国际标准 **ISO/IEC27017**

第一版
2015-12-15

信息技术 安全技术 基于 ISO/IEC27002 云服务信息安全控制实施规程

参考号
ISO/IEC 27017:2015(E)

目 录

前言

ISO（国际标准化组织）和 IEC（国际电工委员会）构成了世界标准化的专业体系。制定特定领域的国际标准工作通常由 ISO 的技术委员会完成。各成员团体对某技术委员会确定的项目感兴趣，均有权参加该委员会的工作。与 ISO 保持联系的各国际组织（官方的或非官方的）也可参加有关工作。在信息技术领域，ISO 和 IEC 已经建立了一个联合技术委员会，ISO/IEC JTC 1。

国际标准的制定遵循 ISO/IEC 导则第 2 部分的要求。

联合技术委员会的主要任务是制定国际标准，由技术委员会通过的国际标准草案需提交各成员团体投票表决。国际标准草案需取得至少 75%参加表决成员团体的同意，才能作为国际标准正式发布。

请注意，本文件的某些要素可能是专利权的主体。ISO IEC 不负责识别任何或所有此类专利权.

ISO/IEC 27017 由 ISO/IEC 由信息技术联合技术委员会（ISO/IEC JTC1）信息技术委员会（SC27）制定。IT 信息安全技术与 ITU-T 合作，共同出版了 ITU-T.X.1631(2015/07)。

1 范围

本国际标准提供了适用于云服务的提供和使用的信息安全控制指南，其方法是：
- ISO/IEC 27002 中规定的相关控制的附加实施指南；
- 附加的控制措施和具体与云服务相关的实施指南。

本国际标准为云服务提供商和云服务客户提供控制和实施指导。

2 规范性引用文件

以下国际标准包含的条款，通过在本文中的引用，构成本国际标准的条款。在出版时，所示版本有效。所有的标准都可能被修改，基于此的协议的缔约方建议鼓励国际标准研究采用下列标准的最新版本的可能性。国际电工委员会（IEC）和国际标准化组织（ISO）的成员保持着现行有效国际标准的注册。国际电联电信标准化局保留了一份目前有效的国际电联-T 建议清单。

2.1 相同建议|国际标准

- ITU-T Y.3500（现行）| ISO/IEC 17788:（现行），信息技术 - 云计算 - 概述和词汇。
- ITU-T Y.3502（生效）| ISO/IEC 17789:（生效），信息技术-云计算-参考体系结构。

2.2 参考文献

- ISO/IEC 27000:（生效），信息技术 - 安全技术 - 信息安全管理系统 - 概述和词汇。
- ISO/IEC 27002:2013，信息技术 - 安全技术 - 信息安全控制措施。

3 定义和缩写

3.1 其他定义的术语

本国际标准，ISO/IEC 27000 中给出的术语和定义，
ITU-T Y.3500 | ISO/IEC 17788，建议 ITU-T Y.3502 | ISO/IEC 17789 和以下定义适用：

3.1.1 以下术语在 ISO 19440 中定义：

- 能力：能够执行给定活动的质量。

3.1.2 ISO/IEC 27040 中定义了以下术语：

- 数据泄露：导致意外或非法销毁、丢失、更改、未经授权披露或访问传输、存储或以其他方式处理的受保护数据的安全危害。
- 安全多租户：一种多租户，它使用安全控件来显式地防止数据泄露，并为适当的治理提供这些控件的验证。

注 1 -当个人租户的风险分布不大于在专用租户单租户环境中时，存在安全多租户。
注 2：在非常安全的环境中，即使是租户的身份也是保密的。

3.1.3 ISO/IEC 17203 中定义了以下术语：

- 虚拟机：支持客户软件执行的完整环境。

注意——虚拟机是虚拟硬件、虚拟磁盘和与之相关的元数据的完整封装。虚拟机允许通过称为管理程序的软件层对底层物理机进行复用。

3.2 缩略语

以下缩写适用：
IaaS：基础设施服务
PaaS：平台服务
SaaS：软件服务
PII：个人可识别信息
SLA：服务级别协议

VM：虚拟机

4 云部门特定概念

4.1 概述

云计算的使用改变了组织评估和减轻信息安全风险的方式，因为计算资源在技术设计、操作和管理方面的重大变化。本国际标准提供了基于ISO/IEC 27002的特定于云的实施指南，并提供了解决云的信息安全威胁和风险考虑的其他控制措施。

本国际标准的用户应参考ISO/IEC 27002中的第5至18条，以获取控制、实施指南和其他信息。由于ISO/IEC 27002的通用性，许多控制、实现指南和其他信息都适用于组织的通用和云计算环境。例如，ISO/IEC 27002的“6.1.2 职责分离”提供了一个控制，无论组织是否作为云服务提供商，都可以应用该控制。此外，云服务客户可以从同一控制中派生出云环境中职责分离的要求，例如，分离云服务客户的云服务管理员和云服务用户。

作为ISO/IEC 27002的扩展，本国际标准进一步提供了云服务特定的控制、实施指南和其他信息（见第4.5条），旨在减轻伴随云服务的技术和操作特征而来的风险（见附件A）。云服务客户和云服务提供商可参考ISO/IEC 27002和本国际标准，根据实施指南选择控制，并在必要时添加其他控制。这个过程可以通过在使用或提供云服务的组织和业务环境中执行信息安全风险评估和风险处理来完成（见第4.4条）。

4.2 云服务中的供应商关系

ISO/IEC 27002第15条“供应商关系”为管理供应商关系中的信息安全提供了控制、实施指南和其他信息。云服务的提供和使用是一种供应商关系，云服务客户是买方，云服务提供商是供应商。因此，本条款适用于云服务客户和云服务提供商。

云服务客户和云服务提供商也可以形成供应链。假设云服务提供商提供基础设施功能类型服务。另外，另一个云服务提供商可以提供应用程序功能类型的服务。在这种情况下，第二云服务提供商是相对于第一云服务的云服务客户，并且是相对于使用其服务的云服务客户的云服务提供商。本例说明了本国际标准适用于作为云服务客户和云服务提供商的组织的情况。由于云服务客户和云服务提供商通过云服务的设计和实施形成一个供应链，因此适用ISO/IEC 27002第15.1.3条“信息和通信技术供应链”。

由多部分组成的国际标准ISO/IEC 27036“供应商关系的信息安全”就供应商关系中的信息安全向产品和服务的收单方和供应商提供了详细的指导。

ISO/IEC 27036第4部分直接涉及供应商关系中云服务的安全性。本标准同样适用于作为收单机构的云服务客户和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，云服务客户数据由云服务提供商存储、传输和处理。因此，云服务客户的业务流程依赖于云服务提供商的信息安全。如果云服务提供商对云服务没有足够的控制，云服务客户可能需要对其信息安全采取额外的预防措施。

在建立供应商关系之前，云服务客户需要选择云服务，同时考虑到云服务客户的信息安全要求与该服务提供的信息安全能力之间可能存在的差距。一旦选择了云服务，云服务客户应以满足其信息安全要求的方式管理云服务的使用。在这种关系中，云服务提供商应提供满足云服务客户信息安全需求所必需的信息和技术支持。当云服务提供商提供的信息安全控制是预置的，且云服务客户无法更改时，云服务客户可能需要实施自己的附加控制以降低风险。

4.4 云服务中的信息安全风险管理

云服务客户和云服务提供商都应该建立信息安全风险管理流程。信息安全管理体系中风险管理的要求，参考ISO/IEC 27001，信息安全风险管理本身的进一步指导请参考ISO/IEC 27005。ISO/IEC 27001和ISO/IEC 27005所遵循的ISO 31000也有助于对风险管理的一般理解。

与信息安全风险管理流程的一般适用性不同，云计算有其自身的风险源类型，包括威胁和漏洞，这些风险源源于云计算的特点，如网络化、系统的可扩展性和弹性、资源共享、自助服务提供等，按需管理、跨辖区的服务提供，以及对控制实现的可见性有限。附件 B 提供了提供和使用云服务中这些风险源和相关风险信息的参考资料。

本建议第 5 至 18 条和附件 A 中给出的控制和实施指南—国际标准涉及云计算特定的风险源和风险。

4.5 本标准的结构

本国际标准的格式与 ISO/IEC 27002 相似，通过在 ISO/IEC 27002 的第 5 至 18 条每个条款和段落中说明其文本的适用性。

当 ISO/IEC 27002 中规定的目标和控制在不需要任何附加信息的情况下适用时，仅提供了对 ISO/IEC 27002 的参考。

当除了 ISO/IEC 27002 的目标之外，在本标准的规范性附录 A 云服务扩展控制集中给出了针对云服务控制的目标。

当 ISO/IEC 27002 或本标准的附件 A 的额外云服务控制特定实施指南时，在副标题**“云服务实施指南”**下给出。指南分为以下两种类型：

当有针对云服务客户和云服务提供商的单独指导时，使用类型 1。

当云服务客户和云服务提供商都提供指导时，使用类型 2。

类型 1：

云服务客户	云服务提供商

类型 2：

云服务客户	云服务提供商

在副标题**“云服务的其他信息”**下提供可能需要考虑的其他信息。

5 信息安全策略

5.1 信息安全的管理指导

ISO/IEC 27002 第 5.1 条规定的目标。

5.1.1 信息安全策略

控制 5.1.1 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。以下针对具体行业的指导也适用。**云服务实施指南：**

云服务客户	云服务提供商
云计算的信息安全策略应定义为云服务客户的特定主题策略。 云服务客户的云计算信息安全策略应与组织对其信息和其他资产的可接受信息安全风险水平相一致。在定义云计算的信息安全策略时，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以由云服务提供商访问和管理； - 资产可以在云计算环境中维护，例如应用程序； - 流程可以在多租户虚拟化云服务上运行； - 云服务用户及其使用云服务的上下文； - 拥有特权访问权限的云服务客户的云服务管理员； - 云服务提供商组织的地理位置，以及云服	云服务提供商应增强其信息安全策略，以解决其云服务的提供和使用，同时考虑以下因素： - 适用于云服务设计和实施的基线信息安全要求； - 来自授权内幕人士的风险； - 多租户和云服务客户隔离（包括虚拟化）； - 云服务提供商的员工访问云服务客户资产； - 访问控制程序，例如，对云服务的管理访问进行强身份验证； - 在变更管理期间与云服务客户进行沟通； - 虚拟化安全； - 访问和保护云服务客户数据； - 云服务客户账户的生命周期管理；

务提供商可以存储云服务客户数据的国家（甚至暂时）。	- 沟通违规行为和信息共享指南，以协助调查和取证。

云服务的其他信息:

云计算的云服务客户信息安全策略是 ISO/IEC 27002 5.1.1 中描述的特定于主题的策略之一。组织的信息安全策略处理其信息和业务流程。当一个组织使用云服务时，它可以作为云服务客户拥有云计算的策略。组织的信息可以在云计算环境中存储和维护，业务流程可以在云计算环境中操作。在顶层信息安全策略中所述的一般信息安全要求之后是云计算策略。

与此相反，用于提供云服务的信息安全策略处理的是云服务客户的信息和业务流程，而不是云服务提供商的信息和业务流程。提供云服务的信息安全要求应满足未来云服务客户的要求。因此，它们可能与云服务提供商的信息和业务流程的信息安全要求不一致。云服务的信息安全策略的范围通常是根据服务定义的，而不仅仅是由组织结构或物理位置定义的。

云计算有几个虚拟化安全方面，包括虚拟实例的生命周期管理、虚拟化映像的存储和访问控制、休眠或脱机虚拟实例的处理、快照、虚拟机监控程序的保护以及管理自助门户使用的安全控制。

5.1.2 信息安全策略的评审

控制 5.1.2 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

6 信息安全组织

6.1 内部组织

ISO/IEC 27002 第 6.1 条规定的目标适用。

6.1.1 信息安全角色和职责

控制 6.1.1 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。以下针对具体行业的指导也适用。**云服务实施指南：**

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适当分配信息安全角色和职责达成一致，并确认其能够履行分配的角色和职责。双方的信息安全角色和责任应在协议中说明。 云服务客户应识别并管理其与云服务提供商的客户支持和关怀功能的关系。	云服务提供商应与其云服务客户、云服务提供商和供应商商定并记录信息安全角色和责任的适当分配。

云服务的其他信息

即使在各方内部和之间确定了责任，云服务客户也要对使用服务的决定负责。应该根据在云服务客户组织中确定的角色和职责来做出决定。云服务提供商对作为云服务协议一部分的信息安全负责。信息安全的实施和配置应根据云服务提供商组织内确定的角色和职责进行。

在角色以及与数据所有权、访问控制和基础设施维护等问题相关的责任的定义和分配方面的模糊性可能会引起业务或法律纠纷，特别是在与第三方打交道时。

在使用云服务期间创建或修改的云服务提供商系统上的数据和文件对服务的安全操作、恢复和连续性至关重要。所有资产的所有权，以及对这些资产相关操作（如备份和恢复操作）负有责任的各方，都应加以定义和记录。否则，云服务提供商可能会假设云服务客户执行这些重要任务（反之亦然），可能会发生数据丢失。

6.1.2 职责分离

控制 6.1.2 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

6.1.3 与职能机构的联系

控制 6.1.3 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。以下针对具体行业的指导也适用。**云服务实施指南：**

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组合操作（联合运营）相关的权限。	云服务提供商应告知云服务客户云服务提供商组织的地理位置以及云服务提供商可以存储云服务客户数据的国家。

云服务的其他信息

有关可存储、处理或传输云服务客户数据的地理位置的信息可以帮助云服务客户确定监管机构和管辖区。

6.1.4 与特定相关方的联系

控制 6.1.4 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

6.1.5 项目管理中的信息安全

控制 6.1.5 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

6.2 移动设备和远程工作

ISO/IEC 27002 第 6.2 条规定的目标适用。

6.2.1 移动设备策略

控制 6.2.1 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

6.2.2 远程工作

控制 6.2.2 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

7 人力资源安全

7.1 任用前

ISO/IEC 27002 第 7.1 条规定的目标适用。

7.1.1 审查

控制 7.1.1 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

7.1.2 任用条款和条件

控制 7.1.2 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

7.2 任用中

ISO/IEC 27002 第 7.2 条规定的目标适用。

7.2.1 管理责任

控制 7.2.1 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

7.2.2 信息安全意识、教育和培训

控制 7.2.2 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。以下针对具体行业的指导也适用。**云服务实施指南：**

云服务客户	云服务提供商
云服务客户应在针对云服务业务经理、云服务管理员、云服务集成商和云服务用户（包括相关员工和承包商）的意识、教育和培训计划中添加以下内容： - 云服务的使用标准和程序； - 与云服务相关的信息安全风险以及如何管理这些风险； - 使用云服务的系统和网络环境风险； - 适用的法律和监管考虑。 应向管理层和监督管理层（包括业务部门的管理层）提供有关云服务的信息安全意识、教育和培训方案。这些努力支持有效协调信息安全活动。	云服务提供商应为员工提供意识、教育和培训，并要求承包商在适当处理云方面也这样做 服务客户数据和云服务衍生数据。这些数据可以包含对云服务客户保密的信息，也可以受云服务提供商访问和使用的特定限制（包括法规限制）。

7.2.3 违规处理过程

控制 7.2.3 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

7.3 任用的终止和变更

ISO/IEC 27002 第 7.3 条规定的目标适用。

7.3.1 任用终止或变更的责任

控制 7.3.1 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

8 资产管理

8.1 有关资产的责任

ISO/IEC 27002 第 8.1 条规定的目标适用。

8.1.1 资产清单

控制 8.1.1 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。以下针对具体行业的指导也适用。**云服务实施指南：**

云服务客户	云服务提供商
云服务客户的资产清单应包含存储在云计算环境中的信息和相关资产。存货的记录应指明资产的维护位置，例如云服务的标识。	云服务提供商的资产清单应明确指出： - 云服务客户数据； - 云服务衍生数据。

云服务的其他信息：

有一些云服务应用程序通过将云服务派生的数据添加到云服务客户数据中来提供管理信息的功能。将云服务派生的数据识别为资产并将其维护在资产清单中，可以有助于提高信息安全性。

8.1.2 资产的所属关系

控制 8.1.2 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

云服务的其他信息

根据使用的云服务类别，资产的所有权可能会有所不同。当使用平台即服务（PaaS）或基础设施即服务（IaaS）服务时，应用软件将属于云服务客户，而对于软件即服务（SaaS）服务，应用软件将属于云服务提供商。

8.1.3 资产的可接受使用

控制 8.1.3 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

8.1.4 资产归还

控制 8.1.4 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

8.2 信息分类

ISO/IEC 27002 第 8.2 条规定的目标适用。

8.2.1 信息分级

控制 8.2.1 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

8.2.2 信息标记

控制 8.2.2 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。以下针对具体行业的指导也适用。**云服务实施指南：**

云服务客户	云服务提供商
云服务客户应根据云服务客户所采用的标记程序标记在云计算环境中维护的信息和相关资产。在适用的情况下，可以采用云服务提供商提供的支持标记的功能。	云服务提供商应记录并披露其提供的任何服务功能，允许云服务客户对其信息和相关资产进行分类和标记。

8.2.3 资产的处理

控制 8.2.3 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

8.3 介质处理

ISO/IEC 27002 第 8.3 条规定的目标适用。

8.3.1 移动介质的管理

控制 8.3.1 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

8.3.2 介质的处置

控制 8.3.2 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

8.3.3 物理介质转移

控制 8.3.3 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

9 访问控制

9.1 访问控制的业务要求

ISO/IEC 27002 第 9.1 条规定的目标适用。

9.1.1 访问控制策略

控制 9.1.1 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

9.1.2 网络和网络服务的访问

控制 9.1.2 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。以下针对具体行业的指导也适用。**云服务实施指南：**

云服务客户	云服务提供商
云服务客户使用网络服务的访问控制策略应指定用户访问所使用的每个单独云服务的要求。	（无附加实施指南）

9.2 用户访问管理

ISO/IEC 27002 第 9.2 条规定的目标适用。

9.2.1 用户注册和注销

控制 9.2.1 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。以下针对具体行业的指导也适用。**云服务实施指南：**

云服务客户	云服务提供商
（无附加实施指南）	要管理云服务客户的云服务用户对云服务的访问，云服务提供商应向云服务客户提供用户注册和注销功能以及使用这些功能的规范。

9.2.2 用户访问供给

控制 9.2.2 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。以下针对具体行业的指导也适用。**云服务实施指南：**

云服务客户	云服务提供商
（无附加实施指南）	云服务提供商应提供管理云服务客户的云服务用户的访问权限的功能，以及这些功能的使用规范。

云服务的其他信息：

云服务提供商应为其云服务和相关的管理接口支持第三方身份和访问管理技术。这些技术可以使云服务客户的系统和云服务之间的集成和用户身份管理更加容易，并且可以方便地使用多个云服务，支持单点登录等功能。

9.2.3 特许访问权管理

控制 9.2.3 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。以下针对具体行业的指导也适用。**云服务实施指南：**

云服务客户	云服务提供商

云服务客户应使用足够的身份验证技术（例如，多因素身份验证）对云服务客户的云服务管理员进行身份验证 根据已识别的风险对云服务的管理能力。	云服务提供商应根据识别出的风险，提供足够的认证技术，对云服务客户的云服务管理员进行云服务管理能力的认证。例如，云服务提供商可以提供多因素身份验证功能或启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

控制 9.2.4 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。以下针对具体行业的指导也适用。**云服务实施指南：**

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密码等机密身份验证信息的管理过程是否符合云服务客户的要求。	云服务提供商应提供云服务客户的秘密认证信息管理程序的信息，包括分配此类信息和用户认证的程序。

云服务的其他信息：

云服务客户应使用自己或第三方的身份和访问管理技术来控制对秘密认证信息的管理。

9.2.5 用户访问权限评审

控制 9.2.5 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

9.2.6 访问权的移除或调整

控制 9.2.6 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

9.3 用户责任

ISO/IEC 27002 第 9.3 条规定的目标适用。

9.3.1 秘密鉴别信息的使用

控制 9.3.1 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

9.4 系统和应用访问控制

ISO/IEC 27002 第 9.4 条规定的目标适用。

9.4.1 信息访问限制

控制 9.4.1 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。以下针对具体行业的指导也适用。**云服务实施指南：**

云服务客户	云服务提供商
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的信息的访问，并实现此类限制。这包括限制对云服务、云服务功能和在服务中维护的云服务客户数据的访问。	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、其云服务功能和在服务中维护的云服务客户数据的访问。

云服务的其他信息：

云计算环境包括需要访问控制的其他区域。作为云服务或云服务功能的一部分，对功能和服务（如 hypervisor 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

控制 9.4.2 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

9.4.3 口令管理系统

控制 9.4.3 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

9.4.4 特权实用程序的使用

控制 9.4.4 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。以下针对具体行业的指导也适用。**云服务实施指南：**

云服务客户	云服务提供商
在允许使用实用程序的情况下，云服务客户应确定要在其云计算环境中使用的实用程序，并确保它们不会干扰云服务的控制。	云服务提供商应该确定云服务中使用的任何实用程序的需求。 云服务提供商应确保能够绕过正常操作或安

	全程序的任何实用程序的使用都严格限制在授权人员的范围内，并定期审查和审核此类程序的使用。

9.4.5 程序源代码的访问控制

控制 9.4.5 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

10 密码

10.1 密码控制

ISO/IEC 27002 第 10.1 条规定的目标适用。

10.1.1 密码控制的使用策略

控制 10.1.1 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。以下针对具体行业的指导也适用。**云服务实施指南：**

云服务客户	云服务提供商
如果风险分析证明合理，云服务客户应为其使用云服务实施加密控制。无论这些控制是由云服务客户还是由云服务提供商提供的，这些控制都应具有足够的强度来减轻已识别的风险。 当云服务提供商提供加密时，云服务客户应查看云服务提供商提供的任何信息，以确认加密功能是否： - 满足云服务客户的政策要求； - 与云服务客户使用的任何其他加密保护兼容； - 适用于云服务的静态和传输中的数据。	云服务提供商应向云服务客户提供有关其使用加密技术保护其处理的信息的情况的信息。云服务提供商还应该向云服务客户提供有关其提供的任何功能的信息，这些功能可以帮助云服务客户应用其自己的加密保护。

云服务的其他信息：

在一些法域中，可能需要应用加密技术来保护特定类型的信息，如健康数据、居民登记号码、护照号码和驾驶执照号码。

10.1.2 秘钥管理

控制 10.1.2 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。以下针对具体行业的指导也适用。**云服务实施指南：**

云服务客户	云服务提供商
云服务客户应该识别每个云服务的加密密钥，并实现密钥管理过程。 在云服务提供密钥管理功能供云服务客户使用的情况下，云服务客户应请求有关用于管理与云服务相关的密钥的过程的以下信息： - 钥匙类型； - 密钥管理系统规范，包括密钥生命周期各阶段的程序，即生成、更改或更新、存储、退役、检索、保留和销毁； - 云服务客户使用的推荐密钥管理程序。 当云服务客户使用其自己的密钥管理或单独和不同的密钥管理服务时，云服务客户不应允许云服务提供商存储和管理加密操作的加密密钥。	（无附加实施指南）

11 物理和环境安全

11.1 安全区域

ISO/IEC 27002 第 11.1 条规定的目标适用。

11.1.1 物理安全边界

控制 11.1.1 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

11.1.2 物理入口控制

控制 11.1.2 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

11.1.3 办公室、房间和设施的安全防护

控制 11.1.3 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

11.1.4 外部和环境威胁的安全防护

控制 11.1.4 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

11.1.5 在安全区域工作

控制 11.1.5 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

11.1.6 交接区

控制 11.1.6 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

11.2 设备

ISO/IEC 27002 第 11.2 条规定的目标适用。

11.2.1 设备安置和保护

控制 11.2.1 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

11.2.2 支持性设施

控制 11.2.2 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

11.2.3 布缆安全

控制 11.2.3 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

11.2.4 设备维护

控制 11.2.4 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

11.2.5 资产移动

控制 11.2.5 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

11.2.6 组织场所外的设备与资产安全

控制 11.2.6 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

11.2.7 设备安全处置或再利用

控制 11.2.7 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。以下针对具体行业的指导也适用。**云服务实施指南：**

云服务客户	云服务提供商
云服务客户应请求确认云服务提供商具有安全处置或重用资源的策略和过程。	云服务提供商应确保及时安排资源（如设备、数据存储、文件、内存）的安全处置或重用。

云服务的其他信息：

有关安全处置的其他信息，请参见 ISO/IEC 27040。

11.2.8 无人值守的用户设备

控制 11.2.8 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

11.2.9 清理桌面和屏幕策略

控制 11.2.9 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

12 运行安全

12.1 运行规程和责任

ISO/IEC 27002 第 12.1 条规定的目标适用。

12.1.1 文件化的操作规程

控制 12.1.1 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

12.1.2 变更管理

控制 12.1.2 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。以下针对具体行业的指导也适用。**云服务实施指南：**

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所做的任何变更的影响。	云服务提供商应向云服务客户提供有关可能对云服务产生不利影响的云服务更改的信息。以下内容将帮助云服务客户确定更改对信息安全的影响： －变更类别； —变更的计划日期和时间； －云服务和底层系统变更的技术描述； －变更开始和完成的通知。 当云服务提供商提供依赖于对等云服务提供商的云服务时，云服务提供商可能需要将对等云服务提供商导致的更改通知云服务客户。

云服务的其他信息：

应包含在通知中的项目列表可以在协议中标识，例如主服务协议或服务级别协议（SLA）。

12.1.3 容量管理

控制 12.1.3 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。以下针对具体行业的指导也适用。**云服务实施指南**

云服务客户	云服务提供商
云服务客户应确保云服务提供的约定容量满足云服务客户的要求。 云服务客户应监控云服务的使用，并预测其容量需求，以确保云服务的性能随时间而变化。	云服务提供商应监控总资源容量，以防止资源短缺导致的信息安全事件。

云服务的其他信息：

云服务涉及由云服务提供商控制的资源，并根据主服务协议和相关的 SLA 条款提供给云服务客户。这些资源包括软件、处理硬件、数据存储和网络连接。

云服务中资源的弹性、可伸缩和按需分配通常会增加服务的总容量。但是，云服务客户应该知道，所提供的资源可能存在容量限制。容量限制的示例包括应用程序的处理器核心数、可用存储量或可用网络带宽。

这些约束可以根据特定的云服务或云服务客户购买的特定订购而变化。如果云服务客户的需求超出了限制，则云服务客户可能需要更改云服务或更改订购。

为了使云服务客户能够对云服务进行容量管理，云服务客户应该能够访问有关资源使用情况的统计数据，例如：

－特定时间段的统计数据；

－资源使用的最大水平。

12.1.4 开发、测试和运行环境的分离

控制 12.1.4 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

12.2 **防恶意软件**

ISO/IEC 27002 第 12.2 条规定的目标适用。

12.2.1 恶意软件的控制

控制 12.2.1 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

12.3 **备份**

ISO/IEC 27002 第 12.3 条规定的目标适用。

12.3.1 信息备份

控制 12.3.1 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。以下针对具体行业的指导也适用。**云服务实施指南：**

云服务客户	云服务提供商
当云服务提供商提供备份功能作为云服务的一部分时，云服务客户应向云服务提供商请求备份功能的规范。云服务客户还应验证其是否满足备份要求。当云服务提供商不提供备份功能时，云服务客户负责实现备份功能。	云服务提供商应向云服务客户提供其备份功能的规范。规范应酌情包括以下信息： - 备份的范围和时间表； - 备份方法和数据格式，包括加密（如果相关）； - 备份数据的保留期； - 验证备份数据完整性的程序； - 从备份中恢复数据所涉及的程序和时间表； - 测试备份能力的程序； - 备份的存储位置。 如果向云服务客户提供备份（如虚拟快照）服务，云服务提供商应提供对备份的安全和隔离访问。

云服务的其他信息：

在云计算环境中进行备份的职责分配常常不清楚。对于 IaaS，备份的责任通常由云服务客户承担。但是，云服务客户可能不知道自己有责任备份云计算系统中生成的所有云服务客户数据，例如使用 PaaS 服务的开发功能生成的可执行文件。

注意--不同级别的备份和恢复可能以附加成本作为服务提供，在这种情况下，云服务客户可以选择备份的内容和时间。

12.4 日志和监视

ISO/IEC 27002 第 12.4 条规定的目标适用。

12.4.1 事态日志

控制 12.4.1 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。以下针对具体行业的指导也适用。**云服务实施指南：**

云服务客户	云服务提供商
云服务客户应该定义其事件日志记录需求，并验证云服务是否满足这些需求。	云服务提供商应该向云服务客户提供日志记录功能。

云服务的其他信息：

云服务客户和云服务提供商对事件日志记录的责任因使用的云服务类型而异。例如，使用 IaaS，云服务提供商的日志记录职责可以限制在云计算基础设施组件的日志记录职责范围内，云服务客户可以负责记录自己虚拟机和应用程序的事件。

12.4.2 日志信息的保护

控制 12.4.2 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

12.4.3 管理员和操作员日志

控制 12.4.3 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。以下针对具体行业的指导也适用。**云服务实施指南：**

云服务客户	云服务提供商
如果将特权操作委派给云服务客户，则应记录这些操作的操作和性能。云服务客户应该确定 云服务提供商提供的日志记录功能是否合适，或者云服务客户是否应该实现其他日志	（无附加实施指南）

记录功能。	

云服务的其他信息：

云服务客户和云服务提供商之间的责任分配（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是必要的，以支持针对这些操作的错误使用的预防和纠正措施。

12.4.4 时钟同步

控制 12.4.4 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。以下针对具体行业的指导也适用。**云服务实施指南：**

云服务客户	云服务提供商
云服务客户应请求有关用于云服务提供商系统的时钟同步的信息。	云服务提供商应向云服务客户提供有关云服务提供商系统所用时钟的信息，以及有关云服务客户可以将本地时钟与云服务时钟同步。

云服务的其他信息：

有必要考虑云服务客户系统与云服务提供商系统的时钟同步，后者运行云服务客户使用的云服务。如果没有这种同步，就很难协调云服务客户系统上的事件与云服务提供商系统上的事件。

12.5 运行软件控制

ISO/IEC 27002 第 12.5 条规定的目标适用。

12.5.1 运行系统的软件安装

控制 12.5.1 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

12.6 技术方面的脆弱性管理

ISO/IEC 27002 第 12.6 条规定的目标适用。

12.6.1 技术方面的脆弱性管理

控制 12.6.1 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。以下针对具体行业的指导也适用。**云服务实施指南：**

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有关管理可能影响所提供云服务的技术漏洞的信息。云服务客户应识别其将负责管理的技术漏洞，并明确定义管理这些漏洞的流程。	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漏洞的信息。

12.6.2 软件安装限制

控制 12.6.2 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

12.7 信息系统审计的考虑

ISO/IEC 27002 第 12.7 条规定的目标适用。

12.7.1 信息系统审计的控制

控制 12.7.1 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

13 通信安全

13.1 网络安全管理

ISO/IEC 27002 第 13.1 条规定的目标适用。

13.1.1 网络控制

控制 13.1.1 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

13.1.2 网络服务的安全

控制 13.1.2 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

13.1.3 网络中的隔离

控制 13.1.3 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。以下针对具体行业的指导也适用。**云服务实施指南：**

云服务客户	云服务提供商
云服务客户应该定义其分离网络的需求，以便在云服务的共享环境中实现租户隔离，并验证云服务提供商满足这些要求	在下列情况下，云服务提供商应实施网络访问隔离： - 多租户环境中租户之间的隔离； - 云服务提供商的内部管理环境和云服务客户的云计算环境之间的隔离。 在适当的情况下，云服务提供商应该帮助云服务客户验证云服务提供商实现的隔离。

云服务的其他信息：

法律法规可能要求隔离网络或隔离网络流量。

13.2 信息传输

ISO/IEC 27002 第 13.2 条规定的目标适用。

13.2.1 信息传递策略和程程

控制 13.2.1 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

13.2.2 信息传输协议

控制 13.2.2 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

13.2.3 电子消息发送

控制 13.2.3 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

13.2.4 保密或不泄露协议

控制 13.2.4 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

14 系统获取、开发和维护

14.1 信息系统的安全要求

ISO/IEC 27002 第 14.1 条规定的目标适用。

14.1.1 信息安全需求分析和说明

控制 14.1.1 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。以下针对具体行业的指导也适用。**云服务实施指南：**

云服务客户	云服务提供商
云服务客户应确定其对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够满足这些要求。 对于此评估，云服务客户应向云服务提供商请求有关信息安全功能的信息。	云服务提供商应该向云服务客户提供他们使用的信息安全功能的信息。此信息应是信息性的，而不应披露可能对具有恶意意图的人有用的信息。

云服务的其他信息：

应注意限制安全控制实施细节的披露，因为它们与提供给那些已签订保密协议的云服务客户或潜在云服务客户的云服务有关。

14.1.2 公共网络上应用服务的安全保护

控制 14.1.2 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

14.1.3 应用服务事务的保护

控制 14.1.3 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

14.2 开发和支持过程的安全

ISO/IEC 27002 第 14.2 条规定的目标适用。

14.2.1 安全的开发策略

控制 14.2.1 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。以下针对具体行业的指导也适用。**云服务实施指南：**

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有关云服务提供商使用安全开发过程和实践的信息。	云服务提供商应提供有关其使用安全开发过程和实践的信息，以符合其披露政策。

云服务的其他信息：

云服务提供商的安全开发过程和实践对 SaaS 至关重要。

14.2.2 系统变更控制规程

控制 14.2.2 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

14.2.3 运行平台变更后对应用的技术评审

控制 14.2.3 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

14.2.4 软件包变更的限制

控制 14.2.4 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

14.2.5 系统安全工程原则

控制 14.2.5 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

14.2.6 安全的开发环境

控制 14.2.6 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

14.2.7 外包开发

控制 14.2.7 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

14.2.8 系统安全测试

控制 14.2.8 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

14.2.9 系统验收测试

控制 14.2.9 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

云服务的其他信息

在云计算中，系统验收测试指南适用于云服务客户对云服务的使用。

14.3 测试数据

ISO/IEC 27002 第 14.3 条规定的目标适用。

14.3.1 测试数据的保护

控制 14.3.1 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

15 供应商关系

15.1 供应商关系中的信息安全

ISO/IEC 27002 第 15.1 条规定的目标适用。

15.1.1 供应商关系的信息安全策略

控制 15.1.1 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。以下针对具体行业的指导也适用。**云服务实施指南：**

云服务客户	云服务提供商
云服务客户应将云服务提供商作为一种供应商纳入其供应商关系信息安全策略中。这将有助于降低与云服务提供商访问和管理云服务客户数据相关的风险。	（无附加实施指南）

15.1.2 在供应商协议中强调安全

控制 15.1.2 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。以下针对具体行业的指导也适用。**云服务实施指南：**

云服务客户	云服务提供商

云服务客户应确认与云服务相关的信息安全角色和责任，如服务协议中所述。这些过程可以包括以下过程： - 恶意软件保护； - 备份； - 加密控制； - 脆弱性管理； - 事件管理； - 技术符合性检查； - 安全测试； - 审计； - 收集、维护和保护证据，包括日志和审计跟踪； - 服务协议终止时的信息保护； - 认证和访问控制； - 身份和访问管理。	云服务提供商应在协议中指定云服务提供商将实施的相关信息安全措施，以确保云服务提供商和云服务客户之间不会产生误解。 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。

15.1.3 信息和通信技术供应链

控制 15.1.3 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。以下针对具体行业的指导也适用。**云服务实施指南：**

云服务客户	云服务提供商
（无附加实施指南）	如果云服务提供商使用对等云服务提供商的云服务，则云服务提供商应确保维护或超过其自身云服务客户的信息安全级别。 当云服务提供商基于供应链提供云服务时，云服务提供商应向供应商提供信息安全目标，并请求供应商执行风险管理活动以达到目标。

15.2 供应商服务交付管理

ISO/IEC 27002 第 15.2 条规定的目标适用。

15.2.1 供应商服务的监视和评审

控制 15.2.1 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

15.2.2 供应商服务的变更管理

控制 15.2.2 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

16 信息安全事件管理

16.1 信息安全事件的管理和改进

ISO/IEC 27002 第 16.1 条规定的目标适用。

16.1.1 责任和规程

控制 16.1.1 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。以下针对具体行业的指导也适用。**云服务实施指南：**

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分配，并确保其满足云服务客户的要求。	作为服务规范的一部分，云服务提供商应定义云服务客户和云服务提供商之间信息安全事件管理职责和程序的分配。 云服务提供商应向云服务客户提供以下文档： - 云服务提供商将向云服务客户报告的信息安全事件的范围； - 信息安全事件检测和相关应对措施的披露

	水平； - 发生信息安全事件通知的目标时间框架； - 信息安全事件通知程序； - 处理信息安全事件相关问题的联系信息； - 在发生某些信息安全事件时可以应用的任何补救措施。

16.1.2 报告信息安全事态

控制 16.1.2 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。以下针对具体行业的指导也适用。**云服务实施指南：**

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有关以下机制的信息： - 云服务客户向云服务提供商报告其检测到的信息安全事件； - 云服务提供商接收有关云服务提供商检测到的信息安全事件的报告； - 云服务客户跟踪报告的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； - 云服务客户跟踪报告的信息安全事件的状态。

云服务的其他信息：

这些机制不仅应该定义流程，还应该为云服务客户和云服务提供商提供基本信息，如联系电话、电子邮件地址和服务时间。

信息安全事件可以由云服务客户或云服务提供商检测。因此，与云计算相关的主要附加责任是检测事件的一方应具有立即向另一方报告事件的过程。

16.1.3 报告信息安全弱点

控制 16.1.3 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

16.1.4 信息安全事态的评估与决策

控制 16.1.4 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

16.1.5 信息安全事件的响应

控制 16.1.5 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

16.1.6 从信息安全事件中学习

控制 16.1.6 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

16.1.7 证据的收集

控制 16.1.7 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。以下针对具体行业的指导也适用。**云服务实施指南：**

云服务客户	云服务提供商
云服务客户和云服务提供商应就响应来自云计算环境中的潜在数字证据或其他信息的请求的过程达成一致。	

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

ISO/IEC 27002 第 17.1 条规定的目标适用。

17.1.1 规划信息安全连续性

控制 17.1.1 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

17.1.2 实现信息安全连续性

控制 17.1.2 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

17.1.3 验证、评审和评价信息安全连续性

控制 17.1.3 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

17.2 冗余

ISO/IEC 27002 第 17.2 条规定的目标适用。

17.2.1 信息处理设施的可用性

控制 17.2.1 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

18 符合性

18.1 符合法律法规和合同要求

ISO/IEC 27002 第 18.1 条规定的目标适用。

18.1.1 适用的法律和合同要求的识别

控制 18.1.1 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。以下针对具体行业的指导也适用。**云服务实施指南：**

云服务客户	云服务提供商
云服务客户应要求提供书面证据，证明云服务信息安全控制和指南的实施符合云服务提供商的任何声明。这些证据可能包括违反相关标准的认证。 云服务提供商应向云服务客户提供书面证据，以证实其实施信息安全控制的声明。 如果个别云服务客户审计不切实际或可能增加信息安全风险，云服务提供商应提供独立证据，证明信息安全是按照云服务提供商的政策和程序实施和操作的。	云服务提供商应将管理云服务的法律辖区告知云服务客户。 云服务提供商应确定其自身的相关法律要求（例如，关于保护个人可识别信息（PII）的加密），该信息也应在要求时提供给云服务客户。 云服务提供商应向云服务客户提供其当前遵守适用法律和合同要求的证据。

云服务的其他信息：

应确定适用于云服务的提供和使用的法律和法规要求，特别是在处理、存储和通信能力在地理上分布且可能涉及多个司法管辖区的情况下。

需要注意的是，法规遵从性要求（无论是法律的还是合同的）仍然是云服务客户的责任。合规责任不能转移到云服务提供商。

18.1.2 知识产权

控制 18.1.2 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。以下针对具体行业的指导也适用。**云服务实施指南：**

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会导致违反软件的许可条款。云服务客户应该有一个识别 在允许在云服务中安装任何许可软件之前，云特定的许可要求。应特别注意云服务具有弹性和可扩展性的情况，并且软件可以在超出许可条款允许的更多系统或处理器核心上运行。	云服务提供商应建立应对知识产权投诉的流程。

18.1.3 记录的保护

控制 18.1.3 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。以下针对具体行业的指导也适用。**云服务实施指南：**

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有关保护云服务提供商收集和存储的与云服务客户使用云服务相关的记录的信息。	云服务提供商应向云服务客户提供有关保护云服务提供商收集和存储的与云服务客户使用云服务相关的记录的信息。

18.1.4 隐私和个人可识别信息保护

控制 18.1.4 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

云服务的其他信息：

ISO/IEC 27018，《信息技术 安全技术 在公有云中个人可识别信息（PII）保护的信息安全控制实施规程》提供了有关此主题的内容。

18.1.5 密码控制规则

控制 18.1.5 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。以下针对具体行业的指导也适用。云服务实施指南：

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加密控制集是否符合相关协议、立法和法规。	云服务提供商应向云服务客户提供云服务提供商实施的加密控制的说明，以审查是否符合适用的协议、法律和法规。

18.2 信息安全评审

ISO/IEC 27002 第 18.2 条规定的目标适用。

18.2.1 信息安全的独立评审

控制 18.2.1 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。以下针对具体行业的指导也适用。**云服务实施指南：**

云服务客户	云服务提供商
云服务客户应要求提供书面证据，证明云服务的信息安全控制和指南的实施符合云服务提供商的任何声明。这些证据可能包括违反相关标准的认证。	云服务提供商应向云服务客户提供书面证据，以证实其实施信息安全控制的声明。 如果个别云服务客户审计不切实际或可能增加信息安全风险，云服务提供商应提供独立证据，证明信息安全是按照云服务提供商的政策和程序实施和操作的。这应该在签订合同之前提供给潜在的云服务客户。云服务提供商选择的相关独立审计通常应是满足云服务客户审查云服务提供商运营的兴趣的可接受方法，前提是提供足够的透明度。当独立审计不切实际时，云服务提供商应进行自我评估，并向云服务客户披露其过程和结果。

18.2.2 符合安全策略和标准

控制 18.2.2 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

18.2.3 技术符合性评审

控制 18.2.3 和相关实施指南以及 ISO/IEC 27002 中规定的其他信息适用。

附件 A　云服务扩展控制集

（本附件构成本建议“国际标准”的组成部分。）

本附件提供了额外的控制目标、控制和实施指南，作为云服务的扩展控制集。与这些控制相关的 ISO/IEC 27002 控制目标不重复。

打算在符合 ISO/IEC 27001 的信息安全管理系统（ISMS）中实施这些控制的组织应通过包括本附件中所述的控制来扩展其适用性声明（SOA）。

CLD.6.3 云服务客户与云服务提供商的关系

目的：明确云服务客户与云服务提供商在信息安全管理中的角色和职责共享关系。

CLD.6.3.1 云计算环境中的共享角色和责任

控制：云服务使用中共享信息安全角色的责任应分配给已确定的各方，由云服务客户和云服务提供商记录、沟通和实施。**云服务实施指南：**

云服务客户	云服务提供商
云服务客户应根据其云服务的使用来定义或扩展其现有的策略和过程，并使云服务用户意识到他们的角色和使用云服务的责任。	云服务提供商应记录并传达其信息安全能力、角色和使用云服务的责任，以及信息作为云服务使用的一部分，云服务客户需要实现和管理的安全角色和责任。

云服务的其他信息：

在云计算中，角色和职责通常在云服务客户的员工和云服务提供商的员工之间划分。角色和职责的分配应考虑云服务客户数据和云服务提供商为其托管的云服务客户应用程序。

CLD.8.1 资产责任

ISO/IEC 27002 第 8.1 条规定的目标适用。

CLD.8.1.5 删除云服务客户资产

控制：云服务提供商所在地的云服务客户的资产应在云服务协议终止后及时移除并返还（如有必要）。**云服务实施指南：**

云服务客户	云服务提供商
云服务客户应要求提供有关服务终止过程的书面说明，包括归还和移除云服务客户的资产，然后从云服务提供商的系统中删除这些资产的所有副本。 说明书应列出所有资产，并记录终止服务的时间表，该时间表应及时发生。	云服务提供商应提供有关在云服务使用协议终止时返还和移除任何云服务客户资产的安排的信息。 资产返还和转移安排应记录在协议中，并应及时执行。安排应具体说明要归还和移走的资产。

CLD.9.5 共享虚拟环境中云服务客户数据的访问控制

目的：降低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：云服务客户在云服务上运行的虚拟环境应受到保护，以防其他云服务客户和未经授权的人员访问。**云服务实施指南：**

云服务客户	云服务提供商
（无附加实施指南）	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，以便： – 云服务客户在多租户环境中使用的资源分离； – 云服务提供商的内部管理与云服务客户使用的资源分离。 当云服务涉及多租户时，云服务提供商应实现信息安全控制，以确保不同租户使用的资

	源得到适当隔离。 云服务提供商应考虑在云服务提供商提供的云服务中运行客户提供的云服务软件的相关风险。

云服务的其他信息：

逻辑隔离的实现取决于应用于虚拟化的技术：

- 当软件虚拟化功能提供虚拟环境（例如，虚拟操作系统）时，可以虚拟化网络和存储配置。另外，在软件虚拟化环境中，可以利用软件的隔离功能来设计和实现云服务客户的隔离。
- 当云服务客户的信息与云服务的“元数据表”存储在物理共享的存储区域中时，可以通过对“元数据表”的访问控制实现与其他云服务客户的信息隔离。

“ISO/IEC 27040，信息技术-安全技术-存储安全”中给出了应用于云计算环境的安全多租户和相关指南。

CLD.9.5.2 虚拟机强化

控制：云计算环境中的虚拟机应该进行加固以满足业务需求。

云服务实施指南：

云服务客户	云服务提供商
在配置虚拟机时，云服务客户和云服务提供商应确保强化了适当的方面（例如，仅需要那些端口、协议和服务），并为所使用的每台虚拟机制定了适当的技术措施（例如，反恶意软件、日志记录）。	在配置虚拟机时，云服务客户和云服务提供商应确保强化了适当的方面（例如，仅需要那些端口、协议和服务），并为所使用的每台虚拟机制定了适当的技术措施（例如，反恶意软件、日志记录）。

CLD.12.1 操作程序和职责

ISO/IEC 27002 第 12.1 条规定的目标适用。

CLD.12.1.5 管理员的操作安全

控制：应定义、记录和监控云计算环境的管理操作过程。

云服务实施指南：

云服务客户	云服务提供商
云服务客户应该记录关键操作的过程，在这些操作中，故障可能会对云计算环境中的资产造成不可恢复的损坏。 关键操作的示例如下： - 安装、更改和删除虚拟化设备，如服务器、网络和存储； - 云服务使用终止程序； - 备份和恢复。 该文件应规定主管应监控这些操作。	云服务提供商应向需要的云服务客户提供有关关键操作和过程的文档。

云服务的其他信息：

云计算具有快速供应和管理以及按需自助服务的优点。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。由于这些关键操作中的人为干预可能导致严重的信息安全事件，因此应考虑保护这些操作的机制，并在必要时加以定义和实施。严重事件的例子包括删除或关闭大量虚拟服务器或销毁虚拟资产。

CLD.12.4 日志记录和监视

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：云服务客户应该能够监控云服务客户使用的云服务操作的特定方面。

云服务实施指南：

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每个云服务可用的服务监视功能的信息。	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相关的云服务操作的特定方面的功能。例如，监视和检测云服务是否被用作攻击他人的平台，或者敏感数据是否从云服务泄漏。 适当的访问控制应确保监视功能的使用。这些功能应该只提供对有关云服务客户自己的云服务实例的信息的访问。 云服务提供商应向云服务客户提供服务监控功能的文档。 监控应提供与第 12.4.1 条所述事件日志一致的数据，并协助处理 SLA 条款。

CLD.13.1 网络安全管理

ISO/IEC 27002 第 13.1 条规定的目标适用。

CLD.13.1.4 虚拟和物理网络安全管理的一致性

控制：在配置虚拟网络时，应根据云服务提供商的网络安全策略验证虚拟网络和物理网络之间配置的一致性。

云服务实施指南：

云服务客户	云服务提供商
（无附加实施指南）	云服务提供商应定义并记录虚拟网络配置的信息安全策略，该策略与物理网络的信息安全策略一致。云服务提供商应确保虚拟网络配置与信息安全策略匹配，而不考虑用于创建配置的方法。

云服务的其他信息

在基于虚拟化技术构建的云计算环境中，虚拟网络配置在物理网络上的虚拟基础设施上。在这种环境下，网络策略的不一致会导致系统中断或访问控制缺陷。

注意：根据云服务的类型，配置虚拟网络的责任在云服务客户和云服务提供商之间可能有所不同。

附件 B　与云计算相关的信息安全风险参考文献

（本附件不构成本建议|国际标准的组成部分。）

正确使用本建议提供的信息安全控制措施|国际标准有赖于本组织的信息安全风险评估和处理。虽然这些都是重要的主题，但本建议国际标准的重点不是信息安全风险评估和处理方法。以下是一个参考列表，其中包括提供和使用云服务时的风险源和风险的描述。需要注意的是，风险来源和风险因服务的类型和性质以及云计算的新兴技术而异。建议国际标准的用户在必要时参考文件的最新版本。

建议 ITU-T X.1601（2014），云计算安全框架。

澳大利亚政府信息管理办公室 2013 年，《澳大利亚政府机构隐私和云计算检查点摘要》，更好的实践指南，1.1 版，2 月，第 8 页。

http://www.finance.gov.au/files/2013/02/privacy-and-cloud-computing-for-australian-government-agencies-v1.1.pdf

澳大利亚政府网络安全中心 2015，租户云计算安全——4 月。

http://www.asd.gov.au/publications/protect/Cloud_Computing_Security_for_Tenants.pdf

澳大利亚政府网络安全中心 2015，云服务提供商的云计算安全–4 月。

http://www.asd.gov.au/publications/protect/Cloud_Computing_Security_for_Cloud_Service_Providers.pdf

云安全联盟 2014，云控制矩阵–1 月。

ENISA 2009，云计算安全风险评估–11 月。

ENISA2009，云计算信息保证框架–11 月。

香港 OGCIO 2013，云服务提供商处理个人身份识别的安全和隐私检查表

云平台中的信息–4 月。

香港 OGCIO 2013，云服务消费者安全检查表-一月。

ISACA 2012，云计算的安全考虑——7 月。

NIST，SP 800-144 2011，《公共云计算安全和隐私指南》，12 月。

NIST，SP 800-146 2012，云计算概要和建议——5 月。

2012 年春季新加坡，附件 A：新加坡虚拟化安全风险评估技术参考 30:2012

服务器虚拟化安全技术参考-三月。

2012 年新加坡之春，附件 A：审查新加坡 SaaS 时的安全和服务水平考量清单技术参考 31:2012

公共云计算服务使用安全和服务水平指南技术参考–3 月。

新加坡 2013 年春季，附件 A：云服务提供商披露新加坡标准 SS 584:2013 多层云计算安全规范-8 月。

2012 年新加坡之春，附件 B：审查《新加坡技术参考 31:2012 安全和服务水平指南》中的 IaaS 时的安全和服务水平考量清单，公共云计算服务使用技术参考 31:2012，3 月。

新加坡 2013 年春季，新加坡标准 SS 584:2013 多层云计算安全规范-8 月。

新加坡 2012 年春季，新加坡技术参考 30:2012 服务器虚拟化安全技术参考–3 月。

新加坡 2012 年春季，新加坡技术参考 31:2012 公共云计算服务使用安全和服务级别指南技术参考–3 月。

美国政府 FedRAMP PMO 2014，FedRAMP 安全控制基线版本 2.0–6 月。

参考文献

- ITU-T X.805（2003），提供端到端系统的安全体系结构通信。
- ISO/IEC 17203:2011，信息技术－开放虚拟化格式（OVF）规范。
- ISO/IEC 27001:2013，信息技术－安全技术－信息安全管理系统－要求。
- ISO/IEC 27005:2011，信息技术－安全技术－信息安全风险管理。
- ISO/IEC 27018:2014，信息技术－安全技术－作为 PII 处理器的公共云中个人识别信息（PII）保护实施规程。
- ISO/IEC 27036-1:2014，信息技术－安全技术－供应商关系的信息安全－第 1 部分：概述和概念。
- ISO/IEC 27036-2:2014,信息技术－安全技术－供应商关系的信息安全－第 2 部分:要求。
- ISO/IEC 27036-3:2013，信息技术－安全技术－供应商关系的信息安全－第 3 部分：信息和通信技术供应链安全指南。
- ISO/IEC CD 27036-4，信息技术－安全技术－供应商关系的信息安全－第 4 部分：云服务安全指南－正在开发中。
- ISO/IEC 27040:2015，信息技术－安全技术－存储安全。
- ISO 19440:2007，企业集成－企业建模结构。
- ISO 31000:2009，风险管理－原则和指南。
- NIST，SP 800-145 2011，NIST 对云计算的定义。
- NIST 2009，有效且安全地使用云计算范式。
- ENISA 2009，云计算的好处、风险和信息安全建议。
- 云安全联盟，云计算 V3.0 关键领域的安全指南。
- 云安全联盟，云计算 1.0 版的最大威胁。
- 云安全联盟，域 12：身份和访问管理指南 2.1 版。
- ISACA，《云计算：从安全、治理和保证的角度看的业务好处》。
- ISACA，云计算管理审计/保证计划。