bsi.

...making excellence a habit.™

ISO/IEC 27017

—ISO/IEC 27001的延伸

云计算服务的信息安全控制

白皮书

安全是云客户担忧的一大问题，尽管云有着出色的灵活性和可拓展性，但安全问题始终是组织在选择使用云服务过程中为何犹豫不决的原因之一。云客户主要的担忧在于云服务供应商(CSP)是否能够认真对待并且备充分重视客户数据。

安全问题主要在于担心数据最终可能会落入不法之徒手中，以及客户就那些粗心大意造成问题的运营商会采取什么样的控制措施。当然还存在这其它的担忧，例如：客户身份、虚拟服务器中的资产隔离、以及在云服务供应商出现停业的况下，资产会发生什么情况等，这些都是潜在云用户关注的问题。

ISO 27001系列标准可以帮助客户解决其中一些担忧，然而新标准——ISO/IEC 27017信息技术—安全技术，则能够更进一步解决问题，使潜在云客户更加安全放心地使用。详尽说明云供应商控制及指导原则的传统云标准和技术标准均旨在云服务供应商。而ISO/IEC 27017标准独特和极具益处的优势在于，它为CSP和云服务客户均提供了指导原则和建议。除了确保服务安全之外，ISO/IEC 27017还旨在让客户真正明白他们应当从其云主机获得什么。

该标准提供了ISO/IEC 27002中的37项控制指导及ISO/IEC 27002未涉及的7个新控制方面。

- **CLD.6.3.1**：客户和供应商之间就共同或单独责任达成协议，以清晰定义、记录和沟通与云服务相关的信息安全角色。
- **CLD.8.1.5**：明确当客户和供应商之间的合同/协议终止时，应如何将资产从云端退回或转移。
- **CLD.9.5.1**：供应商必须保护客户的虚拟环境并将其与其他客户和外部各方的环境分离。
- **CLD.9.5.2**：客户和供应商必须确保对虚拟机进行配置和增强，以满足组织的需求。
- **CLD.12.1.5**：客户有责任定义、记录和监控与云环境相关的管理运营和程序，在客户需要时，CSP要共享关于重要运营和程序的文档。
- **CLD.12.4.5**：供应商的能力将如何支持客户有效监控云计算环境中的活动。
- **CLD.13.1.4**：应进行一致性配置，从而使虚拟网络环境符合物理网络的信息安全政策。

角色与责任

角色、涉及问题（如数据所有权、访问控制和基础设施维护等）责任定义及责任分配的模糊不清，可能引起业务或法律纠纷；尤其在涉及第三方的情况下。正如该标准所规定：

> “云服务使用过程中，云服务供应商系统所创建或修改的数据和文件可能对于确保服务运营、恢复和连续性至关重要。资产所有权以及对于这些资产相关的操作（例如，备份和恢复操作）承担责任的各方应当被定义和记录。否则，将会存在云服务供应商假设云服务客户执行了这些重要任务（反之亦然）的风险，并且可能发生数据丢失。”

本质上来说，该标准要求从一开始就清晰定义各方职责。

安全控制

该标准不仅只是划分责任，还具有下列优势：ISO/IEC 27017更详细地定义了供应商应当实施安全控制的类型，这有助于减少云技术采用的障碍。

ISO/IEC 27017为云服务供应商提供了一种方法以表明已实施控制的级别。这意味着有记录的证据 — 由独立来源（例如，针对某些标准的认证）支持 — 可证明已实施适当的政策，最重要的是，已引入哪些类型的控制。在合同签署前，应当与云客户共享此信息，以规避未来可能出现的任何潜在问题。

在无法进行独立审核或者可能对信息安全构成更大风险的情况下，这一标准为CSP提供了选项以进行自评估。如果出现这种情况，CSP须告知客户已进行自评估。

密码保护

该标准还包含针对所采用密码保护的指导原则，适用于客户和供应商，因双方在此方面均承担责任。供应商应当告知客户如何使用密码保护，并帮助客户应用自身的那些保护措施。与此同时还应当虑到特殊情况，例如健康数据，因其可能涉及其他一些监管指导原则。

客户也应当坦诚告知其所使用的密码保护类型 — 如果风险分析表明有必要，他们应当采用密码保护。实际上，正因为存在争议或误解，才更需要标准。

双方不仅应当彼此确保网络被有效保护，还应当能够确保两个系统之间的兼容性。重要的是，应当确定这些控制是适用于存储的数据、传输的数据，或两者均用，因此处以往常常被误解。

客户关系

该标准对要求进行了拓展，不仅仅局限于技术，还为培训确立了知道原则。对于云服务供应商提供的基础设施，许多客户表示满意，若要进一步支持，则略显担忧。

因为毕竟有大量证据表明，员工往往是组织安全措施中的薄弱环节。客户不仅需要担忧存在缺陷的安全设备，而且还要担心员工是否遵循了所有适当的措施。此新标准不仅规定供应商应当让员工和承包商增强意识并为其提供相关培训，还规定培训应当涵盖监管要求、客户访问以及特定要求。

资产所有权

云资产归谁所有可能是另一外一个混淆点。该标准建议应当建立云储存资产清单，并且还重新提及了ISO/IEC 27002中所规定的针对资产所有权、可接受的资产使用及退还的指导原则信息。

新标准明确了安全处理客户资产的参数，从而使敏感数据不会被简单地“丢弃”于虚拟回收站中。

谁将获益？

答案显而易见：与云相关的任何一方。

通往云端之路常常伴随着误解和担忧。任何将敏感客户数据委托给第三方的组织已然意识到存在权利和责任未被清晰定义的灰色地带。

由于能够实现真正的云计算安全保障，由标准所支持的与CSP关系的变化将使CIO和IT经理深受鼓舞。当组织制定有关采用云技术的决策以及确定哪些合作伙伴能够满足其需求时，围绕ISO/IEC 27017的概述和实施培训被证明非常有帮助。

CSP实施ISO/IEC 27017也能从中受益，其为客户提供了可信赖的安全解决方案，从而有助于与客户建立基于云方面的长期合作关系。当然在与客户合作实施ISO/IEC 27017的过程中，亦可帮助CSP免受业务上的指控和诉讼，损害其品牌及生于。

bsi.

要了解更多信息

www.bsigroup.com
400 005 0046
infochina@bsigroup.com

关注bsi微信