安全管理过程中，并予以实现；
 - 2) 评价这些措施的有效性。

6.1.2 信息安全风险评估

组织应定义并应用信息安全风险评估过程，以：

- a) 建立并维护信息安全风险准则，包括：
 - 1) 风险接受准则；
 - 2) 信息安全风险评估实施准则；
- b) 确保重复实施的信息安全风险评估能产生一致的、有效的和可比较的结果；
- c) 识别信息安全风险：
 - 1) 应用信息安全风险评估过程，以识别云服务信息安全管理范围内与信息保密性、完整性和可用性损失有关的风险；
 - 2) 识别风险责任人；
- d) 分析信息安全风险：
 - 1) 评估 6.1.2 c) 1) 中所识别的风险发生后，可能导致的潜在后果；
 - 2) 评估 6.1.2 c) 1) 中所识别的风险实际发生的可能性；
 - 3) 确定风险级别；
- e) 评价信息安全风险：
 - 1) 将风险分析结果与 6.1.2 a) 中建立的风险准则进行比较；
 - 2) 对已分析的风险进行风险处置优先级排序。

组织应保留有关信息安全风险评估过程的文件化信息。

6.1.3 信息安全风险处置

组织应定义并应用信息安全风险处置过程，以：

- a) 在考虑风险评估结果的基础上，选择适合的信息安全风险处置选项；
- b) 确定实现已选的信息安全风险处置选项所必需的所有控制；

注1：组织能按需设计控制，或识别来自任何来源的控制。

- c) 将 6.1.3 b) 确定的控制与附录 A、B、C 中的控制进行比较，并验证没有遗漏必要的控制；

注2：附录A、B、C包含了可能的信息安全控制清单。本文件的用户在附录A的指引下，确保没有忽略必要的信息安全控制。

注3：附录A、B、C所列的信息安全控制并不是完备的，且如有必要，组织能引入额外的信息安全控制。

- d) 制定适用性声明，其包含：
 - 必要的控制[见6.1.3 b) 和c)]；
 - 选择这些控制的合理性说明；
 - 必要的控制是否已实现；
 - 删减附录A、B、C中控制的合理性说明；

- e) 制定正式的信息安全风险处置计划；

- f) 获得风险责任人对信息安全风险处置计划的批准和对信息安全残余风险的接受。

组织应保留有关信息安全风险处置过程的文件化信息。

注4：本文件中的信息安全风险评估和处置过程与GB/T 24353-2022中给出的原则和通用指南相一致。

6.2 信息安全目标及其实现规划

组织应在相关职能和层级上建立信息安全目标。

信息安全目标应：

- a) 与信息安全方针一致；
- b) 可测量（如可行）；
- c) 考虑适用的信息安全要求，以及风险评估和风险处置的结果；
- d) 得到监视；
- e) 得到沟通；
- f) 适当时予以更新；
- g) 形成文件化信息且可用。

组织应保留有关信息安全目标的文件化信息。

在规划如何达到信息安全目标时，组织应确定：

- h) 要做什么；
- i) 需要什么资源；
- j) 由谁负责；
- k) 何时完成；
- l) 如何评价结果。

6.3 针对变更的规划

当组织确定需要变更云服务信息安全管理体系时，应对这些变更的实施进行规划。

7 支持

7.1 资源

组织应确定并提供建立、实现、维护和持续改进云服务信息安全管理体系所需的资源。

7.2 能力

组织应：

- a) 确定在其控制下工作且影响其信息安全绩效的人员的必要能力；
- b) 确保上述人员在适当的教育、培训或经验的基础上能够胜任其工作；
- c) 适用时，采取措施以获得必要的能力，并评估所采取措施的有效性；
- d) 保留适当的文件化信息作为能力的证据。

注：适用的措施可能包括：例如，针对现有雇员提供培训、指导或重新分配工作；雇佣或签约有能力的人员。

7.3 意识

在组织控制下工作的人员应了解：

- a) 信息安全方针；
- b) 其对云服务信息安全管理体系统效性的贡献，包括改进信息安全绩效带来的益处；
- c) 不符合云服务信息安全管理体系统效要求带来的影响。

7.4 沟通

组织应确定与云服务信息安全管理体系统效相关的内部和外部的沟通需求，包括：

- a) 沟通什么；
- b) 何时沟通；
- c) 与谁沟通；
- d) 如何沟通。

7.5 文件化信息

7.5.1 总则

组织的云服务信息安全管理体系统应包括：

- a) 本文件要求的文件化信息；
- b) 组织所确定的、对于云服务信息安全管理体系统效性所必需的文件化信息。

注：不同组织有关云服务信息安全管理体系统文件化信息的详略程度可能是不同的，这是由于：

- 1) 组织的规模及其活动、过程、产品和服务的类型；
- 2) 过程及其相互作用的复杂性；
- 3) 人员的能力。

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：

- a) 标识和描述（例如，标题、日期、作者或引用编号）；
- b) 格式（例如，语言、软件版本、图表）和介质（例如，纸质的、电子的）；
- c) 对适宜性和充分性的评审和批准。

7.5.3 文件化信息的控制

云服务信息安全管理体系统及本文件所要求的文件化信息应得到控制，以确保其：

- a) 在需要的地点和时间，是可用的和适宜使用的；
- b) 得到充分的保护（例如，避免保密性损失、不恰当使用、完整性损失）。

为控制文件化信息，适用时，组织应开展以下活动：

c) 分发、访问、检索和使用；

注：访问可能隐含着仅允许浏览文件化信息，或允许并授权浏览和更改文件化信息等的决定。

d) 存储和保护，包括保持可读性；

e) 对变更的控制（例如，版本控制）；

f) 保留和处理。

组织确定的、为规划和运行云服务信息安全管理体系所必需的外来的文件化信息，应得到适当的识别，并予以控制。

8 运行

8.1 运行规划和控制

为了满足要求并实现第 6 章中确定的措施，组织应通过以下方式规划、实现和控制所需的过程：

——建立过程的准则；

——根据准则实现对过程的控制。

文件化信息应可用，其程度足以确信这些过程按计划得到执行。

组织应控制计划内的变更并评审非预期变更的后果，必要时采取措施减轻任何负面影响。

组织应确保由外部提供的与云服务信息安全管理体系有关的过程、产品或服务是受控的。

8.2 信息安全风险评估

组织应依据 6.1.2 a) 所建立的准则，按计划的时间间隔，或当重大变更提出或发生时，执行信息安全风险评估。

组织应保留信息安全风险评估结果的文件化信息。

8.3 信息安全风险处置

组织应实现信息安全风险处置计划。

组织应保留信息安全风险处置结果的文件化信息。

9 绩效评价

9.1 监视、测量、分析和评价

组织应确定：

a) 需要被监视和测量的内容，包括信息安全过程和控制；

b) 适用的监视、测量、分析和评价的方法，以确保得到有效的结果。所选的方法宜产生可比较和可再现的结果，才会被视为有效；

c) 何时应执行监视和测量；

d) 谁应监视和测量；

e) 何时应分析和评价监视和测量的结果；

f) 谁应分析和评价这些结果。

作为结果证据的文件化信息应可用。

组织应评价信息安全绩效和云服务信息安全管理体系的有效性。

9.2 内部审核

9.2.1 总则

组织应按计划的时间间隔进行内部审核，以提供下列相关信息：

- a) 云服务信息管理体系是否符合：
 - 1) 组织自身对云服务信息管理体系的要求；
 - 2) 本文件的要求；
- b) 云服务信息管理体系是否得到有效实现和维护。

9.2.2 内部审核方案

组织应规划、建立、实施和维护审核方案（一个或多个），包括审核频次、方法、责任、规划要求和报告。

组织应根据相关过程的重要性和以往审核的结果，建立审核方案。

组织应：

- a) 定义每次审核的审核准则和范围；
- b) 选择审核员并实施审核，确保审核过程的客观性和公正性；
- c) 确保将审核结果报告至相关管理层。

作为审核方案实施和审核结果证据的文件化信息应可用。

9.3 管理评审

9.3.1 总则

最高管理层应按计划的时间间隔评审组织的云服务信息管理体系，以确保其持续的适宜性、充分性和有效性。

9.3.2 管理评审的输入

管理评审应包括下列相关信息：

- a) 以往管理评审提出的措施的状态；
- b) 与云服务信息管理体系相关的外部 and 内部事项的变化；
- c) 云服务信息管理体系相关方的需求和期望的变化；
- d) 有关信息安全绩效的反馈，包括以下方面的趋势：
 - 1) 不符合与纠正措施；
 - 2) 监视和测量结果；
 - 3) 审核结果；
 - 4) 信息安全目标完成情况；
- e) 相关方反馈；
- f) 风险评估结果及风险处置计划的状态；
- g) 持续改进的机会。

9.3.3 管理评审的结果

管理评审的结果应包括与持续改进机会相关的决定以及变更云服务信息管理体系的任何需求。作为管理评审结果证据的文件化信息应可用。

10 改进

10.1 持续改进

组织应持续改进云服务信息安全管理体的适宜性、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：

- a) 对不符合做出反应，且适用时：
 - 1) 采取措施，对其予以控制和纠正；
 - 2) 处理其后果；
- b) 通过以下活动，评价采取消除不符合原因的措施的需求，以防止不符合再次发生或在其他地方发生：
 - 1) 评审不符合；
 - 2) 确定不符合的原因；
 - 3) 确定类似的不符合是否存在，或是否可能发生；
- c) 实现任何需要的措施；
- d) 评审任何所采取的纠正措施的有效性；
- e) 必要时，对云服务信息安全管理体进行变更。

纠正措施应与所发生的不符合的影响相适合。

作为以下证据的文件化信息应可用：

- f) 不符合的性质及所采取的任何后续措施；
- g) 任何纠正措施的结果。

附 录 A
(规范性)
信息安全控制

表 A.1 所列的信息安全控制是直接源自 GB/T 22081-2024 第 5 章到第 8 章中所列的信息安全控制并与之相一致，应与 6.1.3 一起使用。

表 A.1 信息安全控制

5	组织控制	
5.1	信息安全策略	控制 应定义信息安全方针和特定主题策略，由管理层批准后发布，传达并让相关工作人员和相关方知悉，按计划的时间间隔以及在发生重大变更时对其进行评审
5.2	信息安全角色和责任	控制 信息安全角色和责任应根据组织需求进行定义和分配
5.3	职责分离	控制 应分离相互冲突的职责和责任范围
5.4	管理责任	控制 管理层应要求所有工作人员根据组织已建立的信息安全方针、特定主题策略和规程，履行信息安全责任
5.5	与职能机构的联系	控制 组织应建立并维护与相关职能机构的联系
5.6	与特定相关方的联系	控制 组织应建立并维护与特定相关方或其他专业安全论坛和专业协会的联系
5.7	威胁情报	控制 应收集并分析信息安全威胁相关的信息，以生成威胁情报
5.8	项目管理中的信息安全	控制 应将信息安全整合到项目管理中
5.9	信息及其他相关资产的清单	控制 应编制和维护信息及其他相关资产（包括资产拥有者）的清单
5.10	信息及其他相关资产的可接受使用	控制 应识别、文件化并实施信息及其他相关资产的可接受使用规则和处理规程
5.11	资产归还	控制 适宜时，工作人员和其他相关方在任用、合同或协议变更及终止时，应归还其拥有的所有组织资产
5.12	信息分级	控制 应根据组织基于保密性、完整性、可用性的信息安全需求以及相关方的要求，对信息进行分级
5.13	信息标记	控制 应按照组织采用的信息分级方案，制定并实施适当的信息标记规程
5.14	信息传输	控制 应为组织内部以及组织与其他各方之间所有类型的传输设施，制定信息传输规则、规程或协议
5.15	访问控制	控制 应基于业务和信息安全要求，建立和实施信息及其他相关资产的物理和逻辑访问控制规则
5.16	身份管理	控制 应管理身份的全生存周期
5.17	鉴别信息	控制 应通过管理过程控制鉴别信息的分配和管理，包括向工作人员提供鉴别信息的适当处理建议
5.18	访问权限	控制 应根据组织访问控制的特定主题策略和规则来提供、评审、修改和删除信息及其他相关资产的访问权限
5.19	供应商关系中的信息安全	控制 应定义并实施过程和规程，以管理供应商产品或服务使用相关的信息安全风险
5.20	在供应商协议中强调信息安全	控制 应根据供应商关系的类型建立相关的信息安全要求，并与每个供应商达成一致

5.21	管理信息通信技术供应链中的信息安全	控制 应定义并实施过程和规程，以管理与信息通信技术（ICT）产品和服务供应链相关的信息安全风险
5.22	供应商服务的监视、评审和变更管理	控制 组织应定期监视、评审、评价和管理供应商信息安全实践和服务交付的变更
5.23	云服务使用的信息安全	控制 应根据组织的信息安全要求，建立云服务的获取、使用、管理和退出过程
5.24	信息安全事件管理规划和准备	控制 组织应通过定义、建立和传达信息安全事件管理过程、角色和责任，为管理信息安全事件做出规划和准备
5.25	信息安全事态的评估和决策	控制 组织应评估信息安全事态，并决定是否将其归类为信息安全事件
5.26	信息安全事件的响应	控制 应按照文件化的规程响应信息安全事件
5.27	从信息安全事件中学习	控制 应使用从信息安全事件中得到的知识来加强和改进信息安全控制
5.28	证据收集	控制 组织应建立并实施包括识别、收集、获取和保存信息安全事态相关证据的规程
5.29	中断期间的信息安全	控制 组织应制定在中断期间将信息安全维持在适当级别的计划
5.30	业务连续性的信息通信技术就绪	控制 应根据业务连续性目标和信息通信技术（ICT）连续性要求，策划、实施、维护和测试ICT的就绪
5.31	法律、法规、规章和合同要求	控制 应识别与信息安全相关的法律、法规、规章和合同要求，以及组织满足这些要求的方法，并将其文件化且保持更新
5.32	知识产权	控制 组织应实施适当的规程来保护知识产权
5.33	记录的保护	控制 应保护记录不被丢失、破坏、篡改、未经授权的访问和未经授权的发布
5.34	隐私和个人可识别信息保护	控制 组织应根据适用的法律、法规和合同要求，识别并满足有关隐私保护和个人可识别信息（PII）保护的要求
5.35	信息安全的独立评审	控制 组织管理信息安全的方法及其实现，包括人员、过程和技术，应在计划的时间间隔内或发生重大变化时进行独立评审
5.36	符合信息安全的策略、规则 and 标准	控制 应定期评审与组织信息安全方针、特定主题策略、规则和标准的符合性
5.37	文件化的操作规程	控制 信息处理设施的操作规程应形成文件，并对有需要的工作人员可用
6	人员控制	
6.1	审查	控制 加入组织前，应对所有拟录用工作人员的候选人进行背景审查，并在入职后持续进行，同时考虑适用的法律、法规和道德规范，与业务要求、访问信息的级别和感知到的风险相适宜
6.2	任用条款和条件	控制 应在任用合同协议中规定工作人员和组织对信息安全的责任
6.3	信息安全意识、教育和培训	控制 组织工作人员和相关方应接受适宜的信息安全意识、教育和培训，并获得与其工作职能相关的组织信息安全方针、特定主题策略和规程的定期更新信息
6.4	违规处理过程	控制 应正式制定违规处理过程并将之传达给工作人员和相关方，以便对违反信息安全策略的工作人员和其他相关方采取措施
6.5	任用终止或变更后的责任	控制 应确定任用终止或变更后仍有效的信息安全责任及其义务，传达至相关工作人员和其他相关方并执行
6.6	保密或不泄露协议	控制

		应识别、文件化、定期评审反映组织信息保护需求的保密或不泄露协议，并与工作人员和其他相关方签署
6.7	远程工作	控制 应在工作人员远程工作时实施安全措施，以保护在组织场所外所访问的、处理的或存储的信息
6.8	信息安全事态的报告	控制 组织应提供机制，使工作人员通过适当渠道及时报告观察到的或可疑的信息安全事态
7	物理控制	
7.1	物理安全边界	控制 应定义并使用安全边界来保护包含信息及其他相关资产的区域
7.2	物理入口	控制 安全区域应由适当的入口控制和访问点保护
7.3	办公室、房间和设施的安全保护	控制 应对办公室、房间和设施的物理安全进行设计，并予以实施
7.4	物理安全监视	控制 应持续监视场所，以防止发生未经授权的物理访问
7.5	物理和环境威胁防范	控制 应对物理和环境威胁的防范进行设计并予以实施，例如，自然灾害和其它对基础设施有意或无意的物理威胁
7.6	在安全区域工作	控制 应设计并实施在安全区域工作的安全措施
7.7	清理桌面和屏幕	控制 应定义并适当地执行纸质和可移动存储媒体的桌面清理规则和信息处理设施的屏幕清理规则
7.8	设备安置和保护	控制 应安全地安置并保护设备
7.9	组织场所外的资产安全	控制 应保护组织场所外的资产
7.10	存储媒体	控制 存储媒体应在其获取、使用、运输和处置的整个生存周期内，按照组织的分级方案和处理要求进行管理
7.11	支持性设施	控制 应保护信息处理设施使其免于由支持性设施的故障而引起的电源故障和其他中断
7.12	布缆安全	控制 应保护传输电力、数据或支持信息服务的电缆免受窃听、干扰或损坏
7.13	设备维护	控制 设备应予以正确的维护，以确保信息的可用性、完整性和保密性
7.14	设备的安全处置或重复使用	控制 应对包含存储媒体的设备的所有部分进行核查，以确保在处置或重复使用之前，任何敏感数据和获得许可的软件已被删除或安全地覆写
8	技术控制	
8.1	用户终端设备	控制 应保护用户终端设备所存储或处理的，或通过其访问的信息
8.2	特许访问权限	控制 应限制和管理特许访问权限的分配和使用
8.3	信息访问限制	控制 应按照已建立的访问控制特定主题策略，限制对信息及其他相关资产的访问
8.4	源代码的访问	控制 应对源代码、开发工具和软件库的读写访问进行适当的管理
8.5	安全鉴别	控制 应根据信息访问限制和访问控制的特定主题策略实施安全的鉴别技术和规程
8.6	容量管理	控制 应根据当前和预期的容量需求，监视和调整资源的使用
8.7	恶意软件防范	控制 应实施恶意软件防范，并通过适当的用户意识教育予以支持
8.8	技术脆弱性管理	控制

		应获取有关使用中的信息系统的技术脆弱性的信息，评价组织暴露于此类脆弱性的风险，并采取适当措施
8.9	配置管理	控制 应建立、记录、实施、监视和评审硬件、软件、服务和网络的配置，包括安全配置
8.10	信息删除	控制 当不再需要时，应删除存储在信息系统、设备或任何其他存储媒体中的信息
8.11	数据脱敏	控制 应根据组织关于访问控制的特定主题策略和其他相关的特定主题策略以及业务要求使用数据脱敏，并考虑到适用的法律法规
8.12	数据防泄露	控制 数据防泄露措施应用于处理、存储或传输敏感信息的系统、网络 and 任何其他设备
8.13	信息备份	控制 信息、软件和系统的备份副本应按照商定的备份特定主题策略进行维护和定期测试
8.14	信息处理设施的冗余	控制 信息处理设施应具有足够的冗余以满足可用性要求
8.15	日志	控制 应生成、存储、保护和分析用于记录活动、异常、故障及其他相关事态的日志
8.16	监视活动	控制 应监视网络、系统和应用程序，以发现异常行为，并采取适当措施评价潜在的信息安全事件
8.17	时钟同步	控制 组织使用的信息处理系统的时钟应与批准的时间源同步
8.18	特权实用程序的使用	控制 应限制并严格控制可能超越系统和应用程序控制的实用程序的使用
8.19	运行系统软件的安装	控制 应实施规程和措施以安全地管理运行系统上的软件安装
8.20	网络安全	控制 应保护、管理和控制网络和网络设备以保护系统和应用程序中的信息
8.21	网络服务的安全	控制 应识别、实施和监视网络服务的安全机制、服务级别和服务要求
8.22	网络隔离	控制 应在组织的网络中隔离信息服务组、用户组和信息系统组
8.23	网页过滤	控制 应管理对外部网站的访问，以减少对恶意内容的暴露
8.24	密码技术的使用	控制 应定义并实施有效使用密码技术的规则，包括密钥管理
8.25	安全开发生存周期	控制 应建立并应用软件和系统安全开发规则
8.26	应用程序安全要求	控制 在开发或获取应用程序时，应识别、规定和批准信息安全要求
8.27	系统安全架构和工程原则	控制 应建立、文件化、维护系统安全工程的原则，并将其应用于所有的信息系统开发活动
8.28	安全编码	控制 软件开发中应应用安全编码原则
8.29	开发和验收中的安全测试	控制 应在开发生存周期中定义和实施安全测试过程
8.30	开发外包	控制 组织应指导、监视和评审系统开发外包相关的活动
8.31	开发、测试和生产环境的隔离	控制 应隔离并保护开发、测试和生产环境
8.32	变更管理	控制 信息处理设施和信息系统的变更应遵从变更管理规程
8.33	测试信息	控制 应适当地选择、保护和管理测试信息
8.34	在审计测试中保护信息系统	控制 应对涉及运行系统评估的审计测试和其他保障活动进行规划，并在测试人员和适合的管理人员之间达成一致

附录B

(规范性附录)

云服务信息安全 控制集

1 范围

本附录为云服务的提供与使用提供适用的信息安全控制规范，具体包括：

- 对ISO/IEC 27002 中相关控制措施的补充实施规范；
 - 针对云服务的新增控制措施及实施规范。
- 本附录同时面向云服务提供商与云服务客户，提供控制措施与实施规范。

2 规范性引用文件

下列标准与文件通过引用构成本附录的条款。发布时所列版本有效，所有标准均会修订，鼓励使用最新版本。

2.1 等同标准

ISO/IEC 17788：信息技术 云计算 概述与词汇
ISO/IEC 17789：信息技术 云计算 参考架构

2.2 其他引用

ISO/IEC 27000：信息技术 安全技术 信息安全管理体系 概述与词汇
ISO/IEC 27002：信息技术 安全技术 信息安全控制实施规范

3 术语和缩略语

3.1 术语

除 ISO/IEC 27000、ITU-T Y.3500/ISO/IEC 17788、ITU-T Y.3502/ISO/IEC 17789 外，本附录采用以下术语：

3.1.1 下列术语源自 ISO 19440：

能力 (capability)：能够执行特定活动的特性。

3.1.2 下列术语源自 ISO/IEC 27040：

• **数据泄露 (data breach)**：指安全性受损，导致受保护数据（在传输、存储或其他处理过程中）被意外或非法破坏、丢失、篡改、未经授权披露或访问的情况。

• **安全多租户 (secure multi-tenancy)**：一种多租户模式，通过实施安全控制明确防范数据泄露，并对这些控制进行验证以确保合规治理。

• 注 1：当单个租户的风险状况不高于其在专用单租户环境中的风险状况时，即存在安全多租户。

• 注 2：在高度安全的环境中，甚至租户的身份也需保密。

3.1.3 下列术语源自 ISO/IEC 17203：

虚拟机 (virtual machine, VM)：支持客户软件执行的完整环境。

注：虚拟机是对虚拟硬件、虚拟磁盘及其相关元数据的完整封装。通过名为“虚拟机监控程序（hypervisor）”的软件层，虚拟机可实现对底层物理机资源的多路复用。

3.2 缩略语

IaaS：基础设施即服务

PaaS：平台即服务

PII：个人可识别信息

SaaS：软件即服务

SLA：服务等级协议

VM：虚拟机

4 云领域特定概念

4.1 概述

云计算的使用，改变了组织评估与缓解信息安全风险的方式，原因是计算资源在技术设计、运行与治理方式上发生了显著变化。本推荐性标准 | 国际标准基于 ISO/IEC 27002，提供云专属补充实施指南，并提供新增控制措施，以应对云特有信息安全威胁与风险考量。

本推荐性标准 | 国际标准的使用者应参考 ISO/IEC 27002 第 5 至 18 章的控制措施、实施指南及其他信息。由于 ISO/IEC 27002 具有通用性，其多数控制措施、实施指南及其他信息同时适用于组织的常规环境与云计算环境。例如，ISO/IEC 27002 的“6.1.2 职责分离”控制措施，无论组织是否作为云服务提供商，均可适用。此外，云服务客户可从同一控制措施中推导出云环境下的职责分离要求，例如分离云服务客户的云服务管理员与云服务用户。

作为 ISO/IEC 27002 的扩展，本推荐性标准 | 国际标准进一步提供云服务专属控制措施、实施指南及其他信息（见 4.5 节），旨在缓解伴随云服务技术与运行特性而来的风险（见附录 B）。云服务客户与云服务提供商可参考 ISO/IEC 27002 与本推荐性标准 | 国际标准，选择带实施指南的控制措施，并在必要时增加其他控制措施。该过程可在使用或提供云服务的组织与业务场景下，通过开展信息安全风险评估与风险处置完成（见 4.4 节）。

4.2 云服务中的供应商关系

ISO/IEC 27002 第 15 章“供应商关系”为管理供应商关系中的信息安全提供控制措施、实施指南及其他信息。云服务的提供与使用属于一类供应商关系，其中云服务客户为采购方，云服务提供商为供应商。因此，该章节适用于云服务客户与云服务提供商。

云服务客户与云服务提供商可形成供应链。假设某云服务提供商提供基础设施能力类服务，另一云服务提供商提供应用能力类服务。在此情形下，第二家云服务提供商相对于第一家而言是云服务客户，相对于使用其服务的云服务客户而言是云服务提供商。该示例说明本推荐性标准 | 国际标准可同时适用于兼具云服务客户与云服务提供商身份的组织。由于云服务客户与云服务提供商通过云服务的设计与实施形成供应链，ISO/IEC 27002 的“15.1.3 信息通信技术供应链”条款适用。

多部分标准 ISO/IEC 27036《供应商关系信息安全》为产品与服务的采购方及供应商提供供应商关系信息安全的详细指南。ISO/IEC 27036 第 4 部分直接针对供应商关系中的云服务安全。该标准同样适用于作为采购方的云服务客户与作为供应商的云服务提供商。

4.3 云服务客户与云服务提供商的关系

在云计算环境中，云服务客户的数据由云服务存储、传输与处理。因此，云服务客户的业务流程可能依赖云服务的信息安全。若对云服务缺乏足够控制，云服务客户可能需要在自身信息安全实践中采取额外预防措施。

在建立供应商关系前，云服务客户需选择云服务，同时考虑自身信息安全要求与服务所提供信息安全能力之间可能存在的差距。选定云服务后，云服务客户应以满足自身信息安全要求的方式管理云服务的使用。在此关系中，云服务提供商应提供满足云服务客户信息安全要求所需的信息与技术支持。当云服务提供商提供的信息安全控制为预设且无法由云服务客户更改时，云服务客户可能需要自行实施额外控制措施以缓解风险。

4.4 云服务中的信息安全风险管理

云服务客户与云服务提供商均应建立信息安全风险管理流程。建议双方参考 ISO/IEC 27001 中关于在信息安全管理体系中开展风险管理的要求，并参考 ISO/IEC 27005 获取信息安全风险管理的进一步指南。ISO/IEC 27001 与 ISO/IEC 27005 所遵循的 ISO 31000，也有助于理解通用风险管理。

与信息安全风险管理流程的通用性不同，云计算具有自身特有的风险来源，包括威胁与脆弱性，这些风险来源于其特性，例如：网络、系统可扩展性与弹性、资源共享、自助服务开通、按需管理、跨司法辖区服务提供、控制措施实施可见性有限等。附录 B 提供相关参考资料，说明云服务提供与使用中的这些风险来源及相关风险。

本推荐性标准 | 国际标准第 5 至 18 章及附录 A 给出的控制措施与实施指南，针对云计算特有的风险来源与风险。

4.5 标准结构

本推荐性标准 | 国际标准采用与 ISO/IEC 27002 相似的结构。本推荐性标准 | 国际标准在各条款与段落中说明适用性，从而纳入 ISO/IEC 27002 第 5 至 18 章。

- 当 ISO/IEC 27002 规定的目标与控制措施无需补充信息即可适用时，仅提供对 ISO/IEC 27002 的引用。

- 当需要在 ISO/IEC 27002 之外增加某目标及控制措施，或某目标下的控制措施时，在规范性附录 A：云服务扩展控制集中给出。

- 当 ISO/IEC 27002 的控制措施或本推荐性标准 | 国际标准附录 A 的控制措施需要与该控制措施相关的云服务专属补充实施指南时，在副标题云服务实施指南下给出。

指南分为以下两类：

类型 1：云服务客户与云服务提供商分别给出指南

云服务客户	云服务提供商

类型 2：云服务客户与云服务提供商共用指南

云服务客户	云服务提供商

5 信息安全方针

5.1 信息安全管理方向

适用 ISO/IEC 27002 第 5.1 条规定的目标。

5.1.1 信息安全方针

适用 ISO/IEC 27002 标准中控制措施 5.1.1 及其实施指南与其他信息。同时下述专用指南适用：

云服务实施规范

云服务客户	云服务提供商
云计算信息安全方针应被定义为云服务客户的一项专项方针。云服务客户的云计算信息安全方针，	云服务提供商应扩充其信息安全方针，以覆盖其云服务的提供与使用，并需考虑以下因素：

应与组织对其信息及其他资产所设定的可接受信息安全风险等级保持一致。 在制定云计算信息安全方针时，云服务客户应考虑以下因素： - 存储在云计算环境中的信息，可能会被云服务提供商访问和管理； - 资产（例如应用程序）可能会在云计算环境中维护； - 业务流程可能在多租户、虚拟化的云服务上运行； - 云服务用户及其使用云服务的场景； - 拥有特权访问权限的云服务客户方云服务管理员； - 云服务提供商所在的组织地理位置，以及云服务提供商可（即使是临时）存储云服务客户数据的国家 / 地区	- 适用于云服务设计与实施的基线信息安全要求； - 授权内部人员带来的风险； - 多租户与云服务客户隔离（含虚拟化）； - 云服务提供商员工对云服务客户资产的访问； - 访问控制程序，例如云服务管理访问的强认证； - 变更管理期间与云服务客户的沟通； - 虚拟化安全； - 云服务客户数据的访问与保护； - 云服务客户账户的生命周期管理； - 向客户通报安全事件的流程，以及协助调查与取证的信息共享指南
---	--

其他与云服务有关的信息

云服务客户的云计算信息安全方针属于 ISO/IEC 27002 5.1.1 所述专项方针之一。组织的信息安全方针规范其信息与业务流程。当组织使用云服务时，可作为云服务客户制定云计算专项方针。组织信息可存储与维护在云计算环境中，业务流程可在云计算环境中运行。顶层信息安全方针所述通用安全要求由云计算方针承接。

与之相对，提供云服务的信息安全方针规范云服务客户的信息与业务流程，而非云服务提供商自身的信息与业务流程。云服务提供的安全要求应满足潜在客户的要求，因此可能与提供商自身信息与业务流程的安全要求不一致。安全方针范围通常按服务界定，而非仅按组织结构或物理位置界定。

云计算虚拟化安全包含多个方面，包括虚拟实例生命周期管理、虚拟化镜像存储与访问控制、休眠 / 离线虚拟实例处理、快照、虚拟机管理程序保护、管控自助门户使用的安全控制等。

5.1.2 信息安全方针评审

适用 ISO/IEC 27002 标准中控制措施 5.1.2 及其实施指南与其他信息。

6 信息安全组织

6.1 内部组织

适用 ISO/IEC 27002 第 6.1 条规定的目标。

6.1.1 信息安全角色与职责

适用 ISO/IEC 27002 标准中控制措施 6.1.1 及其实施指南与其他信息。同时下述专用指南适用：

云服务实施规范

云服务客户	云服务提供商
云服务客户应与云服务提供商就信息安全角色与职责的合理分配达成一致，并确认自身能够履行所分配的角色与职责。双方的信息安全角色与职责应在协议中予以明确。 云服务客户应识别并维护与云服务提供商客户支持及服务关怀部门的关系。	云服务提供商应与云服务客户、其上游云服务提供商及自身供应商，就信息安全角色与职责的合理分配达成一致并形成书面记录。

其他与云服务有关的信息

即便各方内部及各方之间已明确责任划分，云服务客户仍需对使用该服务的决策承担最终责任。该决策应依据客户组织内部已确定的角色与职责作出。云服务提供商则需对云服务协议中约定的信息安全要求负责，其信息安全的实施与交付工作，也应遵循提供商组织内部的角色与职责划分开展。

在数据所有权、访问控制、基础设施维护等事项上，角色界定不清、责任定义与分配模糊，极易引发业务纠纷或法律争议，涉及第三方时风险尤为突出。

在云服务使用过程中创建或修改的、存储于提供商系统内的数据与文件，对服务的安全运行、灾难恢复与业务连续性至关重要。因此，所有资产的所有权归属，以及备份恢复等关键操作的责任方，均需明确定义并形成书面文档。否则，可能出现“提供商默认由客户执行这些关键任务（反之亦然）”的责任真空，进而导致数据丢失风险。

6.1.2 职责分离

适用 ISO/IEC 27002 标准中控制措施 6.1.2 及其实施指南与其他信息。

6.1.3 与主管部门的联系

适用 ISO/IEC 27002 标准中控制措施 6.1.3 及其实施指南与其他信息。同时下述专用指南适用：

云服务实施规范

云服务客户	云服务提供商
云服务客户应识别与云服务客户和云服务提供商联合运营相关的主管部门。	云服务提供商应向云服务客户告知其组织的地理位置，以及可存储云服务客户数据的国家 / 地区。

其他与云服务有关的信息

关于云服务客户数据可存储、处理或传输的地理位置信息，可帮助云服务客户确定监管机构与司法管辖区域。

6.1.4 与特殊利益相关方的联系

适用 ISO/IEC 27002 标准中控制措施 6.1.4 及其实施指南与其他信息。

6.1.5 项目管理中的信息安全

适用 ISO/IEC 27002 标准中控制措施 6.1.5 及其实施指南与其他信息。

6.2 移动设备与远程办公

适用 ISO/IEC 27002 第 6.2 条规定的目标。

6.2.1 移动设备策略

适用 ISO/IEC 27002 标准中控制措施 6.2.1 及其实施指南与其他信息。

6.2.2 远程办公

适用 ISO/IEC 27002 标准中控制措施 6.2.2 及其实施指南与其他信息。

7 人力资源安全

7.1 聘用前

适用 ISO/IEC 27002 第 7.1 条规定的目标。

7.1.1 背景审查

适用 ISO/IEC 27002 标准中控制措施 7.1.1 及其实施指南与其他信息。

7.1.2 聘用条款与条件

适用 ISO/IEC 27002 标准中控制措施 7.1.2 及其实施指南与其他信息。

7.2 聘用期间

适用 ISO/IEC 27002 第 7.2 条规定的目标。

7.2.1 管理职责

适用 ISO/IEC 27002 标准中控制措施 7.2.1 及其实施指南与其他信息。

7.2.2 信息安全意识、教育与培训

适用 ISO/IEC 27002 标准中控制措施 7.2.2 及其实施指南与其他信息。同时下述专用指南适用：

云服务实施规范

云服务客户	云服务提供商
云服务客户应在面向云服务业务管理人员、云服务管理员、云服务集成人员和云服务用户（包括相关员工与承包商）的意识、教育与培训计划中，补充以下内容： - 云服务使用标准与流程； - 与云服务相关的信息安全风险及其管理方式； - 使用云服务带来的系统与网络环境风险； - 适用的法律法规与监管要求。 应向管理层及主管经理（包括业务单元管理人员）提供云服务相关的信息安全意识、教育与培训计划，以支持信息安全活动的有效协调。	云服务提供商应为员工提供关于云服务客户数据及云服务衍生数据妥善处理意识、教育与培训，并要求承包商也开展同类培训。此类数据可能包含云服务客户的保密信息，或受到访问和使用方面的特定限制（包括监管约束）。

7.2.3 纪律处理流程

适用 ISO/IEC 27002 标准中控制措施 7.2.3 及其实施指南与其他信息。

7.3 内部组织

适用 ISO/IEC 27002 第 7.3 条规定的目标。

7.3.1 聘用终止与岗位变更

适用 ISO/IEC 27002 标准中控制措施 7.3.1 及其实施指南与其他信息。

8 资产管理

8.1 资产责任

适用 ISO/IEC 27002 第 8.1 条规定的目标。

8.1.1 资产清单

适用 ISO/IEC 27002 标准中控制措施 8.1.1 及其实施指南与其他信息。

云服务实施规范

云服务客户	云服务提供商
云服务客户的资产清单，应记录存储在云计算环境中的信息及相关资产。清单记录应标明资产的维护位置，例如：云服务的标识。	云服务提供商的资产清单，应明确识别： - 云服务客户数据； - 云服务衍生数据。

其他与云服务有关的信息

部分云服务应用可通过向云服务客户数据中添加云服务衍生数据，提供信息管理功能。将此类云服务衍生数据识别为资产并纳入资产清单，有助于提升信息安全水平。

8.1.2 资产所有权

适用 ISO/IEC 27002 标准中控制措施 8.1.2 及其实施指南与其他信息。

其他与云服务有关的信息

资产所有权可能因所使用的云服务类别而异：使用平台即服务（PaaS）或基础设施即服务（IaaS）时，应用软件的所有权属于云服务客户；而使用软件即服务（SaaS）时，应用软件的所有权属于云服务提供商。

8.1.3 资产的可接受使用

适用 ISO/IEC 27002 标准中控制措施 8.1.3 及其实施指南与其他信息。

8.1.4 资产归还

适用 ISO/IEC 27002 标准中控制措施 8.1.4 及其实施指南与其他信息。同时下述专用指南适用：

8.2 信息分类

适用 ISO/IEC 27002 第 8.2 条规定的目标。

8.2.1 信息的分类

适用 ISO/IEC 27002 标准中控制措施 8.2.1 及其实施指南与其他信息。

8.2.2 信息的标识

适用 ISO/IEC 27002 标准中控制措施 8.2.2 及其实施指南与其他信息。同时下述专用指南适用：

云服务实施规范

云服务客户	云服务提供商
云服务客户应根据其采用的标识流程，对维护在云计算环境中的信息及相关资产进行标识。适用时，	云服务提供商应记录并披露其提供的、允许云服务客户对其信息及相关资产进行分类与标示的任

可采用云服务提供商提供的支持标识功能。	何服务功能。
---------------------	--------

8.2.3 资产处置

适用 ISO/IEC 27002 标准中控制措施 8.2.3 及其实施指南与其他信息。

8.3 介质处理

适用 ISO/IEC 27002 第 8.3 条规定的目标。

8.3.1 可移动介质的管理

适用 ISO/IEC 27002 标准中控制措施 8.3.1 及其实施指南与其他信息。

8.3.2 介质处置

适用 ISO/IEC 27002 标准中控制措施 8.3.2 及其实施指南与其他信息。

8.3.3 物理介质的转移

适用 ISO/IEC 27002 标准中控制措施 8.3.3 及其实施指南与其他信息。

9 访问控制

9.1 访问控制的业务要求

适用 ISO/IEC 27002 第 9.1 条规定的目标。

9.1.1 访问控制策略

适用 ISO/IEC 27002 标准中控制措施 9.1.1 及其实施指南与其他信息。

9.1.2 网络与网络服务访问

适用 ISO/IEC 27002 标准中控制措施 9.1.2 及其实施指南与其他信息。同时下述专用指南适用：

云服务实施规范

云服务客户	云服务提供商
云服务客户针对网络服务使用的访问控制策略，应规定用户对所使用的每项独立云服务的访问要求。	（无额外实施指南）

9.2 用户访问管理

适用 ISO/IEC 27002 第 9.2 条规定的目标。

9.2.1 用户注册与注销

适用 ISO/IEC 27002 标准中控制措施 9.2.1 及其实施指南与其他信息。同时下述专用指南适用：

云服务实施规范

云服务客户	云服务提供商
（无额外实施指南）	为管理云服务客户用户对云服务的访问，云服务提供商应提供用户注册与注销功能，并向云服务

	客户提供这些功能的使用说明。
--	----------------

9.2.2 用户访问权限配置

适用 ISO/IEC 27002 标准中控制措施 9.2.2 及其实施指南与其他信息。同时下述专用指南适用：

云服务实施规范

云服务客户	云服务提供商
(无额外实施指南)	云服务提供商应提供管理云服务客户用户访问权限的功能，并提供这些功能的使用说明。

其他与云服务有关的信息

云服务提供商应在其云服务及相关管理接口中支持第三方身份与访问管理技术。此类技术可简化云服务客户系统与云服务之间的集成及用户身份管理，并支持单点登录等能力，方便用户使用多项云服务。

9.2.3 特权访问权限管理

适用 ISO/IEC 27002 标准中控制措施 9.2.3 及其实施指南与其他信息。同时下述专用指南适用：

云服务实施规范

云服务客户	云服务提供商
云服务客户应根据识别出的风险，使用足够的身份验证技术（例如多因素身份验证）对云服务管理员访问云服务管理功能进行身份验证。	云服务提供商应根据识别出的风险，提供足够的身份验证技术，对云服务客户的管理员访问云服务管理功能进行身份验证。例如，云服务提供商可提供多因素身份验证功能，或支持使用第三方多因素身份验证机制。

9.2.4 用户的秘密鉴别信息管理

适用 ISO/IEC 27002 标准中控制措施 9.2.4 及其实施指南与其他信息。同时下述专用指南适用：

云服务实施规范

云服务客户	云服务提供商
云服务客户应验证云服务提供商分配秘密身份验证信息（如密码）的管理流程是否满足云服务客户的要求。	云服务提供商应提供关于管理云服务客户秘密身份验证信息的流程说明，包括此类信息的分配流程及用户身份验证流程。

其他与云服务有关的信息

云服务客户可通过使用自有或第三方身份与访问管理技术，控制秘密身份验证信息的管理。

9.2.5 用户访问权限评审

适用 ISO/IEC 27002 标准中控制措施 9.2.5 及其实施指南与其他信息。

9.2.6 访问权限的移除或调整

适用 ISO/IEC 27002 标准中控制措施 9.2.6 及其实施指南与其他信息。

9.3 用户责任

适用 ISO/IEC 27002 第 9.3 条规定的目标。

9.3.1 秘密鉴别信息的使用

适用 ISO/IEC 27002 标准中控制措施 9.3.1 及其实施指南与其他信息。

9.4 系统和应用访问控制

适用 ISO/IEC 27002 第 9.4 条规定的目标。

9.4.1 信息访问限制

适用 ISO/IEC 27002 标准中控制措施 9.4.1 及其实施指南与其他信息。同时下述专用指南适用：

云服务实施规范

云服务客户	云服务提供商
若允许使用实用程序，云服务客户应识别其在云计算环境中使用的实用程序，并确保其不会干扰云服务的控制措施。	云服务提供商应提供访问控制机制，允许云服务客户限制对其云服务、云服务功能及服务中存储的云服务客户数据的访问。

其他与云服务有关的信息

云计算环境包含额外需要访问控制的领域。作为云服务或云服务功能的一部分，对功能和服务（如虚拟机管理功能和管理控制台）的访问可能需要额外的访问控制。

9.4.2 安全登录规程

适用 ISO/IEC 27002 标准中控制措施 9.4.2 及其实施指南与其他信息。

9.4.3 口令管理系统

适用 ISO/IEC 27002 标准中控制措施 9.4.3 及其实施指南与其他信息。

9.4.4 特权实用程序的使用

适用 ISO/IEC 27002 标准中控制措施 9.4.4 及其实施指南与其他信息。同时下述专用指南适用：

云服务实施规范

云服务客户	云服务提供商
云服务客户应根据识别出的风险，使用足够的身份验证技术（例如多因素身份验证）对云服务管理员访问云服务管理功能进行身份验证。	云服务提供商应识别云服务内部使用的所有实用程序的使用要求。云服务提供商应确保：任何能够绕过正常操作或安全流程的实用程序的使用，严格限于授权人员；此类程序的使用定期接受评审与审计。

9.4.5 程序源代码的访问控制

适用 ISO/IEC 27002 标准中控制措施 9.4.5 及其实施指南与其他信息。

10 密码学

10.1 密码控制

适用 ISO/IEC 27002 第 9.3 条规定的目标。

10.1.1 密码控制的使用策略

适用 ISO/IEC 27002 标准中控制措施 10.1.1 及其实施指南与其他信息。同时下述专用指南适用：

云服务实施规范

云服务客户	云服务提供商
云服务客户在风险分析表明有必要时，应针对云服务的使用实施密码控制措施。控制措施应具备足够强度，以缓解已识别风险，无论这些控制措施由云服务客户还是云服务提供商提供。 当云服务提供商提供密码学相关能力时，云服务客户应审查其提供的信息，确认相关密码能力是否： - 符合云服务客户的策略要求； - 与云服务客户使用的其他任何密码保护措施兼容； - 适用于云服务中静态数据、传输至云服务的数据、从云服务传出的数据及云服务内部的数据。	云服务提供商应向云服务客户提供信息，说明其在处理信息时使用密码学保护信息的场景。 云服务提供商还应向云服务客户提供信息，说明其提供的可协助云服务客户自行实施密码保护的能力。

其他与云服务有关的信息

在部分司法管辖区，可能要求使用密码学保护特定类型的信息，例如健康数据、居民身份证号码、护照号码和驾驶证号码。

10.1.2 密钥管理

适用 ISO/IEC 27002 标准中控制措施 10.1.2 及其实施指南与其他信息。同时下述专用指南适用：

云服务实施规范

云服务客户	云服务提供商
云服务客户应为每项云服务识别所需的密钥，并实施密钥管理流程。 当云服务提供商提供可供云服务客户使用的密钥管理功能时，云服务客户应请求获取与云服务相关的密钥管理流程的以下信息： - 密钥类型； - 密钥管理系统的规范，包括密钥生命周期各阶段（即生成、变更或更新、存储、停用、检索、保留和销毁）的流程； - 供云服务客户使用的推荐密钥管理流程。 当云服务客户使用自有密钥管理系统或独立的密钥管理服务时，不应允许云服务提供商存储和管理用于密码操作的加密密钥。	（无额外实施指南）

11 物理和环境安全

11.1 安全区域

适用 ISO/IEC 27002 第 11.1 条规定的目标。

11.1.1 物理安全边界

适用 ISO/IEC 27002 标准中控制措施 11.1.1 及其实施指南与其他信息。

11.1.2 物理入口控制

适用 ISO/IEC 27002 标准中控制措施 11.1.2 及其实施指南与其他信息。

11.1.3 办公室、房间和设施的安全保护

适用 ISO/IEC 27002 标准中控制措施 11.1.3 及其实施指南与其他信息。

11.1.4 外部和环境威胁的安全防护

适用 ISO/IEC 27002 标准中控制措施 11.1.4 及其实施指南与其他信息。

11.1.5 在安全区域工作

适用 ISO/IEC 27002 标准中控制措施 11.1.5 及其实施指南与其他信息。

11.1.6 交接区

适用 ISO/IEC 27002 标准中控制措施 11.1.6 及其实施指南与其他信息。

11.2 设备

适用 ISO/IEC 27002 第 11.2 条规定的目标。

11.2.1 设备安置和保护

适用 ISO/IEC 27002 标准中控制措施 12.2.1 及其实施指南与其他信息。

11.2.2 支持性设施

适用 ISO/IEC 27002 标准中控制措施 12.2.2 及其实施指南与其他信息。

11.2.3 布缆支全

适用 ISO/IEC 27002 标准中控制措施 12.2.3 及其实施指南与其他信息。

11.2.4 设备维护

适用 ISO/IEC 27002 标准中控制措施 12.2.4 及其实施指南与其他信息。

11.2.5 资产的移动

适用 ISO/IEC 27002 标准中控制措施 12.2.5 及其实施指南与其他信息。

11.2.6 组织场所外的设备与资产安全

适用 ISO/IEC 27002 标准中控制措施 12.2.6 及其实施指南与其他信息。

11.2.7 设备的安全处置或再利用

适用 ISO/IEC 27002 标准中控制措施 12.2.7 及其实施指南与其他信息。同时下述专用指南适用：
云服务实施规范

云服务客户	云服务提供商
云服务客户应要求云服务提供商确认其具备资源安全处置或复用的策略与流程。	云服务提供商应确保制定资源（例如设备、数据存储介质、文件、内存）安全处置或及时复用的相关安排。

其他与云服务有关的信息

关于安全处置的更多信息可参考 ISO/IEC 27040 标准。

11.2.8 无人值守的用户设备

适用 ISO/IEC 27002 标准中控制措施 12.2.8 及其实施指南与其他信息。

11.2.9 清理桌面和屏幕策略

适用 ISO/IEC 27002 标准中控制措施 12.2.9 及其实施指南与其他信息。

12 运行安全

12.1 运行规程和责任

适用 ISO/IEC 27002 第 12.1 条规定的目标。

12.1.1 文件化的操作规程

适用 ISO/IEC 27002 标准中控制措施 12.1.1 及其实施指南与其他信息。

12.1.2 变更管理

适用 ISO/IEC 27002 标准中控制措施 12.1.2 及其实施指南与其他信息。同时下述专用指南适用：

云服务实施规范

云服务客户	云服务提供商
云服务客户的变更管理流程，应考虑云服务提供商实施的任何变更带来的影响。	云服务提供商应向云服务客户提供可能对云服务造成不利影响的变更信息。以下信息可帮助云服务客户确定变更对信息安全的影响： – 变更类别； – 变更的计划日期与时间； – 对云服务及底层系统的变更技术说明； – 变更启动与完成的通知。 若云服务提供商提供的云服务依赖于同级云服务提供商，则该云服务提供商可能需要将同级云服务提供商导致的变更告知云服务客户。

其他与云服务有关的信息

通知中应包含的事项清单可在协议（如主服务协议或服务水平协议 SLA）中明确约定。

12.1.3 容量管理

适用 ISO/IEC 27002 标准中控制措施 12.1.3 及其实施指南与其他信息。同时下述专用指南适用：

云服务实施规范

云服务客户	云服务提供商
云服务客户应确保云服务提供商提供的约定容量满足自身需求。	云服务提供商应监控总资源容量，防止因资源短缺引发信息安全事件。

云服务客户应监控云服务的使用情况，并预测容量需求，以确保云服务的长期性能。

其他与云服务有关的信息

云服务涉及云服务提供商控制、并根据主服务协议及相关 SLA 提供给云服务客户的资源，包括软件、处理硬件、数据存储和网络连接。

云服务中资源的弹性、可扩展和按需分配特性通常会提升服务的总容量。但云服务客户应了解，提供的资源可能存在容量限制。例如：应用的处理器核心数量、可用存储量、可用网络带宽。

限制条件可能因云服务客户购买的特定云服务或订阅方案而异。若云服务客户的需求超出限制，可能需要更换云服务或变更订阅方案。

为对云服务实施容量管理，云服务客户应获取资源使用的相关统计数据，例如：

- 特定时间段的统计数据；
- 资源使用的最高水平。

12.1.4 开发、测试和运行环境的分离

适用 ISO/IEC 27002 标准中控制措施 12.1.4 及其实施指南与其他信息。

12.2 恶意软件防范

适用 ISO/IEC 27002 第 12.2 条规定的目标。

12.2.1 恶意软件的控制

适用 ISO/IEC 27002 标准中控制措施 12.2.1 及其实施指南与其他信息。

12.3 备份

适用 ISO/IEC 27002 第 12.3 条规定的目标。

12.3.1 信息备份

适用 ISO/IEC 27002 标准中控制措施 12.1.3 及其实施指南与其他信息。同时下述专用指南适用：

云服务实施规范

云服务客户	云服务提供商
若云服务提供商提供备份功能，云服务客户应向其请求备份功能的规格说明，并验证该功能是否满足自身备份需求。 若云服务提供商不提供备份功能，云服务客户应自行实施备份功能。	云服务提供商应向云服务客户提供其备份功能的规格说明。规格说明应根据情况包含以下信息： - 备份的范围与计划； - 备份方法与数据格式（含加密，如适用）； - 备份数据的保留期限； - 验证备份数据完整性的流程； - 从备份恢复数据的流程与时间要求； - 测试备份功能的流程； - 备份的存储位置。 云服务提供商应提供安全、隔离的备份访问方式（如虚拟快照），若向云服务客户提供此类服务。

其他与云服务有关的信息

云计算环境中备份职责的划分往往不明确。在 IaaS 模式下，备份职责通常由云服务客户承担。但云服务客户可能未意识到，其使用 PaaS 服务的开发功能生成的所有云服务客户数据，均需自行备份。

注：备份与恢复服务可能以额外费用的形式提供不同等级的服务，此时云服务客户可

自行选择备份的内容与时间。

12.4 日志和监视

适用 ISO/IEC 27002 第 12.4 条规定的目标。

12.4.1 事态日志

适用 ISO/IEC 27002 标准中控制措施 12.4.1 及其实施指南与其他信息。同时下述专用指南适用：

云服务实施规范

云服务客户	云服务提供商
云服务客户应明确事件日志要求，并验证云服务提供商是否满足这些要求。	云服务提供商应向云服务客户提供日志功能。

其他与云服务有关的信息

云服务客户与云服务提供商在事件日志方面的职责，取决于所使用的云服务类型。例如：在 IaaS 模式下，云服务提供商的日志职责可能仅限于云计算基础设施组件，而云服务客户需负责记录其自身虚拟机和应用程序的事件。。

12.4.2 日志信息的保护

适用 ISO/IEC 27002 标准中控制措施 12.4.2 及其实施指南与其他信息。

12.4.3 管理员和操作员日志

适用 ISO/IEC 27002 标准中控制措施 12.4.3 及其实施指南与其他信息。同时下述专用指南适用：

云服务实施规范

云服务客户	云服务提供商
若特权操作委托给云服务客户，应对这些操作的执行情况进行日志记录。云服务客户应确定云服务提供商提供的日志功能是否适用，或是否需要自行实施额外的日志功能。	（无额外实施指南）

其他与云服务有关的信息

云服务客户与云服务提供商之间的职责划分（见第 6.1.1 条）应涵盖与云服务相关的特权操作。监控和记录特权操作的使用情况，对于支持针对不当使用采取预防和纠正措施至关重要。

12.4.4 时钟同步

适用 ISO/IEC 27002 标准中控制措施 12.4.4 及其实施指南与其他信息。同时下述专用指南适用：

云服务实施规范

云服务客户	云服务提供商
云服务客户应请求获取云服务提供商系统所使用的时钟同步相关信息。	云服务提供商应向云服务客户提供其系统所使用的时钟的相关信息，以及云服务客户将本地时钟与云服务时钟同步的方法说明。

其他与云服务有关的信息

云计算环境中备份职责的划分往往不明确。在 IaaS 模式下，备份职责通常由云服务客户承担。但云服务客户可能未意识到，其使用 PaaS 服务的开发功能生成的所有云服务客户数据，均需自行备份。

注：备份与恢复服务可能以额外费用的形式提供不同等级的服务，此时云服务客户可自行选择备份的内容与时间。

12.5 运行软件控制

适用 ISO/IEC 27002 第 12.5 条规定的目标。

12.5.1 运行系统的软件安装

适用 ISO/IEC 27002 标准中控制措施 12.5.1 及其实施指南与其他信息。

12.6 技术方面的脆弱性管理

适用 ISO/IEC 27002 第 12.6 条规定的目标。

12.6.1 技术方面脆弱性的管理

适用 ISO/IEC 27002 标准中控制措施 12.6.1 及其实施指南与其他信息。同时下述专用指南适用：

云服务实施规范

云服务客户	云服务提供商
云服务客户应向云服务提供商请求获取影响所提供云服务的技术漏洞管理相关信息。云服务客户应识别需自行管理的技术漏洞，并明确管理流程。	云服务提供商应向云服务客户提供影响所提供云服务的技术漏洞管理相关信息。

12.6.2 软件安装限制

适用 ISO/IEC 27002 标准中控制措施 12.6.2 及其实施指南与其他信息。

12.7 信息系统审计的考虑

适用 ISO/IEC 27002 第 12.7 条规定的目标。

12.7.1 信息系统审计的控制

适用 ISO/IEC 27002 标准中控制措施 12.7.1 及其实施指南与其他信息。

13 通信安全

13.1 网络安全管理

适用 ISO/IEC 27002 第 13.1 条规定的目标。

13.1.1 网络控制

适用 ISO/IEC 27002 标准中控制措施 13.1.1 及其实施指南与其他信息。

13.1.2 网络服务的安全

适用 ISO/IEC 27002 标准中控制措施 13.1.2 及其实施指南与其他信息。

13.1.3 网络中的隔离

适用 ISO/IEC 27002 标准中控制措施 13.1.3 及其实施指南与其他信息。同时下述专用指南适用：

云服务实施规范

云服务客户	云服务提供商
云服务客户应定义网络隔离的相关要求，以在云服务共享环境中实现租户隔离，并验证云服务提供商是否满足这些要求。	云服务提供商应在以下场景中实施网络访问隔离： – 多租户环境下不同租户之间的隔离； – 云服务提供商内部管理环境与云服务客户云计算环境之间的隔离。 在适当情况下，云服务提供商应协助云服务客户验证其实施的隔离措施。

其他与云服务有关的信息

法律法规可能要求实施网络隔离或网络流量隔离。

13.2 信息传输

适用 ISO/IEC 27002 第 13.2 条规定的目标。

13.2.1 信息传输策略和规程

适用 ISO/IEC 27002 标准中控制措施 13.2.1 及其实施指南与其他信息。

13.2.2 信息传输协议

适用 ISO/IEC 27002 标准中控制措施 13.2.2 及其实施指南与其他信息。

13.2.3 电子消息发送

适用 ISO/IEC 27002 标准中控制措施 13.2.3 及其实施指南与其他信息。

13.2.4 保密或不泄露协议

适用 ISO/IEC 27002 标准中控制措施 13.2.4 及其实施指南与其他信息。

14 系统获取、开发和维护

14.1 信息系统的安全要求

适用 ISO/IEC 27002 第 14.1 条规定的目标。

14.1.1 信息安全要求分析和说明

适用 ISO/IEC 27002 标准中控制措施 14.1.1 及其实施指南与其他信息。同时下述专用指南适用：

云服务实施规范

云服务客户	云服务提供商
云服务客户应确定云服务的信息安全需求，然后评估云服务提供商提供的服务是否能满足这些需求。 为开展此项评估，云服务客户应向云服务提供商请求获取信息安全能力相关信息。	云服务提供商应向云服务客户提供其所使用的信息安全能力相关信息。此类信息应具有说明性，且不得披露可能被恶意方利用的信息。

其他与云服务有关的信息

应注意限制向已签署保密协议的云服务客户或潜在云服务客户披露与所提供云服务相关的安全控制实施细节。

14.1.2 公共网络上应用服务的安全保护

适用 ISO/IEC 27002 标准中控制措施 14.1.2 及其实施指南与其他信息。

14.1.3 应用服务事务的保护

适用 ISO/IEC 27002 标准中控制措施 14.1.3 及其实施指南与其他信息。

14.2 开发和支持过程中的安全

适用 ISO/IEC 27002 第 14.2 条规定的目标。

14.2.1 安全的开发策略

适用 ISO/IEC 27002 标准中控制措施 14.2.1 及其实施指南与其他信息。同时下述专用指南适用：

云服务实施规范

云服务客户	云服务提供商
云服务客户应向云服务提供商请求获取其安全开发流程与实践的使用情况相关信息。	云服务提供商应在符合其信息披露策略的前提下，提供其安全开发流程与实践的使用情况相关信息。

其他与云服务有关的信息

云服务提供商的安全开发流程与实践对软件即服务（SaaS）至关重要。

14.2.2 系统变更控制规程

适用 ISO/IEC 27002 标准中控制措施 14.2.2 及其实施指南与其他信息。

14.2.3 运行平台变更后对应用的技术评审

适用 ISO/IEC 27002 标准中控制措施 14.2.3 及其实施指南与其他信息。

14.2.4 软件包变更的限制

适用 ISO/IEC 27002 标准中控制措施 14.2.4 及其实施指南与其他信息。

14.2.5 系统安全工程原则

适用 ISO/IEC 27002 标准中控制措施 14.2.5 及其实施指南与其他信息。

14.2.6 安全的开发环境

适用 ISO/IEC 27002 标准中控制措施 14.2.6 及其实施指南与其他信息。

14.2.7 外包开发

适用 ISO/IEC 27002 标准中控制措施 14.2.7 及其实施指南与其他信息。

14.2.8 系统安全测试

适用 ISO/IEC 27002 标准中控制措施 14.2.8 及其实施指南与其他信息。

14.2.9 系统验收测试

适用 ISO/IEC 27002 标准中控制措施 14.2.9 及其实施指南与其他信息。

14.3 测试数据

适用 ISO/IEC 27002 第 14.3 条规定的目标。

14.3.1 测试数据的保护

适用 ISO/IEC 27002 标准中控制措施 14.3.1 及其实施指南与其他信息。

15 供应商关系

15.1 供应商关系中的信息安全

适用 ISO/IEC 27002 第 15.1 条规定的目标。

15.1.1 供应商关系的信息安全策略

适用 ISO/IEC 27002 标准中控制措施 15.1.1 及其实施指南与其他信息。同时下述专用指南适用：

云服务实施规范

云服务客户	云服务提供商
云服务客户应在其供应商关系信息安全策略中，将云服务提供商列为一类供应商。这有助于缓解与云服务提供商访问和管理云服务客户数据相关的风险。	（无额外实施指南）

15.1.2 在供应商协议中强调安全

适用 ISO/IEC 27002 标准中控制措施 15.1.2 及其实施指南与其他信息。同时下述专用指南适用：

云服务实施规范

云服务客户	云服务提供商
云服务客户应确认服务协议中描述的与云服务相关的信息安全角色与职责。这些可包括以下流程： – 恶意软件防护； – 备份； – 密码控制； – 漏洞管理； – 事件管理； – 技术合规检查； – 安全测试； – 审计； – 证据（包括日志和审计跟踪）的收集、维护与保护； – 服务协议终止时的信息保护； – 身份验证与访问控制；	云服务提供商应在协议中明确其将实施的相关信息安全措施，以确保与云服务客户之间不存在误解。 云服务提供商将实施的相关信息安全措施，可能因云服务客户使用的云服务类型而异。

- 身份与访问管理。

15.1.3 信息与通信技术供应链

适用 ISO/IEC 27002 标准中控制措施 15.1.3 及其实施指南与其他信息。同时下述专用指南适用：

云服务实施规范

云服务客户	云服务提供商
(无额外实施指南)	若云服务提供商使用同级云服务提供商的云服务，应确保其向自有云服务客户提供的信息安全水平不降低或高于原有水平。 当云服务提供商基于供应链提供云服务时，应向供应商提供信息安全目标，并要求各供应商开展风险管理活动以实现这些目标。

15.2 供应商服务交付管理

适用 ISO/IEC 27002 第 15.2 条规定的目标。

15.2.1 供应商服务的监视和评审

适用 ISO/IEC 27002 标准中控制措施 15.2.1 及其实施指南与其他信息。

15.2.2 供应商服务的变更管理

适用 ISO/IEC 27002 标准中控制措施 15.2.2 及其实施指南与其他信息。

16 信息安全事件管理

16.1 信息安全事件的管理和改进

适用 ISO/IEC 27002 第 16.1 条规定的目标。

16.1.1 责任和规程

适用 ISO/IEC 27002 标准中控制措施 16.1.1 及其实施指南与其他信息。同时下述专用指南适用：

云服务实施规范

云服务客户	云服务提供商
云服务客户应验证信息安全事件管理职责的划分，确保其满足自身要求。	作为服务规格的一部分，云服务提供商应定义云服务客户与自身之间的信息安全事件管理职责划分。 云服务提供商应向云服务客户提供涵盖以下内容的文档： - 云服务提供商将向云服务客户报告的信息安全事件范围； - 信息安全事件检测及相关响应的披露程度； - 信息安全事件通知的目标时限； - 信息安全事件的通知流程； - 处理与信息安全事件相关问题的联系信息； - 发生特定信息安全事件时可采取的补救措施。

16.1.2 报告信息安全事态

适用 ISO/IEC 27002 标准中控制措施 16.1.2 及其实施指南与其他信息。同时下述专用指南适用：

云服务实施规范

云服务客户	云服务提供商
云服务客户应向云服务提供商请求获取以下机制的相关信息： - 云服务客户向云服务提供商报告检测到的信息安全事件； - 云服务提供商接收云服务客户检测到的信息安全事件相关报告； - 云服务客户跟踪已报告信息安全事件的状态。	云服务提供商应提供以下机制： - 云服务客户向云服务提供商报告信息安全事件； - 云服务提供商向云服务客户报告信息安全事件； - 云服务客户跟踪已报告信息安全事件的状态。

其他与云服务有关的信息

此类机制不仅应明确流程，还应提供云服务客户和云服务提供商的联系电话、电子邮箱和服务时间等关键信息。

信息安全事件可由云服务客户或云服务提供商检测到。因此，云计算相关的额外主要责任是：检测到事件的一方应具备立即向另一方报告事件的流程。

16.1.3 报告信息安全弱点

适用 ISO/IEC 27002 标准中控制措施 16.1.3 及其实施指南与其他信息。

16.1.4 信息安全事态的评估和决策

适用 ISO/IEC 27002 标准中控制措施 16.1.4 及其实施指南与其他信息。

16.1.5 信息安全事件的响应

适用 ISO/IEC 27002 标准中控制措施 16.1.5 及其实施指南与其他信息。

16.1.6 从信息安全事件中学习

适用 ISO/IEC 27002 标准中控制措施 16.1.6 及其实施指南与其他信息。

16.1.7 证据的收集

适用 ISO/IEC 27002 标准中控制措施 16.1.7 及其实施指南与其他信息。同时下述专用指南适用：

云服务实施规范

云服务客户	云服务提供商
云服务客户与云服务提供商应就响应云计算环境中潜在数字证据或其他信息请求的流程达成一致。	（无额外实施指南）

17 业务连续性管理的信息安全方面

17.1 信息安全的连续性

适用 ISO/IEC 27002 第 17.1 条规定的目标。

17.1.1 规划信息安全连续性

适用 ISO/IEC 27002 标准中控制措施 17.1.1 及其实施指南与其他信息。

17.1.2 实现信息安全连续性

适用 ISO/IEC 27002 标准中控制措施 17.1.2 及其实施指南与其他信息。

17.1.3 验证、评审和评价信息安全连续性

适用 ISO/IEC 27002 标准中控制措施 17.1.3 及其实施指南与其他信息。

17.2 冗余

适用 ISO/IEC 27002 第 17.2 条规定的目标。

17.2.1 信息处理设施的可用性

适用 ISO/IEC 27002 标准中控制措施 17.2.1 及其实施指南与其他信息。

18 符合性

18.1 符合法律和合同要求

适用 ISO/IEC 27002 第 18.1 条规定的目标。

18.1.1 适用的法律和合同要求的识别

适用 ISO/IEC 27002 标准中控制措施 18.1.1 及其实施指南与其他信息。同时下述专用指南适用：

云服务实施规范

云服务客户	云服务提供商
云服务客户应考虑相关法律法规可能同时适用于云服务提供商和自身的司法管辖区。 云服务客户应请求获取云服务提供商遵守其业务所需相关法规与标准的证据。此类证据可为第三方审计机构出具的认证文件。	云服务提供商应向云服务客户告知管辖云服务的法律司法管辖区。 云服务提供商应识别自身的相关法律要求（例如，关于加密以保护个人身份信息（PII）的要求），并在收到请求时向云服务客户提供此类信息。 云服务提供商应向云服务客户提供其当前遵守适用法律法规与合同要求的证据。

其他与云服务有关的信息

应识别适用于云服务提供与使用的法律法规要求，尤其是当处理、存储和通信能力地理分布广泛、涉及多个司法管辖区时。

需要注意的是，合规要求（无论是法律还是合同层面）的责任始终由云服务客户承担，无法转移给云服务提供商。

18.1.2 知识产权

适用 ISO/IEC 27002 标准中控制措施 18.1.2 及其实施指南与其他信息。同时下述专用指南适用：

云服务实施规范

云服务客户	云服务提供商
在云服务中安装商业许可软件可能违反软件的许可条款。云服务客户应制定流程，在允许在云服务中安装任何许可软件前，识别云服务特有的许可要求。应特别注意云服务具有弹性、可扩展性，软件可能在超出许可条款允许的更多系统或处理器核心上	云服务提供商应建立响应知识产权投诉的流程。

运行的情况。	
--------	--

18.1.3 记录的保护

适用 ISO/IEC 27002 标准中控制措施 18.1.3 及其实施指南与其他信息。同时下述专用指南适用：

云服务实施规范

云服务客户	云服务提供商
云服务客户应向云服务提供商请求获取其收集和存储的、与云服务客户使用云服务相关记录的保护情况信息。	云服务提供商应向云服务客户提供其收集和存储的、与云服务客户使用云服务相关记录的保护情况信息。

18.1.4 隐私和个人可识别信息保护

适用 ISO/IEC 27002 标准中控制措施 18.1.4 及其实施指南与其他信息。

其他与云服务有关的信息

ISO/IEC 27018《公共云中作为个人身份信息处理方的个人身份信息保护实践准则》提供了关于此主题的额外信息。

18.1.5 密码控制规则

适用 ISO/IEC 27002 标准中控制措施 18.1.5 及其实施指南与其他信息。同时下述专用指南适用：

云服务实施规范

云服务客户	云服务提供商
云服务客户应验证适用于云服务使用的一套密码控制措施是否符合相关协议、法律法规。	云服务提供商应提供其实施的密码控制措施说明，供云服务客户审查是否符合适用协议、法律法规。

18.2 信息安全评审

适用 ISO/IEC 27002 第 18.2 条规定的目标。

18.2.1 信息安全的独立评审

适用 ISO/IEC 27002 标准中控制措施 18.2.1 及其实施指南与其他信息。同时下述专用指南适用：

云服务实施规范

云服务客户	云服务提供商
云服务客户应请求获取证明文件，以验证云服务提供商实施的云服务信息安全控制措施与指南是否符合其作出的任何声明。此类证据可包括相关标准的认证。	云服务提供商应提供证明文件，以证实其声称实施了信息安全控制措施。 当单个云服务客户审计不切实际或可能增加信息安全风险时，云服务提供商应提供独立证据，证明信息安全是按照其政策和程序实施与运行的。此类证据应在签订合同前向潜在云服务客户提供。 由云服务提供商选定的相关独立审计，通常是满足云服务客户审查云服务提供商运营、获取足够透明度需求的可接受方式。当独立审计不切实际时，云服务提供商应开展自我评估，并向云服务客户披露其流程与结果。

18.2.2 符合安全策略和标准

适用 ISO/IEC 27002 标准中控制措施 18.2.2 及其实施指南与其他信息。

18.2.3 技术符合性评审

适用 ISO/IEC 27002 标准中控制措施 18.2.3 及其实施指南与其他信息。

附录 C 云服务扩展控制集

（本附录为本建议书 / 国际标准的组成部分）

本附录提供额外的控制目标、控制措施和实施指南，作为云服务的扩展控制集。与这些控制相关的 ISO/IEC 27002 控制目标不再重复。

计划在符合 ISO/IEC 27001 的信息安全管理体系（ISMS）中实施这些控制的组织，应通过纳入本附录中规定的控制措施，扩展其适用性声明（SOA）。

CLD. 6.3 云服务客户与云服务提供商的关系

目标：

明确云服务客户与云服务提供商之间信息安全管理共享角色与职责的关系。

CLD. 6.3.1 云计算环境中的共享角色与职责

控制：

云服务客户和云服务提供商应将云服务使用中共享的信息安全角色职责分配给已识别的各方，形成文件、进行沟通并予以实施。

云服务实施规范

云服务客户	云服务提供商
云服务客户应根据其云服务使用情况，制定或扩展现有政策与流程，并让云服务用户了解其在使用云服务中的角色与职责。	云服务提供商应记录并传达其云服务使用的信息安全能力、角色与职责，以及云服务客户作为云服务使用的一部分需要实施和管理的信息安全角色与职责。

其他与云服务有关的信息

在云计算中，角色与职责通常在云服务客户员工和云服务提供商员工之间划分。角色与职责的分配应考虑云服务客户数据，以及云服务提供商作为保管人的云服务客户应用程序。

CLD. 8.1 资产责任

目标：

ISO/IEC 27002 第 8.1 条规定的目标适用。

CLD. 8.1.5 云服务客户资产的移除

控制：

云服务协议终止时，位于云服务提供商场所的云服务客户资产应及时移除，必要时予以归还。

云服务实施规范

云服务客户	云服务提供商
云服务客户应请求一份书面描述，涵盖服务终止流程，包括云服务客户资产的归还、移除，以及从云服务提供商系统中删除这些资产的所有副本。 描述中应列出所有资产，并记录服务终止的时间表，且该过程应及时完成。	云服务提供商应提供关于云服务协议终止时归还和移除云服务客户资产的安排信息。 资产归还与移除安排应在协议中记录，并及时执行。安排中应明确需归还和移除的资产。

CLD. 9.5 共享虚拟环境中云服务客户数据的访问控制

目标：

缓解使用云计算共享虚拟环境时的信息安全风险。

CLD. 9.5.1 虚拟计算环境中的隔离

控制：

在云服务上运行的云服务客户虚拟环境，应受到保护，免受其他云服务客户和未授权人员的访问。

云服务实施规范

云服务客户	云服务提供商
(无额外实施指南)	云服务提供商应为以下对象实施适当的逻辑隔离：云服务客户数据、虚拟化应用程序、操作系统、存储和网络： – 多租户环境中云服务客户使用资源的分离； – 云服务提供商内部管理与云服务客户使用资源的分离。 当云服务涉及多租户时，云服务提供商应实施信息安全控制，确保不同租户使用资源的适当隔离。 云服务提供商应考虑在其提供的云服务中运行云服务客户提供的软件相关的风险。

其他与云服务有关的信息

逻辑隔离的实施取决于应用于虚拟化的技术：

- 网络和存储配置可在软件虚拟化功能提供虚拟环境（如虚拟操作系统）时实现虚拟化。此外，云服务客户在软件虚拟化环境中的隔离可使用软件的隔离功能进行设计和实施。
- 当云服务客户的信息存储在与云服务“元数据表”物理共享的存储区域中时，可通过对“元数据表”实施访问控制，实现与其他云服务客户信息的隔离。

ISO/IEC 27040《信息技术 安全技术 存储安全》中给出的安全多租户及相关指南可适用于云计算环境。

CLD. 9. 5. 2 虚拟机强化

控制：

云计算环境中的虚拟机应根据业务需求进行强化。

云服务实施规范

云服务客户	云服务提供商
配置虚拟机时，云服务客户和云服务提供商应确保适当方面得到强化（例如，仅开放必要的端口、协议和服务），并为每个使用的虚拟机实施适当的技术措施（例如，反恶意软件、日志记录）。	(无额外实施指南)

CLD. 12. 1 运行流程与职责

目标：

ISO/IEC 27002 第 12.1 条规定的目标适用。

CLD. 12. 1. 5 管理员操作安全

控制：

云计算环境管理操作的流程应予以定义、记录和监控。

云服务实施规范

云服务客户	云服务提供商
云服务客户应记录关键操作的流程，这些操作的失败可能对云计算环境中的资产造成不可恢复的损失。关键操作示例包括： – 虚拟化设备（如服务器、网络和存储）的安装、变更和删除； – 云服务使用的终止流程； – 备份与恢复。	云服务提供商应向有需求的云服务客户提供关键操作和流程的文档。

文件中应规定主管人员需监控这些操作。	
--------------------	--

其他与云服务有关的信息

云计算的优势在于快速配置与管理，以及按需自助服务。这些操作通常由云服务客户和云服务提供商的管理员执行。由于人工干预可能在这些关键操作中引发严重的信息安全事件，应考虑并在必要时制定和实施保障这些操作的机制。严重事件的示例包括擦除或关闭大量虚拟服务器，或销毁虚拟资产。

CLD. 12.4 日志与监控**目标：**

ISO/IEC 27002 第 12.4 条规定的目标适用。

CLD. 12.4.5 云服务监控**控制：**

云服务客户应具备监控其所使用云服务运行特定方面的能力。

云服务实施规范

云服务客户	云服务提供商
云服务客户应向云服务提供商请求获取每个云服务可用的服务监控能力信息。	云服务提供商应提供能力，使云服务客户能够监控与自身相关的云服务运行特定方面。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露。 适当的访问控制应确保监控能力的使用仅提供对云服务客户自身云服务实例信息的访问。 云服务提供商应向云服务客户提供服务监控能力的文档。 监控应提供与第 12.4.1 条所述事件日志一致的数据，并支持服务水平协议（SLA）条款。。

CLD. 13.1 网络安全管理**目标：**

ISO/IEC 27002 第 13.1 条规定的目标适用。

CLD. 13.1.4 虚拟与物理网络安全管理的一致性**控制：**

虚拟网络配置完成后，应根据云服务提供商的网络安全策略，验证虚拟网络与物理网络配置的一致性。

云服务实施规范

云服务客户	云服务提供商
（无额外实施指南）	云服务提供商应制定并记录虚拟网络配置的信息安全策略，该策略应与物理网络的信息安全策略保持一致。无论采用何种方式创建配置，云服务提供商都应确保虚拟网络配置符合信息安全策略。

其他与云服务有关的信息

在基于虚拟化技术构建的云计算环境中，虚拟网络在物理网络上的虚拟基础设施上进行配置。在此类环境中，网络策略的不一致可能导致系统中断或访问控制缺陷。

注：根据云服务的类型，配置虚拟网络的职责可能在云服务客户和云服务提供商之间有所不同。

参考文献

- [1] GB/T 22080-2025/ISO/IEC 27001:2022 《网络安全技术 数据存储安全管理体系 要求》
- [2] ISO/IEC 27040:2024 《信息技术 安全技术 数据存储安全》