CSA 一致性评估倡议问卷

2017 年 1 月

版权声明

本文档仅用于参考。本文档代表截至其发行之日的 AWS 的最新产品服务和实践，如有变更，恕不另行通知。客户负责对此文件的信息以及对 AWS 的产品或服务的任何使用进行自我独立的评估，每项产品或服务均按“原样”提供，无任何类型的保证，不管是明示还是暗示。本文档不形成 AWS、其附属公司、供应商或许可方的任何保证、表示、合同承诺、条件或担保。AWS 对其客户承担的责任和义务受 AWS 协议制约，本文档不是 AWS 与客户之间的协议的一部分，也不构成对该协议的修改。

目录

摘要

CSA 一致性评估倡议问卷提供了一组问题，它们是 CSA 预测云消费者和/或云审计师会向云提供商提出的问题。它包含一系列安全、控制和流程问题，可供广泛使用，可用于云提供商选择和安全评估。AWS 已完成此问卷调查，回答如下。

介绍

云安全联盟 (CSA) 是一个“非盈利性组织，其使命是推广最佳实践的使用，保证云计算领域的安全，提供云计算使用方面的培训，协助确保其他形式的计算的安全”。有关更多信息，请参阅 https://cloudsecurityalliance.org/about/。

各行安全领域的实践者、公司和协会均参与此组织，以便完成此使命。

CSA 一致性评估倡议问卷

控制组	CID	一致性评估问题	AWS 的回答
应用程序和界面安全 *应用程序安全*	AIS-01.1	您是否利用行业标准 (在成熟模型中构建安全 [BSIMM] 度量、Open Group ACS 可信技术提供商框架、NIST 等) 为您的系统/软件生命周期 (SDLC) 内建安全架构？	AWS 系统开发生命周期融合了行业最佳实践，其中包括由 AWS 安全团队执行的正式设计审查、威胁建模和完成风险评估。请参阅《AWS 安全过程概述》以了解更多详情。 AWS 已实施各种规程来管理新的资源开发。请参阅 ISO 27001 标准、附录 A、域 14 了解更多详情。AWS 已通过独立审计师的验证和认证，确认符合 ISO 27001 认证标准。
	AIS-01.2	在部署到生产环境之前，您是否使用自动化源代码分析工具来检测代码中的安全缺陷？	
	AIS-01.3	在部署到生产环境之前，您是否使用人工源代码分析来检测代码中的安全缺陷？	
	AIS-01.4	您是否依据系统/软件生命周期 (SDLC) 安全相关的行业标准来验证所有软件供应商？	
	AIS-01.5	(仅适用于 SaaS) 在部署到生产环境之前，您是否审查应用程序有无安全漏洞并解决所有问题？	

控制组	CID	一致性评估问题	AWS 的回答
应用程序和界面安全 *客户访问要求*	AIS-02.1	在授予客户对数据、资产和信息系统的访问权限之前，是否已按合同约定，补救了所有已识别的安全问题并到达合同与监管要求？	AWS 客户保留确保其对 AWS 的使用符合适用的法律法规的责任。AWS 通过行业资质证书、第三方鉴证、白皮书 (可在以下网址获取：http://aws.amazon.com/compliance)，并直接向 AWS 客户提供资质证书、报告和其他相关文档，向客户传达了其安全和控制环境信息。
	AIS-02.2	是否针对客户访问定义并记录了所有的要求和信任级别？	
应用程序和界面安全 *数据完整性*	AIS-03.1	是否已针对应用程序接口和数据库实施了数据输入和输出完整性例行检查 (例如，调节和编辑检查)，以防人工或系统处理错误或数据破坏？	AWS SOC 报告中所述的 AWS 数据完整性控制体系阐释了数据完整性控制贯穿所有阶段 (包括传输、存储和处理环节)。 此外，可参阅 ISO 27001 标准、附录 A、域 14 以了解更多信息。AWS 已通过独立审计师的验证和认证，确认符合 ISO 27001 认证标准。
应用程序和界面安全 *数据安全性/完整性*	AIS-04.1	您是否采用行业标准 (如 CDSA、MULITSAFE、CSA Trusted Cloud Architectural Standard、FedRAMP、CAESARS 等) 来设计数据安全架构？	AWS 数据安全架构是专为融合行业先进实践而设计。 有关 AWS 遵守的各种主要实践的更多信息，请参阅 AWS 认证、报告和白皮书 (http://aws.amazon.com/compliance)。
审计保障和合规性 *审计计划*	AAC-01.1	您是否生产使用结构化且行业认可的格式的审计声明 (如 CloudAudit/A6 URI Ontology、CloudTrust、SCAP/CYBEX、GRC XML、ISACA 云计算管理审计/保障程序等)？	AWS 已获得特定行业资质证书和独立第三方认证，并直接向 AWS 客户提供特定资质证书、报告和其他相关文档。
审计保障和合规性 *独立审计*	AAC-02.1	是否支持租户查看您的 SOC2/ISO 27001 或类似第三方审计报告或认证报告？	AWS 根据保密协议直接向客户提供第三方鉴证、认证、服务性机构控制体系 (SOC) 报告以及其他相关合规性报告。 AWS ISO 27001 认证可从此处下载。 AWS SOC 3 报告可从此处下载。 AWS 安全会定期扫描所有面向 Internet 的服务终端节点 IP 地址，检查是否存在安全漏洞 (扫描范围不包括用户实例)。AWS 安全会通知相关方修复发现的任何安全漏洞。另外，独立的安全公司会定期执行外部漏洞威胁评估。然后，将从这些评估中发现的问题以及相关建议进行归类并提交给 AWS 领导层。 另外，AWS 控制环境还接受内外审计和风险评估机构的定期评估。AWS 邀请外部认证机构和独立审计师审查并测试 AWS 的总体控制环境。
	AAC-02.2	您是否按照行业最佳实践与指南中的描述，定期对云服务基础设施执行网络渗透测试？	
	AAC-02.3	您是否按照行业最佳实践与指南中的描述，定期对云服务基础设施执行应用程序渗透测试？	

控制组	CID	一致性评估问题	AWS 的回答
	AAC-02.4	您是否按照行业最佳实践与指南中的描述，定期进行内部审计？	
	AAC-02.5	您是否按照行业最佳实践与指南中的描述，定期进行外部审计？	
	AAC-02.6	是否能根据租户要求向其提供渗透的测试结果？	
	AAC-02.7	是否能根据租户要求向其提供内外审计结果？	
	AAC-02.8	您是否设有内部审计程序，可进行跨职能的评估审计？	
审计保障和合规性 *信息系统法规映射*	AAC-03.1	您是否能够以逻辑方式隔离或加密用户的数据，以便仅针对一个租户输出数据，而不会无意中访问到其他租户的数据？	由 AWS 代表客户存储的所有数据均享有强大的租户隔离安全和控制保护。客户保留对其数据的控制权和所有权，因此有责任选择对数据加密。AWS 的几乎所有服务，包括 S3、EBS、SimpleDB 和 EC2，都支持客户使用自己的加密机制。VPC 的 IPSec 隧道也进行了加密。此外，客户还可利用 AWS Key Management Systems (KMS) 创建和控制加密密钥 (请参阅 https://aws.amazon.com/kms/)。有关更多信息，请参阅 AWS 云安全白皮书：http://aws.amazon.com/security AWS allows customers to perform their own backups to tapes using their own tape backup service provider.但是，磁带备份不是 AWS 提供的服务。Amazon S3 和 Glacier 服务旨在通过数据存储冗余实现接近零的数据丢失率，且数据持久性相当于采用多站点复制数据对象所达到的效果。要了解有关数据持久性和冗余的信息，请参阅 AWS 网站。
	AAC-03.2	发生故障或数据丢失时，是否能恢复特定客户的数据？	
	AAC-03.3	能否将客户数据的存储限制在特定的国家/地区或地理位置？	AWS 客户可以指定其内容所在的地理区域。除非应法律或政府部门的要求，否则 AWS 不会在未通知客户的情况下，从客户选择的区域移动客户的内容。有关可用区域的完整列表，请访问 AWS 全球基础设施页面。

控制组	CID	一致性评估问题	AWS 的回答
	AAC-03.4	您是否已设立满足以下要求的程序：监测相关司法管辖区的监管要求变更、调整安全计划以顺应法律要求变更、确保遵从相关的法规要求？	AWS 监测相关的法律和法规要求。 请参阅 ISO 27001 标准附录 18 了解更多详情。AWS 已通过独立审计师的验证和认证，确认符合 ISO 27001 认证标准。
业务连续性管理和运营恢复能力 *业务连续性计划*	BCR-01.1	您是否为租户提供地理上的弹性承载选项？	数据中心是在全球多个地区的集群中构建的。AWS 为客户提供在多个地理区域内以及在每个地理区域的多个可用区域之间放置实例并存储数据的灵活性。客户应自行设计其 AWS 使用方式，以利用多个区域和可用区。 有关更多信息，请参阅 AWS 云安全概述白皮书：http://aws.amazon.com/security。
	BCR-01.2	您是否提供租户将基础设施服务故障转移到其他提供商服务的功能？	
业务连续性管理和运营恢复能力 *业务连性测试*	BCR-02.1	业务连续性计划是否会按计划定期测试，或组织和或环境发生明显变化后进行测试，以确保其持续有效？	AWS 业务连续性政策与计划是根据 ISO 27001 标准进行开发和测试的。 请参阅 ISO 27001 标准、附录 A、域 17，了解有关 AWS 以及业务连续性的进一步详情。
业务连续性管理和运营恢复能力 *电力/通讯*	BCR-03.1	您是否向租户提供相关文档，显示数据在系统间的传输路径？	AWS 客户可以指定其数据和服务器所处的地理区域。除非应法律或政府部门的要求，否则 AWS 不会在未通知客户的情况下，从客户选择的区域移动客户的内容。AWS SOC 报告提供了更多详情。客户还可以选择至 AWS 设施的网络路径，包括由客户控制流量路径选择的高度专用的私有网络。
	BCR-03.2	租户能否定义如何传输其数据以及经过哪些法律辖区？	
业务连续性管理和运营恢复能力 文档	BCR-04.1	是否已向授权人员提供了信息系统文档 (例如：管理员和用户指南、架构图表等) 以确保信息系统的配置、安装和运行？	信息系统文档是通过 Amazon 局域网站向 AWS 内部人员提供的。有关更多信息，请参阅 AWS 云安全白皮书：http://aws.amazon.com/security/。 请参阅 ISO 27001 附录 A、域 12。
业务连续性管理和运营恢复能力 *环境风险*	BCR-05.1	是否针对因自然原因、自然灾害、蓄意攻击等而造成的损坏应用物理保护和其他对策？	AWS 数据中心包含针对环境风险的物理防护。AWS 针对环境风险的物理防护已经获得独立审计师的验证，符合 ISO 27002 最佳实践。 请参阅 ISO 27001 标准、附录 A、域 11。

控制组	CID	一致性评估问题	AWS 的回答
业务连续性管理和运营恢复能力 *设备位置*	BCR-06.1	目前是否有任何数据中心位于易受环境风险 (洪水、台风、地震、飓风等) 影响的地区？	AWS 数据中心包含针对环境风险的物理防护。AWS 针对环境风险的物理防护已经获得独立审计师的验证，符合 ISO 27002 最佳实践。请参阅 ISO 27001 标准、附录 A、域 11。
业务连续性管理和运营恢复能力 *设备维护*	BCR-07.1	如果使用虚拟基础设施，您的云解决方案是否具有独立于硬件的存储和恢复功能？	EBS 快照可供支持客户随时捕获和恢复虚拟机镜像。客户可以导出并在其内部或其他提供商处使用其 AMI (具体取决于软件许可限制)。有关更多信息，请参阅 AWS 云安全白皮书：http://aws.amazon.com/security。
	BCR-07.2	如果使用虚拟基础设施，您是否提供租户将虚拟机适时恢复到前一状态 (在时间上) 的能力？	
	BCR-07.3	如果使用虚拟基础设施，您是否支持将虚拟机镜像下载并传输到新的云提供商处？	
	BCR-07.4	如果使用虚拟基础设施，是否支持客户以在场外存储位置复制这些虚拟机镜像方式获取镜像？	
	BCR-07.5	您的云解决方案是否提供软件/提供商独立的恢复和还原功能？	
业务连续性管理和运营恢复能力 *设备电力故障*	BCR-08.1	您是否实施了安全冗余机制，以防设备遭到公共设施服务故障 (例如：停电、网络中断等) 的影响？	AWS 设备采取了公共设施服务故障防护措施，符合 ISO 27001 标准。AWS 已通过独立审计师的验证和认证，确认符合 ISO 27001 认证标准。 AWS SOC 报告对 AWS 控制体系进行了详细描述，这些体系用于尽可能减小故障或物理灾难对计算机和数据中心设施的影响。 此外，可参阅 AWS 云安全白皮书，网址为：http://aws.amazon.com/security。

控制组	CID	一致性评估问题	AWS 的回答
业务连续性管理和运营恢复能力 *影响分析*	BCR-09.1	您是否不间断地使租户了解并向其报告您的运营服务等级协议 (SLA) 的性能？	AWS CloudWatch 可对 AWS 云资源以及客户通过 AWS 运行的应用程序进行监控。请参阅 aws.amazon.com/cloudwatch 以了解更多详情。AWS 还在我们的服务运行状况仪表板上公布最新的服务可用性信息。请参阅 status.aws.amazon.com。
	BCR-09.2	您是否向租户提供基于标准的信息安全指标 (CSA、CAMM 等)？	
	BCR-09.3	您是否不间断地使客户了解并向其报告您的 SLA 的履行情况？	
业务连续性管理和运营恢复能力 *策略*	BCR-10.1	您是否已制定并使所有人员了解相关策略和程序以充分支持服务运营角色？	AWS 已通过基于 NIST 800-53、ISO 27001、ISO 27017、ISO 27018、ISO 9001 标准和 PCI DSS 要求的 AWS 信息安全框架，制定了相关策略和程序。 请参阅《AWS 风险与合规性》白皮书了解更多详情，网址为：http://aws.amazon.com/compliance。
业务连续性管理和运营恢复能力 *保留政策*	BCR-11.1	您是否具有强制实施租户数据保留政策的技术控制能力?	AWS 为客户提供删除数据的功能。但是，AWS 客户保留对其数据的控制权和所有权，因此客户负责管理数据的保留，以满足其要求。有关更多信息，请参阅 AWS 云安全白皮书：http://aws.amazon.com/security。 AWS 负责保护客户隐私权，并在判断遵从哪些执法部门的要求方面保持警惕。如果 AWS 认为执法部门发布的命令缺乏有力的根据，则会毫不犹豫地提出质询。有关其他信息，请参阅 https://aws.amazon.com/compliance/data-privacy-faq/。
	BCR-11.2	您是否拥有作业程序，以响应来自政府或第三方的租户数据请求？	
	BCR-11.4	您是否实施了备份或冗余机制，以确保满足法规、法律、合同或业务要求？	AWS 备份和冗余机制是按照 ISO 27001 标准开发和测试的。请参阅 ISO 27001 标准、附录 A、域 12 和 AWS SOC 2 报告，了解有关 AWS 备份和冗余机制的更多信息。
	BCR-11.5	您是否至少每年测试一次备份或冗余机制？	

控制组	CID	一致性评估问题	AWS 的回答
变更控制和配置管理 *新开发/采购*	CCC-01.1	您是否已制定相关策略和程序，用于管理针对开发或购买新的应用程序、系统、数据库、基础设施、服务、运营和设施的授权？	AWS 已通过基于 NIST 800-53、ISO 27001、ISO 27017、ISO 27018、ISO 9001 标准和 PCI DSS 要求的 AWS 信息安全框架，制定了相关策略和程序。 不管客户是初次使用 AWS 还是高级用户，都可在我们的网站 (https://aws.amazon.com/documentation/) 的 AWS 文档部分找到有关服务从入门到高级功能的实用文档。
	CCC-01.2	您是否提供了介绍产品/服务/功能安装、配置和使用的文档？	
变更控制和配置管理 *外包开发*	CCC-02.1	您是否实施了相应控制体系以确保所有软件开发均达到质量标准？	AWS 一般不会将软件开发外包。AWS 将质量标准融入系统开发生命周期 (SDLC) 流程中。 请参阅 ISO 27001 标准、附录 A、域 14 以了解更多详情。AWS 已通过独立审计师的验证和认证，确认符合 ISO 27001 认证标准。
	CCC-02.2	您是否实施了相应的控制体系，以针对任何已外包软件开发活动检测源代码安全缺陷？	
变更控制和配置管理 *质量测试*	CCC-03.1	您是否向租户提供描述您的质量控制流程的文档？	AWS 一直保有 ISO 9001 认证。这是对 AWS 质量体系的独立验证，并判定 AWS 活动符合 ISO 9001 标准。 AWS 安全公告旨在向客户通报安全和隐私事件。客户可在我们的网站上订阅 AWS 安全公告 RSS 源。请参阅 aws.amazon.com/security/security-bulletins/。 AWS 还在我们的服务运行状况仪表板上公布最新的服务可用性信息。请参阅 status.aws.amazon.com。 AWS 系统开发生命周期 (SDLC) 融合了行业最佳实践，其中包括由 AWS 安全团队执行的正式设计审查、威胁建模和完成风险评估。请参阅《AWS 安全过程概述》以了解更多详情。 此外，可参阅 ISO 27001 标准、附录 A、域 14 以了解更多详情。AWS 已通过独立审计师的验证和认证，确认符合 ISO 27001 认证标准。
	CCC-03.2	您是否提供了说明特定产品/服务已知问题的文档？	
	CCC-03.3	您是否设立了用于筛选和修复产品及服务已报告的错误和安全漏洞的策略和程序？	
	CCC-03.4	您是否具备了确保从所发布的软件版本中移除所有调试和测试代码元素的机制？	
变更控制和配置管理 *未授权软件安装*	CCC-04.1	您是否实施了相应的控制体系，以严格限制和监视在您的系统上安装未授权软件的行为？	AWS 用于管理恶意软件的计划、流程、程序符合 ISO 27001 标准。 请参阅 ISO 27001 标准、附录 A、域 12 以了解更多详情。AWS 已通过独立审计师的验证和认证，确认符合 ISO 27001 认证标准。

控制组	CID	一致性评估问题	AWS 的回答
变更控制和配置管理 *生产变更*	CCC-05.1	您是否向租户提供相关文档，描述您的生产变更管理程序以及租户在这个程序中的角色/权利/责任？	AWS SOC 报告对控制 AWS 环境变化的现有控制体系进行了概述。 此外，可参阅 ISO 27001 标准、附录 A、域 12 了解进一步详情。AWS 已通过独立审计师的验证和认证，确认符合 ISO 27001 认证标准。
数据安全和信息生命周期管理 *分类*	DSI-01.1	您是否提供通过策略标签/元数据识别虚拟机的功能 (例如：标签可用于限制操作系统在不适用国家/地区启动/实例化/传输数据)？	虚拟机是作为 EC2 服务的一部分配给客户的。客户保留对使用哪些资源以及在哪里驻存资源的控制权。请参阅 AWS 网站以了解更多详情，网址为：http://aws.amazon.com。
	DSI-01.2	您是否提供通过策略标签/元数据/硬件标签 (例如 TXT/TPM、VN 标签等) 识别硬件的功能？	AWS 提供给 EC2 资源贴标签的功能。EC2 标签是元数据的一种形式，可用于创建便于用户识别的名称，增强可搜索性并改善多个用户之间的协作。AWS 管理控制台也支持贴标签。
	DSI-01.3	您是否能够将系统地理位置用作身份验证因素？	AWS 提供基于 IP 地址控制用户访问的功能。客户可通过添加条件来控制用户使用 AWS 的方式，如时间、原始 IP 地址，或者是否可使用 SSL 等。
	DSI-01.4	您能否一经请求即刻提供租户数据存储的物理位置/地理方位？	AWS 让客户能够在多个地理区域内灵活存放实例和存储数据。AWS 客户指定其数据和服务器所处的物理位置。除非应法律或政府部门的要求，否则 AWS 不会在未通知客户的情况下，从客户选择的区域移动客户的内容。截至本白皮书编写之时，共有十二个区域：美国东部 (弗吉尼亚北部)、美国西部 (俄勒冈)、美国西部 (加利福尼亚北部)、AWS GovCloud (美国) (俄勒冈)、欧洲 (爱尔兰)、欧洲 (法兰克福)、亚太地区 (首尔) 、亚太地区 (新加坡)、亚太地区 (东京)、亚太地区 (悉尼)、中国 (北京) 区域和南美洲 (圣保罗)。
	DSI-01.5	您能否事先提供租户数据存储的物理位置/地理方位？	
	DSI-01.6	您是否遵循结构化数据标记标准 (例如：ISO 15489 、 Oasis XML Catalog Specification、CSA 数据类型指导)？	AWS 客户保留对其数据的控制权和所有权，可以自行实施结构化数据标记标准，以满足其要求。

控制组	CID	一致性评估问题	AWS 的回答
	DSI-01.7	是否支持租户为数据路由或资源实例化定义可接受的地理位置？	AWS 让客户能够在多个地理区域内灵活存放实例和存储数据。AWS 客户指定其数据和服务器所处的物理位置。除非应法律或政府部门的要求，否则 AWS 不会在未通知客户的情况下，从客户选择的区域移动客户的内容。截至本白皮书编写之时，共有十二个区域：美国东部 (弗吉尼亚北部)、美国西部 (俄勒冈)、美国西部 (加利福尼亚北部)、AWS GovCloud (美国) (俄勒冈)、欧洲 (爱尔兰)、欧洲 (法兰克福)、亚太地区 (首尔)、亚太地区 (新加坡)、亚太地区 (东京)、亚太地区 (悉尼)、中国 (北京) 区域和南美洲 (圣保罗)。
数据安全和信息生命周期管理 *数据清单/流程*	DSI-02.1	您是否设置了对服务应用程序和基础设施网络及系统中永久或临时保留的数据进行清点、记录和维护的数据流程？	AWS 客户可以指定其内容所在的地理区域。除非应法律或政府部门的要求，否则 AWS 不会在未通知客户的情况下，从客户选择的区域移动客户的内容。截至本白皮书编写之时，共有十二个区域：美国东部 (弗吉尼亚北部)、美国西部 (俄勒冈)、美国西部 (加利福尼亚北部)、AWS GovCloud (美国) (俄勒冈)、欧洲 (爱尔兰)、欧洲 (法兰克福)、亚太地区 (首尔)、亚太地区 (新加坡)、亚太地区 (东京)、亚太地区 (悉尼)、中国 (北京) 区域和南美洲 (圣保罗)。
	DSI-02.2	能否确保数据不迁移到规定以外的地理区域？	
数据安全和信息生命周期管理 *电子商务交易*	DSI-03.1	如果需要通过公共网络 (如 Internet) 传输租户数据，您是否向租户提供开放的加密方法 (3.4ES、AES 等)，以便保护其数据？	所有的 AWS API 均可通过 SSH 保护的终端节点访问，它们可提供服务器身份验证。AWS 的几乎所有服务，包括 S3、EBS、SimpleDB 和 EC2，都支持客户使用自己的加密机制。VPC 的 IPSec 隧道也进行了加密。此外，客户还可利用 AWS Key Management Systems (KMS) 创建和控制加密密钥 (请参阅 https://aws.amazon.com/kms/)。客户也可以使用第三方加密技术。 有关更多信息，请参阅 AWS 云安全白皮书：http://aws.amazon.com/security。
	DSI-03.2	当基础设施组件需要通过公共网络相互通信时 (例如：通过 Internet 将数据从一个环境复制到另一个环境)？	
数据安全和信息生命周期管理 *处理/标签/安全策略*	DSI-04.1	您是否已针对数据和包含数据的对象的标签、处理和安全建立策略和程序？	AWS 客户保留对数据的控制权和所有权，可以自行实施标签和处理政策及规程，以满足其要求。
	DSI-04.2	是否已对作为数据聚合容器的数据元实施标签继承机制？	

控制组	CID	一致性评估问题	AWS 的回答
数据安全和信息生命周期管理 *非生产数据*	DSI-05.1	您是否已采用适当流程，以确保生产数据不会被复制或用于非生产环境？	AWS 客户保留对其数据的控制权和所有权。AWS 为客户提供维护和开发生产和非生产环境的能力。确保其生产数据不会被复制到非生产环境是客户的责任。
数据安全和信息生命周期管理 *所有权/管理权*	DSI-06.1	您是否规定、分配、记录和传达了数据管理权的相关责任？	AWS 客户保留对其数据的控制权和所有权。有关更多信息，请参阅 AWS 客户协议。
数据安全和信息生命周期管理 *安全报废*	DSI-07.1	您是否支持按租户的决定安全删除 (如：消磁/去除加密) 已存档和备份的数据？	当某个存储设备已达到其使用寿命的终点时，AWS 程序包括一个退役进程，此进程是为防止客户数据暴露给未授权的个人而设计的。作为退役流程的一部分，AWS 会使用 DoD 5220.22-M (“国家行业安全程序操作手册”) 或 NIST 800-88 (“存储介质清理指南”) 中详细描述的技术来销毁数据。如果无法使用这些程序来报废硬件设备，将依据行业标准实践进行消磁或物理销毁。有关更多信息，请参阅 AWS 云安全白皮书：http://aws.amazon.com/security。 Amazon EBS 卷作为原始未格式化的块设备提供给您，在使它可供使用之前已经对它进行了擦除。重用之前立即擦除，以便您可以确认完成擦除操作。如果您具有要求通过某个特定方法擦除所有数据的程序，例如 DoD 5220.22-M (“国家行业安全程序操作手册”) 或 NIST 800-88 (“媒介卫生处理指南”) 中详述的程序，就有在 Amazon EBS 上执行此操作的能力。您在删除卷之前应该进行专门的擦除程序，以满足您已规定的要求。 敏感数据加密通常是一种不错的安全做法，并且 AWS 允许用户使用 AES-256 对 EBS 卷及其快照进行加密。加密还发生在托管 EC2 实例的服务器上，当数据在 EC2 实例和 EBS 存储之间移动时提供数据加密。为了高效并以较低延迟执行此操作，EBS 加密功能只在更强大的 EC2 实例类型 (如 M3、C3、R3、G2) 上提供。
	DSI-07.2	您是否能提供用于退出服务的公开程序，包括当客户退出您的环境或腾空资源后，保证清除所有租户数据计算资源的程序。	
数据中心安全 *资产管理*	DCS-01.1	您是否保留了全部重要资产的完整清单，包括资产所有关系？	为了达到 ISO 27001 标准，AWS 硬件资产分配给一个所有人，由 AWS 专人通过 AWS 财产管理工具进行跟踪和监视。AWS 采购和供应团队会与所有 AWS 供应商保持联系。 请参阅 ISO 27001 标准；附录 A、域 8 以了解更多详情。AWS 已通过独立审计师的验证和认证，确认符合 ISO 27001 认证标准。
	DCS-01.2	您是否保留了包含全部重要供应商的完整清单？	

控制组	CID	一致性评估问题	AWS 的回答
数据中心安全 *控制的访问点*	DCS-02.1	是否实施了实体周边安全防护措施 (如隔离栅、围墙、障碍、守卫、大门、电子监视、实体身份验证机制、接待处以及安全巡逻)?	物理安全控制包括但不限于界限控制，如隔离栏、围墙、保安人员、视频监视、入侵检测系统以及其他电子方式。AWS SOC 报告提供了与 AWS 执行的特定控制活动有关的更多详情请参阅 ISO 27001 标准；附录 A、域 11 了解进一步信息。AWS 已通过独立审计师的验证和认证，确认符合 ISO 27001 认证标准。
数据中心安全 *设备识别*	DCS-03.1	自动化设备识别是否已用作一种方法，用于根据已知设备的位置验证连接身份验证的完整性?	AWS 对设备识别的管理符合 ISO 27001 标准。 AWS 已通过独立审计师的验证和认证，确认符合 ISO 27001 认证标准。
数据中心安全 *异地授权*	DCS-04.1	您是否向租户提供相关文档，描述将数据从一个物理位置转移到另一个的各种方案。(例如，异地备份、业务连续性故障转移、复制)	AWS 客户可以指定其数据所在的地理区域。除非应法律或政府部门的要求，否则 AWS 不会在未通知客户的情况下，从客户选择的区域移动客户的内容。 有关更多信息，请参阅 AWS 云安全白皮书：http://aws.amazon.com/security。
数据中心安全 *离线设备*	DCS-05.1	您能否向租户提供证明文档，描述控制资产管理和设备再利用策略和程序?	为了满足 ISO 27001 标准，当存储设备的有效使用寿命即将完结时，AWS 程序中包含了防客户数据泄露给没有授权的个人的报废流程。作为退役流程的一部分，AWS 会使用 DoD 5220.22-M (“国家行业安全程序操作手册”) 或 NIST 800-88 (“存储介质清理指南”) 中详细描述的技术来销毁数据。如果无法使用这些程序来报废硬件设备，将依据行业标准实践进行消磁或物理销毁。 请参阅 ISO 27001 标准；附录 A、域 8 以了解更多详情。AWS 已通过独立审计师的验证和认证，确认符合 ISO 27001 认证标准。
数据中心安全 *策略*	DCS-06.1	您是否能提供证据，证明已制定相应的策略、标准和程序，用于在办公室、房间、设施和安全地区维持一个安全无忧的工作环境?	AWS 邀请外部认证机构和独立审计师通过合规性框架审查，来验证我们的合规性。AWS SOC 报告提供了 AWS 执行的具体物理安全控制活动的更多详情。请参阅 ISO 27001 标准；附录 A、域 11 以了解更多详情。AWS 已通过独立审计师的验证和认证，确认符合 ISO 27001 认证标准。

控制组	CID	一致性评估问题	AWS 的回答
	DCS-06.2	您能否提供证据，以证明您的员工、相关第三方经过明文规定的策略、标准和程序方面的培训？	为了达到 ISO 27001 标准，所有 AWS 均已完成需要专家提供的定期信息安全培训。定期执行合规性审查，以验证员工是否了解并遵从既定策略。有关更多信息，请参阅 AWS 云安全白皮书：http://aws.amazon.com/security。 AWS 已通过独立审计师的验证和认证，确认符合 ISO 27001 认证标准。此外，AWS SOC 1 和 SOC 2 报告还提供进一步信息。
数据中心安全 *安全区域授权*	DCS-07.1	您是否支持租户指定其数据流经哪些地理位置(需基于所存储、访问数据所在的位置解决合法管辖权事宜)？	AWS 客户指定其数据所在的地理区域。除非应法律或政府部门的要求，否则 AWS 不会在未通知客户的情况下，从客户选择的区域移动客户的内容。截至本白皮书编写之时，共有十二个区域：美国东部 (弗吉尼亚北部)、美国西部 (俄勒冈) 、美国西部 (加利福尼亚北部) 、AWS GovCloud (美国) (俄勒冈)、欧洲 (爱尔兰)、欧洲 (法兰克福)、亚太地区 (首尔)、亚太地区 (新加坡)、亚太地区 (东京)、亚太地区 (悉尼)、中国 (北京) 区域和南美洲 (圣保罗)。
数据中心安全 *未授权人员进入*	DCS-08.1	您是否存在这样的出入口 (例如服务区或其他地点)，可能让未经授权的人员通过这些地点进入受监控、受控制以及远离数据存储和处理的地点？	周边和建筑物入口的物理访问受到严格控制，包括但不限于专业的安保人员利用视频监控、入侵检测系统和其他电子方式执行此工作。授权员工必须经过至少两次双重身份验证才能进入数据中心层。服务器地点的物理入口点根据 AWS 数据中心物理安全政策的规定，采用闭路电视摄像机 (CCTV) 进行影像记录。
数据中心安全 *用户访问*	DCS-09.1	您是否限制用户和支持人员对信息资产和功能的物理访问？	在审核我们的 SOC、PCI DSS、ISO 27001 和 FedRAMP 合规性期间，独立的外部审计师将审核 AWS 物理安全机制。
加密和密钥管理 *授权*	EKM-01.1	您是否设置了将密钥与可识别的所有者绑定的密钥管理策略？	AWS 支持客户对几乎所有服务 (包括 S3、EBS 和 EC2) 使用自己的加密机制。VPC 会话也是加密的。此外，客户还可利用 AWS Key Management Systems (KMS) 创建和控制加密密钥 (请参阅 https://aws.amazon.com/kms/)。 AWS 在内部为 AWS 基础设施内采用的所需密码术创建密钥并进行管理。AWS 生成的安全密钥和凭证管理器用于创建、保护和分发对称密钥，并用于保护和分配以下内容：主机上所需的 AWS 凭证、RSA 公有/私有密钥和 X.509 认证。 AWS 加密过程由独立的第三方审计师进行审查，以便让我们持续符合 SOC、PCI DSS、ISO 27001 和 FedRAMP。

控制组	CID	一致性评估问题	AWS 的回答
加密和密钥管理 *密钥生成*	EKM-02.1	您能否给每个租户创建唯一的加密密钥？	AWS 的几乎所有服务，包括 S3、EBS 和 EC2，都支持客户使用自己的加密机制。VPC 的 IPSec 隧道也进行了加密。此外，客户还可利用 AWS Key Management Systems (KMS) 创建和控制加密密钥 (请参阅 https://aws.amazon.com/kms/)。有关 KMS 的更多信息，请参阅 AWS SOC 报告。 有关更多信息，请参阅 AWS 云安全白皮书：http://aws.amazon.com/security。 AWS 在内部为 AWS 基础设施内采用的所需密码术创建密钥并进行管理。AWS 在 AWS 信息系统中使用由 NIST 批准的密钥管理技术来生成、控制和分发对称加密密钥。AWS 生成的安全密钥和凭证管理器用于创建、保护和分发对称密钥，并用于保护和分配以下内容：主机上所需的 AWS 凭证、RSA 公有/私有密钥和 X.509 认证。 AWS 加密过程由独立的第三方审计师进行审查，以便让我们持续符合 SOC、PCI DSS、ISO 27001 和 FedRAMP。
	EKM-02.2	您是否能代表租户管理加密密钥？	
	EKM-02.3	您是否维护密钥管理程序？	
	EKM-02.4	您是否记录了加密密钥生命周期各个阶段的所有权？	
	EKM-02.5	您是否利用任意第三方/开源/专有框架来管理加密密钥？	
加密和密钥管理 *加密*	EKM-03.1	您是否将您的环境中的静态租户数据加密 (即磁盘/存储上的数据)？	AWS 的几乎所有服务，包括 S3、EBS 和 EC2，都支持客户使用自己的加密机制。VPC 的 IPSec 隧道也进行了加密。此外，客户还可利用 AWS Key Management Systems (KMS) 创建和控制加密密钥 (请参阅 https://aws.amazon.com/kms/)。有关 KMS 的更多信息，请参阅 AWS SOC 报告。 有关更多信息，请参阅 AWS 云安全白皮书：http://aws.amazon.com/security。
	EKM-03.2	您是否利用加密来保护在网络和管理程序实例间传输的数据和虚拟机映像？	
	EKM-03.3	您是否支持租户生成加密密钥或支持租户将数据加密到没有公有密钥证书访问权限的身份 (如基于身份的加密)？	
	EKM-03.4	您是否设有制订和规定加密管理策略、程序和准则的文档？	

控制组	CID	一致性评估问题	AWS 的回答
加密和密钥管理 *存储和访问*	EKM-04.1	您是否具有使用开放/已验证格式和标准算法的平台和数据加密措施？	AWS 的几乎所有服务，包括 S3、EBS 和 EC2，都支持客户使用自己的加密机制。此外，客户还可利用 AWS Key Management Systems (KMS) 创建和控制加密密钥 (请参阅 https://aws.amazon.com/kms/)。有关 KMS 的更多信息，请参阅 AWS SOC 报告。 AWS 为 AWS 基础设施内采用的所需密码术创建密钥并进行管理。AWS 在 AWS 信息系统中使用由 NIST 批准的密钥管理技术来生成、控制和分发对称加密密钥。AWS 生成的安全密钥和凭证管理器用于创建、保护和分发对称密钥，并用于保护和分配以下内容：主机上所需的 AWS 凭证、RSA 公有/私有密钥和 X.509 认证。 AWS 加密过程由独立的第三方审计师进行审查，以便让我们持续符合 SOC、PCI DSS、ISO 27001 和 FedRAMP。
	EKM-04.2	您的加密密钥由云消费者还是可信的密钥管理供应商持有？	
	EKM-04.3	您将加密密钥存储在云中吗？	
	EKM-04.4	您是否有独立的密钥管理和密钥使用职责？	
治理和风险管理 *底线安全*	GRM-01.1	您是否已针对基础设施 (例如：管理程序、操作系统、路由器、DNS 服务器等) 的每个组件记录信息安全基线？	为达到 ISO 27001 标准，AWS 保持着每个重要组件的系统基线。请参阅 ISO 27001 标准、附录 A、域 14 和 18 了解更多详情。AWS 已通过独立审计师的验证和认证，确认符合 ISO 27001 认证标准。 客户可提供自己的虚拟机镜像。VM Import 使客户能够将虚拟机映像从现有环境轻松导入 Amazon EC2 实例。
	GRM-01.2	您是否能针对信息安全基线持续监视并报告基础设施的合规性情况？	
	GRM-01.3	您是否支持客户提供其信任的虚拟机镜像，以确保符合其内部标准？	
治理和风险管理 *风险评估*	GRM-02.1	您是否提供对健康数据的安全控制，以支持租户实施行业标准连续性监视 (支持租户持续验证您的物理和逻辑控制状态)？	AWS 确实公布了独立审计报告和资质证书，用以向客户提供关于由 AWS 制定和运行的策略、流程和控制体系的大量信息。可向 AWS 客户提供相关资质证书和报告。客户可在其自己的系统上执行对逻辑控制体系的持续监视。
	GRM-02.2	您是否至少每年执行一次与数据治理要求相关的风险评估？	为了达到 ISO 27001 标准，AWS 通过维护风险管理计划来抑制并管理风险。此外，AWS 一直保有 AWS ISO 27018 认证。符合 ISO 27018 可向客户证明 AWS 已实施了专门用于解决客户内容隐私保护问题的控制体系。有关更多信息，请参阅 AWS 合规性 ISO 27018 常见问题：http://aws.amazon.com/compliance/iso-27018-faqs/。

控制组	CID	一致性评估问题	AWS 的回答
治理和风险管理 *管理监督*	GRM-03.1	您的技术、业务和行政主管是否负责使自己及员工了解并遵从与其职责范围相关安全策略、程序、标准？	Amazon 的控制环境的起点是最高级别，即公司。公司的管理层和高级领导层在建立公司的基调和核心价值方面起重要作用。每名员工均可获得公司的商业行为和道德准则，并完成定期培训。执行合规性审计，以使员工理解并遵从既定策略。请参阅《AWS 风险与合规性》白皮书了解更多详情，网址为：http://aws.amazon.com/compliance。
治理和风险管理 *管理计划*	GRM-04.1	是否向租户提供了描述信息安全管理计划 (ISMP) 的文档？	AWS 向客户提供了 ISO 27001 认证。ISO 27001 认证专门针对 AWS ISMS，并且针对 AWS 的内部流程遵循 ISO 标准的情况进行评测。认证意味着经由第三方认可的独立审计机构已经对我们的流程和控制进行了评估，并确认他们的操作遵循了 ISO 27001 认证标准。有关更多信息，请参阅 AWS 合规性 ISO 27001 常见问题网站：http://aws.amazon.com/compliance/iso-27001-faqs/。
	GRM-04.2	您是否至少每年审查一次信息安全管理计划 (ISMP)？	
治理和风险管理 *管理支持/参与*	GRM-05.1	您是否与供应商签署相关协议以确保其遵守您的信息安全和隐私策略？	AWS 已建立了信息安全框架和策略，并根据 ISO 27002 控制体系、美国注册公开会计师协会 (AICPA) 信托服务原则、PCI DSS V3.1 和美国国家标准与技术研究院 (NIST) 刊物 800-53 (即：《联邦信息系统安全控制推荐》) 集成了 ISO 27001 可认证框架。 AWS 管理第三方关系以使其符合 ISO 27001 标准。 在审核我们的 PCI DSS、ISO 27001 和 FedRAMP 合规性期间，独立的外部审计师将审核 AWS 第三方要求。 有关 AWS 合规性计划的信息，请访问我们的网站：http://aws.amazon.com/compliance/。
治理和风险管理 *策略*	GRM-06.1	您的信息安全和隐私策略是否符合行业标准 (ISO-27001、ISO-22307、CoBIT 等)？	
	GRM-06.2	您是否已与供应商签署相关协议，确保其遵守您的信息安全和隐私策略？	
	GRM-06.3	您是否可以提供证据，能够反映您已针对规章和/或标准尽职管理了您的控制体系、架构和流程？	
	GRM-06.4	您是否公开自己遵循的控制体系、标准、认证和/或法规？	

控制组	CID	一致性评估问题	AWS 的回答
治理和风险管理 *策略执行*	GRM-07.1	针对违反安全策略和程序的员工，是否有正式的惩罚或制裁策略？	AWS 为员工提供安全策略和安全培训，按他们的角色和责任提供有关信息安全方面的教育。违反 Amazon 标准或协议的员工将受到调查，随后会采取适当的惩罚措施 (如：警告、写行动计划、停职和/或终止雇佣合同)。 有关更多信息，请参阅 AWS 云安全白皮书：http://aws.amazon.com/security 。请参阅 ISO 27001 附录 A、域 7 了解更多详情。AWS 已通过独立审计师的验证和认证，确认符合 ISO 27001 认证标准。
	GRM-07.2	是否已使员工了解，如果发生违反行为，公司可能会采取策略和程序中的哪些措施？	
治理和风险管理 *业务/策略变更影响*	GRM-08.1	是否在风险评估结果包含对安全策略、程序、标准以及控制体系的更新，可确保风险评估结果的相关性和有效性？	根据 ISO 27001 标准，AWS 每年对 AWS 安全策略、程序、标准和控制体系进行一次更新。 有关更多信息，请参阅 ISO 27001。AWS 已通过独立审计师的验证和认证，确认符合 ISO 27001 认证标准。
治理和风险管理 *策略审查*	GRM-09.1	当您更改信息安全和/或隐私策略时，是否通知租户？	AWS 会定期更新其 AWS 云安全白皮书和《风险与合规性》白皮书 (网址：http://aws.amazon.com/security 和 http://aws.amazon.com/compliance)，以反映 AWS 策略的更新情况。
	GRM-09.2	您是否至少每年审查一次隐私策略和安全策略？	AWS SOC 报告提供了与隐私策略和安全策略审查有关的详细信息。
治理和风险管理 *评估*	GRM-10.1	正式风险评估是否符整个企业的框架？是否每年至少执行一次或按计划定期执行风险评估？从而使用定性和定量方法确定所有已识别风险的可能性及其影响。	为了达到 ISO 27001 标准，AWS 制定了风险管理计划来抑制并管理风险。 AWS 已通过独立审计师的验证和认证，确认符合 ISO 27001 认证标准。 请参阅《AWS 风险与合规性》白皮书 (网址为：aws.amazon.com/security) 以了解有关 AWS 风险管理框架的更多详情。
	GRM-10.2	就所有风险类别而言 (例如，审计结果、威胁和漏洞分析以及监管合规性)，是否独立确定与固有风险与残余风险相关的可能性和影响？	

控制组	CID	一致性评估问题	AWS 的回答
治理和风险管理 *计划*	GRM-11.1	您是否制订并实施了涵盖整个组织的风险管理计划？	为了达到 ISO 27001 标准，AWS 通过维护风险管理计划来抑制并管理风险。 AWS 管理已制定战略业务计划，其中包括风险识别和控制体系的实施，从而减轻或管理风险。AWS 管理会每隔半年重新对该战略业务计划进行一次评估。此过程要求管理层识别其负责区域内的风险并实施已设计好的相应措施来解决那些风险。 在审核我们的 PCI DSS、ISO 27001 和 FedRAMP 合规性期间，独立的外部审计师将审核 AWS 风险管理计划。
	GRM-11.2	您是否公开了涵盖整个组织的风险管理计划文档？	
人力资源 *资产收益*	HRS-01.1	现有系统是否会监视违反保密性行为？在发现可能会影响租户数据的侵犯隐私权事件时，系统是否会迅速通知租户？	AWS 客户保留监视其环境、防止违反保密性行为的责任。 AWS SOC 报告提供了监视 AWS 托管环境的现有控制体系的概述。
	HRS-01.2	您的隐私策略是否符合行业标准？	
人力资源 *背景审查*	HRS-02.1	您是否依据当地法律、规章、道德和合同要求，对所有雇佣候选人、合约商以及第三方进行过背景调查？	AWS 在雇佣员工前，会根据招聘职位以及该职位可访问 AWS 设施的级别，对候选人进行筛选，而作为该筛选流程的一部分，AWS 会依据相应法律进行犯罪背景调查。 AWS SOC 报告提供了针对背景调查实施的控制体系的详细信息。
人力资源 *雇佣合同*	HRS-03.1	您是否就员工的特定角色及其必须满足的信息安全控制要求为员工提供专门的培训？	为了达到 ISO 27001 标准，所有 AWS 员工均须完成基于角色的定期培训，其中包括 AWS 安全培训和对需完成内容的要求。定期执行合规性审查，以验证员工是否了解并遵从既定策略。有关更多信息，请参阅 SOC 报告。 支持 AWS 系统和设备的所有人员都必须先签订保密协议，然后才能获得访问权。此外，一经雇佣，员工必须阅读并接受可接受使用策略和 Amazon 商业行为和道德准则 (行为准则) 策略。
	HRS-03.2	是否记录了完成培训的员工的信息？	
	HRS-03.3	为保护客户/租户信息，您是否要求所有人员在入职前都必须签署 NDA 或保密协议？	
	HRS-03.4	要获得和维持对敏感系统的访问权限，是否必须先成功、按时完成培训计划？	
	HRS-03.5	人员是否至少每年参加一次安全意识培训计划？	

控制组	CID	一致性评估问题	AWS 的回答
人力资源 *雇佣终止*	HRS-04.1	是否制订并实施了管理雇佣和/或解雇相关问题的策略、程序和准则？	AWS 人力资源团队定义了内部管理责任，以便在雇佣中止、员工和供应商角色变更时，有章可循。 AWS SOC 报告提供了更多详情。
	HRS-04.2	上述程序和准则是否规定了及时撤消访问权限和返回资产？	当 Amazon 人力资源系统终止员工的记录时，系统会自动取消访问权限。当员工的工作职能发生变化时，必须明确批准继续访问权限，否则将被自动取消。AWS SOC 报告提供了有关用户访问权限取消的详细信息。此外，AWS 安全白皮书的“员工生命周期”部分还提供了其他信息。 请参阅 ISO 27001 附录 A、域 7 了解更多详情。AWS 已通过独立审计师的验证和认证，确认符合 ISO 27001 认证标准。
人力资源 *便携性/移动设备*	HRS-05.1	是否已制定相关策略和程序，并采取了相关措施来严格限制便携和移动设备 (包括笔记本电脑、移动电话、电子记事簿 (PDA)) 对敏感数据和租户数据的访问？一般而言，这些设备访问敏感数据的风险系数要于非便携设备 (例如：提供商组织设施内的台式电脑)。	客户保留对其数据和相关媒体资产的控制权和责任。管理移动安全设备和客户内容访问权限是客户的责任。
人力资源 *保密协议*	HRS-06.1	关于反映组织对于保护数据和运营细节的需要的保密协议要求，是否按计划定期进行鉴定、验证和审查？	Amazon 法律顾问管理并定期修订 Amazon 保密协议，以反映 AWS 业务需要。
人力资源 *角色/责任*	HRS-07.1	您是否向租户提供了角色定义文档，清楚阐述了您与租户的管理责任？	AWS 云安全白皮书和 AWS 风险与合规性白皮书提供了有关 AWS 与客户的角色和责任的详细信息。白皮书下载地址：http://aws.amazon.com/security 和 http://aws.amazon.com/compliance。
人力资源 *可接受使用*	HRS-08.1	您是否会提供有关您如何访问租户数据和元数据的记录？	AWS 有一个正式访问控制策略，该策略每年 (或者在发生影响该策略的任何重大系统变化时) 都会接受审查和更新。该策略陈述了目的、范围、角色、责任和管理承诺。AWS 采用了最小权限的概念，即仅允许用户为实现其工作职能而进行的必要访问。 客户保留对其数据和相关媒体资产的控制权和责任。管理移动安全设备和客户内容访问权限是客户的责任。
	HRS-08.2	您是否通过检测技术 (如搜索引擎等) 收集或创建有关租户数据使用情况的元数据？	

控制组	CID	一致性评估问题	AWS 的回答
	HRS-08.3	您是否支持租户选择不支持通过检测技术访问其数据/元数据？	请参阅 ISO 27001 标准和 27018 实施规程了解更多信息。AWS 已通过独立审计师的验证和认证，确认符合 ISO 27001 和 ISO 27018 认证标准。
人力资源 *培训/认知*	HRS-09.1	您是否已向具有租户数据访问权限的所有人员提供安全意识方面基于角色的正式培训计划，帮助其了解有关云访问权限和数据管理方面的问题（如：多租户、国籍、云交付模式职责划分影响、利益冲突）？	为了达到 ISO 27001 标准，所有 AWS 均已完成需要专家提供的定期信息安全培训。定期执行合规性审查，以验证员工是否了解并遵从既定策略。 在审核我们的 SOC、PCI DSS、ISO 27001 和 FedRAMP 合规性期间，独立的外部审计师将审核 AWS 角色和责任。
	HRS-09.2	系统管理员和数据管理员是否就与安全性和数据完整性方面的法律责任接受过适当的培训？	
人力资源 *用户责任*	HRS-10.1	是否已使用户意识到其在保持遵从已公布安全策略、程序、标准和适用法规要求方面的责任？	AWS 在全球范围内使用各种内部通信方法，帮助员工了解他们各自的任务和责任，并及时传达重大事件。这些方式包括针对新进员工的入职培训计划、电子邮件信息以及通过 Amazon 局域网发布信息。请参阅 ISO 27001 标准、附录 A、域 7 和 8。AWS 已通过独立审计师的验证和认证，确认符合 ISO 27001 认证标准。此外，可参阅 AWS 云安全白皮书了解更多详情，网址为：http://aws.amazon.com/security。
	HRS-10.2	是否使用户意识到其在维持安全无忧的工作环境方面的责任？	
	HRS-10.3	是否使用户意识到其有责任以安全的方式离开自动化装置？	
人力资源 *工作空间*	HRS-11.1	您的数据管理策略和程序是否解决了租户与服务水平利益冲突问题？	AWS 数据管理策略符合 ISO 27001 标准。请参阅 ISO 27001 标准、附录 A、域 8 和 9。AWS 已通过独立审计师的验证和认证，确认符合 ISO 27001 认证标准。AWS SOC 报告提供了 AWS 为防止未授权访问 AWS 资源而执行的特定控制活动的有关详情。 AWS 已确定 AWS 系统内的系统和设备中可审核的事件类别。服务团队将根据要求配置审核功能以持续记录安全相关事件。审核记录包含一组数据元素以满足必要的分析要求。此外，审核记录可供 AWS 安全团队或其他合适的团队按需执行检查或分析，并且响应安全相关事件或影响业务的事件。
	HRS-11.2	您的管理策略和程序是否包含针对未授权访问租户信息的篡改审计或软件完整性功能？	
	HRS-11.3	虚拟机管理基础设施是否包含检篡改审计或软件完整性功能，用以检测对虚拟机构建/配置的更改？	

控制组	CID	一致性评估问题	AWS 的回答
身份和权限管理 *审计工具访问*	IAM-01.1	您是否限制、记录并监视对您的信息安全管理系统的访问？(如管理程序、防火墙、漏洞扫描程序、网络嗅探器、API 等)	为了达到 ISO 27001 标准，AWS 已制定正式的策略和程序，以描述对 AWS 资源进行逻辑访问的最低标准。AWS SOC 报告概述了管理 AWS 资源访问权限配置的现有控制体系。 有关更多信息，请参阅 AWS 云安全白皮书：http://aws.amazon.com/security。
	IAM-01.2	您是否监视和记录对您的信息安全管理系统的特权访问 (管理员级别)？	AWS 已确定 AWS 系统内的系统和设备中可审核的事件类别。服务团队将根据要求配置审核功能以持续记录安全相关事件。日志存储系统旨在提供高度可扩展且高度可用的服务，此类服务会随着日志存储量的增长而自动增加容量。审核记录包含一组数据元素以满足必要的分析要求。此外，审核记录可供 AWS 安全团队或其他合适的团队按需执行检查或分析，并且响应安全相关事件或影响业务的事件。 AWS 团队中的指定人员将接收审核处理失败时的自动警告。审核处理失败包括软件/硬件错误等。当收到提醒时，随时待命的人员会发出一份故障单并跟踪该事件，直到该事件得到解决。 AWS 日志记录和监控过程由独立的第三方审计师进行审查，以便让我们持续符合 SOC、PCI DSS、ISO 27001 和 FedRAMP 合规性。
身份和权限管理 *用户访问政策*	IAM-02.1	是否已实施相应的控制体系，确保及时删除业务不再需要的系统访问权限？	AWS SOC 报告提供了有关用户访问权限取消的详细信息。此外，AWS 安全白皮书的“员工生命周期”部分还提供了其他信息。 请参阅 ISO 27001 附录 A、域 9 了解更多详情。AWS 已通过独立审计师的验证和认证，确认符合 ISO 27001 认证标准。
	IAM-02.2	您是否提供了相应的度量，用以跟踪何时能够删除业务不再需要的系统访问权限？	
身份和权限管理 *诊断/配置端口访问权限*	IAM-03.1	您是否利用专用安全网络来提供对云服务基础设施的管理访问权限？	现有控制体系会根据 AWS 访问政策限制对系统和数据的访问，并且约束和监视对系统和数据的访问权。另外，默认情况下，客户数据和服务器实例在逻辑上是与其他客户隔离的。在 AWS SOC、ISO 27001、PCI、ITAR 和 FedRAMP 审计期间，特权用户访问控制由独立审计师审查。
身份和权限管理 *策略和程序*	IAM-04.1	您是否管理和存储具有 IT 基础设施访问权限 (包括其访问级别) 的所有人员的身份？	

控制组	CID	一致性评估问题	AWS 的回答
	IAM-04.2	您是否管理和存储具有网络访问权限 (包括其访问级别) 的所有人员的用户身份？	
身份和权限管理 *职责划分*	IAM-05.1	您是否为租户提供描述如何在您提供的云服务中维持职责划分的相关文档？	客户保留管理其 AWS 资源职责划分的能力。 在内部，AWS 达到了管理职责划分相关的 ISO 27001 标准。请参阅 ISO 27001 标准、附录 A、域 6 了解更多详情。AWS 已通过独立审计师的验证和认证，确认符合 ISO 27001 认证标准。
身份和权限管理 *源代码访问限制*	IAM-06.1	现有控制体系是否能够防止对应用程序、程序或对象元源代码的未授权访问，并确保仅限授权人员访问？	为了达到 ISO 27001 标准，AWS 已制定正式的策略和程序，以描述对 AWS 资源进行逻辑访问的最低标准。AWS SOC 报告概述了管理 AWS 资源访问权限配置的现有控制体系。 请参阅《AWS 安全过程概述》白皮书以了解更多详情，网址为：http://aws.amazon.com/security。
	IAM-06.2	现有控制体系是否能够防止对租户应用程序、程序或对象源代码的未授权访问，并确保仅限授权人员访问？	
身份和权限管理 *第三方访问*	IAM-07.1	您是否提供多故障灾难恢复能力？	AWS 为客户提供在多个地理区域内以及在每个地理区域的多个可用区中放置实例和存储数据的灵活性。每个可用区域均设计为独立的故障区域。如果出现故障，自动化流程会将客户数据流量从受影响区域转移出去。AWS SOC 报告提供更多详情。ISO 27001 标准附录 A、域 15 提供更多详情。AWS 已通过独立审计师的验证和认证，确认符合 ISO 27001 认证标准。
	IAM-07.2	您是否监视上流提供商服务的连续性以避免出现供应商方面的故障？	
	IAM-07.3	您依赖的每个服务是否均有多个提供商？	
	IAM-07.4	您是否提供访问权限，以便访问包含您依赖的服务的操作冗余和连续性总结？	
	IAM-07.5	您是否允许租户宣布灾难的发生？	
	IAM-07.6	您是否提供可由租户触发的故障转移选项？	
	IAM-07.7	您是否与租户分享您的业务连续性和冗余计划？	

控制组	CID	一致性评估问题	AWS 的回答
身份和权限管理 *用户访问限制/授权*	IAM-08.1	是否记录了如何授予和批准对租户数据的访问权限？	AWS 客户保留控制和拥有其数据的权利。现有控制体系会限制对系统和数据的访问，并且约束和监视对系统和数据的访问权。另外，默认情况下，客户数据和服务器实例在逻辑上是与其他客户隔离的。在 AWS SOC、ISO 27001、PCI、ITAR 和 FedRAMP 审计期间，特权用户访问控制由独立审计师审查。
	IAM-08.2	您是否有办法匹配提供商和租户数据分类方法，以便进行访问控制？	
身份和权限管理 *用户访问授权*	IAM-09.1	在用户访问数据及任意所有的或托管的 (物理及虚拟) 应用程序、基础设施系统和网络组件之前，您的管理系统是否会为该用户访问 (如员工、合同工、客户 (租户)、业务合作伙伴和/或供应商) 预置授权和限制？	在 AWS 人力资源管理系统中创建唯一的用户标识符以作为入职工作流程的一部分。设备配置过程有助于确保设备具有唯一的标识符。两个过程均包含针对建立用户账户或设备的经理审批。作为配置过程的一部分，初始配置验证符将传递到用户手上和设备中。内部用户可将 SSH 公有密钥与其账户关联。在核实请求者的身份后，会向请求者提供系统账户验证符，以作为账户创建过程的一部分。
	IAM-09.2	您是否提供针对数据及任意所有的或托管的 (物理及虚拟) 应用程序、基础设施系统和网络组件的按需用户访问？	AWS 建立了控制体系以解决不当的内部访问的威胁。所有资质证书和第三方认证评估了逻辑访问预防和检测控制体系。此外，定期风险评估也主要针对如何控制和监视内部访问。
身份和权限管理 *用户访权限审查*	IAM-10.1	您是否要求针对所有系统用户和管理员 (租户维护的用户除外) 权限每年至少执行一次审查？	为了达到 ISO 27001 标准，所有访问授权均定期审查；需要重新进行授权，否则系统会自动取消对该资源的访问权限。SOC 报告中概述了针对用户访问权限审查的控制体系。SOC 报告中描述了用户权限控制体系的例外。 请参阅 ISO 27001 标准、附录 A、域 9 以了解更多详情。AWS 已通过独立审计师的验证和认证，确认符合 ISO 27001 认证标准。
	IAM-10.2	如果发现用户拥有不当的授权，是否记录所有补救和认证措施？	
	IAM-10.3	如果可能已经针对租户数据授予了不当访问权，您是否愿意与该租户共享用户权限补救和认证报告？	

控制组	CID	一致性评估问题	AWS 的回答
身份和权限管理 *用户访问权限的取消*	IAM-11.1	当员工、合同工、客户、业务合作伙伴或相关第三方的状态发生任何变化后，是否能及时实施取消配置、取消或修改该用户对组织系统、信息资产和数据的访问权限？	当 Amazon 人力资源系统终止员工的记录时，系统会自动取消访问权限。当员工的工作职能发生变化时，必须明确批准继续访问权限，否则将被自动取消。AWS SOC 报告提供了有关用户访问权限取消的详细信息。此外，AWS 安全白皮书的“员工生命周期”部分还提供了其他信息。 请参阅 ISO 27001 附录 A、域 9 了解更多详情。AWS 已通过独立审计师的验证和认证，确认符合 ISO 27001 认证标准。
	IAM-11.2	用户访问状态方面的任意变化是否包括雇佣、合同或协议的终止、雇佣变化或组织内职位变动？	
身份和权限管理 *用户 ID 凭证*	IAM-12.1	您的服务是否支持使用或与现有基于客户的单点登录 (SSO) 解决方案集成？	AWS Identity and Access Management (IAM) 服务提供至 AWS 管理控制台的身份联合功能。多重身份验证是一项客户可以选用的功能。请参阅 AWS 网站以了解更多详情，网址为：http://aws.amazon.com/mfa。 AWS Identity and Access Management (IAM) 支持联合身份，以对 AWS 管理控制台或 AWS API 进行委派访问。借助联合身份，外部身份 (联合身份用户) 可以安全访问 AWS 账户中的资源，而无需创建 IAM 用户。这些外部身份可来自公司身份提供程序 (如 Microsoft Active Directory 或 AWS Directory Service) 或来自 Web 身份提供程序，如 Amazon Cognito、Login with Amazon、Facebook、Google 或任意 OpenID Connect (OIDC) 兼容提供程序。
	IAM-12.2	您是否采用开放标准向租户委派身份验证功能？	
	IAM-12.3	您是否支持将身份联合标准 (SAML、SPML、WS 联合等) 用作一种用户身份验证/授权的方法？	
	IAM-12.4	您是否具备策略执行点功能 (如 XACML) 以对用户访问强制实施区域性法律和政策限制？	
	IAM-12.5	您是否已实施身份管理系统 (实现针对一个租户进行数据分类)，以支持基于角色和基于语境的数据访问授权？	
	IAM-12.6	您是否针对用户访问向租户提供了强大的 (多因素) 身份验证选项 (数字证书、令牌、生物识别信息等)？	
	IAM-12.7	您是否支持租户使用第三方身份保证服务？	

控制组	CID	一致性评估问题	AWS 的回答
	IAM-12.8	您是否支持密码 (最小长度、年龄、历史记录、复杂性) 和账户锁定 (锁定阈值、锁定时间) 策略的实施？	AWS Identity and Access Management (IAM) 使客户能够安全地控制用户对 AWS 服务和资源的访问。有关 IAM 的其他信息可以在网站 https://aws.amazon.com/iam/ 上找到。AWS SOC 报告提供了 AWS 执行的具体控制活动的进一步信息。
	IAM-12.9	您是否允许租户/客户为其账户制订密码和账户锁定策略？	
	IAM-12.10	您是否支持首次登录时强制更改密码的功能？	
	IAM-12.11	您是否设立了解锁已锁定账户的机制 (如通过电子邮件、定义的安全问题、手动解锁进行自助服务)？	
身份和权限管理 *实用程序计划* *访问权限*	IAM-13.1	是否已对显著管理虚拟分区 (如：关闭、克隆等) 的实用程序采取了适当的限制和监视措施？	为了达到 ISO 27001 标准，已对系统实用程序采取了适当的限制和监视措施。AWS SOC 报告提供了 AWS 执行的具体控制活动的进一步信息。 请参阅《AWS 安全过程概述》白皮书以了解更多详情，网址为：http://aws.amazon.com/security。
	IAM-13.2	您是否能够检测直接针对虚拟基础设施的攻击 (如：匀场、Blue Pill、网络劫持等)？	
	IAM-13.3	是否已利用技术控制体系阻止针对虚拟基础设施的攻击？	
基础设施和虚拟化安全 *审计记录/入侵检测*	IVS-01.1	是否已采用文件完整性 (主机) 和网络入侵检测 (IDS) 工具，及时检测并通过根本原因分析和事故响应进行调查？	AWS 事故响应计划 (事故检测、事故调查和事故响应) 的制定符合 ISO 27001 标准，已对系统实用程序采取了适当的限制和监视措施。AWS SOC 报告提供了有关限制系统访问的现有控制体系的更多详情。 请参阅《AWS 安全过程概述》白皮书以了解更多详情，网址为：http://aws.amazon.com/security。
	IVS-01.2	是否仅授权人员可对审计日志进行实际访问和逻辑用户访问？	
	IVS-01.3	您是否可以提供证据，能够反映您已针对规章和标准尽职地对您的控制体系/架构/流程进行了管理？	

控制组	CID	一致性评估问题	AWS 的回答
	IVS-01.4	审计日志是否集中存储和保留？	为了达到 ISO 27001 标准，AWS 信息系统采用的是通过 NTP (网络时间协议) 同步的内部系统时钟。AWS 已通过独立审计师的验证和认证，确认符合 ISO 27001 认证标准。 AWS 利用自动化监控系统提供高水平的服务性能和可用性。通过各种网上工具，主动式监控既可供内部使用，也可供外部使用。Systems within AWS 内的系统拥有齐全的检测功能，以监控关键的运行度量。配置了警报，在关键运行度量的早期报警阈值被超越的时候，警报会通知运行及管理人员。使用一个随时待命方案，因此始终有人对运行问题做出响应。此方案包括一个寻呼系统，因此警报能够迅速可靠地传递至运行人员。 有关更多信息，请参阅 AWS 云安全白皮书：http://aws.amazon.com/security。
	IVS-01.5	是否定期审查审计日志以防范安全事故 (如使用自动化工具)？	
基础设施和虚拟化安全 *变更检测*	IVS-02.1	您是否记录并提醒对虚拟机映像所做的任何更改而不管其运行状态 (如休眠、关闭或运行) 为何？	虚拟机是作为 EC2 服务的一部分配给客户的。客户保留对使用哪些资源以及在哪里驻存资源的控制权。请参阅 AWS 网站以了解更多详情，网址为：http://aws.amazon.com。
	IVS-02.2	在对虚拟机做出更改、移动映像及随后对映像的完整性进行验证时，是否通过电子方式 (如门户或提醒) 立即通知客户？	
基础设施和虚拟化安全 *时钟同步*	IVS-03.1	您是否使用同步的时间服务协议 (如 NTP) 确保所有系统保持一致的时间？	为了达到 ISO 27001 标准，AWS 信息系统采用的是通过 NTP (网络时间协议) 同步的内部系统时钟。 AWS 已通过独立审计师的验证和认证，确认符合 ISO 27001 认证标准。
基础设施和虚拟化安全 *容量/资源计划*	IVS-04.1	您是否提供相关文档，说明您维护什么级别和环境/方案下的系统超额订购 (网络、存储、内容、I/O 等)？	有关 AWS 服务限制及如何请求提高特定服务的限制的信息，请访问 AWS 网站：http://docs.aws.amazon.com/general/latest/gr/aws_service_limits.html。 AWS 根据 ISO 27001 标准来管理容量和数据使用。AWS 已通过独立审计师的验证和认证，确认符合 ISO 27001 认证标准。
	IVS-04.2	您是否在管理程序中限制使用内存超额订购功能？	

控制组	CID	一致性评估问题	AWS 的回答
	IVS-04.3	您的系统容量要求是否考虑到用于为租户提供服务的所有系统的当前、预计和预期的容量需求？	
	IVS-04.4	您是否监测和调整系统性能，以不断满足用于为租户提供服务的所有系统的法规、合约和业务要求？	
基础设施和虚拟化安全 *管理 — 漏洞管理*	IVS-05.1	您的安全漏洞评估工具或服务能够适应所使用的虚拟化技术 (如虚拟化感知)？	Amazon EC2 目前采用高度自定义版 Xen 管理程序。内部和外部防窃取团队会定期评估该管理程序的新旧漏洞和攻击载体，非常适合维护虚拟客户机间的强隔离状态。在评估和审计期间，AWS Xen 管理程序安全由独立审计师定期评估。 在使用各种工具的 AWS 环境中，定期对主机操作系统、Web 应用程序和数据库进行内部和外部漏洞扫描。作为 AWS 持续遵从 PCI DSS 和 FedRAMP 的一部分，定期审核漏洞扫描和补救实践。
基础设施和虚拟化安全 *网络安全*	IVS-06.1	对于您的 IaaS 产品，您是否向客户提供有关如何使用您的虚拟解决方案创建类似于分层安全架构的架构？	AWS 通过其公共网站发布了大量白皮书，其中提供了有关创建分层安全架构的指导，网址为：http://aws.amazon.com/documentation/。
	IVS-06.2	您是否定期更新网络架构图 (包括安全域/区域之间的数据流程)？	边界保护设备使用规则集合、访问控制列表 (ACL) 和配置来管控网络架构间的信息流。 Amazon 提供了多个网络结构，每个网络结构由控制结构间的信息流的设备分隔开。结构间的信息流由经过批准的授权建立，这些授权在设备上以访问控制列表 (ACL) 形式出现。这些设备按照 ACL 的要求控制结构间的信息流。ACL 由合适的人员定义和批准，并通过使用 AWS ACL 管理工具进行管理和部署。 Amazon 的信息安全团队将审批这些 ACL。网络结构间的已批准的防火墙规则集和访问控制列表将信息流限于特定的信息系统服务。定期 (至少每 24 小时) 对访问控制列表和规则集进行审核和审批，并将其自动推送到边界保护设备以确保规则集和访问控制列表最新。

控制组	CID	一致性评估问题	AWS 的回答
	IVS-06.3	您是否定期审查允许在网络中的安全域/区域之间进行的访问/连接 (如防火墙规则) 的适用性？	作为 AWS 对 SOC、PCI DSS、ISO 27001 和 FedRAMPsm 的持续合规性的一部分，独立的第三方审计师将定期审核 AWS 网络管理。 AWS 对其所有基础设施组件实施最小特权。AWS 禁止没有特定商业目的的所有端口和协议。AWS 遵循一种严格的方法，来最低程度地实施仅对设备的使用来说必不可少的特性和功能。执行网络扫描，并纠正使用中的任何不必要的端口和协议。 在使用各种工具的 AWS 环境中，定期对主机操作系统、Web 应用程序和数据库进行内部和外部漏洞扫描。作为 AWS 持续遵从 PCI DSS 和 FedRAMP 的一部分，定期审核漏洞扫描和补救实践。
	IVS-06.4	是否所有防火墙访问控制列表都标注了业务理由？	
基础设施和虚拟化安全 *操作系统强化和基本控制*	IVS-07.1	作为基准构建标准或模板的一部分，是否借助技术控制手段 (即防病毒、文件完整性监控和日志记录) 对操作系统进行了强化，从而只提供满足业务需求所需的必要端口、协议和服务？	
基础设施和虚拟化安全 *生产/非生产环境*	IVS-08.1	对于您的 SaaS 或 PaaS 产品，您是否为租户提供独立的生产和测试环境？	AWS 客户保留了创建并维护生产和测试环境的能力和责任。AWS 网站提供了关于使用 AWS 服务创建环境的指导，网址为：http://aws.amazon.com/documentation/。
	IVS-08.2	对于您的 IaaS 产品，您是否向租户提供有关如何创建合适的生产和测试环境的指导？	
	IVS-08.3	您是否对生产和非生产环境进行了逻辑及物理隔离？	AWS 客户有责任根据其定义的要求对其网络进行隔离。 在内部，AWS 网络隔离操作符合 ISO 27001 标准。请参阅 ISO 27001 标准、附录 A、域 13 以了解更多详情。AWS 已通过独立审计师的验证和认证，确认符合 ISO 27001 认证标准。
基础设施和虚拟化安全 *隔离*	IVS-09.1	系统和网络环境是否受到防火墙或虚拟防火墙的保护，以确保达到业务和客户安全要求？	
	IVS-09.2	系统和网络环境是否受到防火墙或虚拟防火墙的保护，以确保符合法律、监管和合同要求？	
	IVS-09.3	系统和网络环境是否受到防火墙或虚拟防火墙的保护，以确保隔离生产与非生产环境？	

控制组	CID	一致性评估问题	AWS 的回答
	IVS-09.4	系统和网络环境是否受到防火墙或虚拟防火墙的保护，以保护和隔离敏感数据？	
基础设施和虚拟化安全 *VM 安全 — vMotion 数据保护*	IVS-10.1	在将物理服务器、应用程序或数据迁移到虚拟服务器时，是否使用了安全、加密的通信信道？	AWS 支持客户对几乎所有服务 (包括 S3、EBS 和 EC2) 使用自己的加密机制。VPC 会话也是加密的。
	IVS-10.2	在将物理服务器、应用程序或数据迁移到虚拟服务器时，是否使用了与生产级网络隔离的网络？	AWS 客户保留对其数据的控制权和所有权。AWS 为客户提供维护和开发生产和非生产环境的能力。确保其生产数据不会被复制到非生产环境是客户的责任。
基础设施和虚拟化安全 *VMM 安全 — 管理程序强化*	IVS-11.1	对于托管虚拟系统的系统，您是否基于最小权限原则并辅以技术控制手段 (如：对管理控制台实施双因素身份验证、审计跟踪、IP 地址过滤、防火墙和 TLS 加密通信) 限制员工对其所有管理程序管理功能或管理控制台的访问？	AWS 采用了最小权限的概念，即仅允许用户为实现其工作职能而进行的必要访问。创建用户账户后，所创建的用户账户拥有最小访问权限。获得上述最小权限需要适当的授权。有关访问控制的更多信息，请参阅 AWS SOC 报告。
基础设施和虚拟化安全 *无线网络安全*	IVS-12.1	是否已制定相关策略和程序并配置和实施了相关机制，以保护无线网络周边环境和限制未授权的无线流量？	用于保护 AWS 网络环境的策略、程序和机制均已到位。 在审核我们的 SOC、PCI DSS、ISO 27001 和 FedRAMP 合规性期间，独立的外部审计师将审核 AWS 安全控制体系。
	IVS-12.2	是否已制定相关策略和程序并实施了相关机制，以确保针对身份验证和数据传输启用了无线强加密安全设置，以取代供应商默认设置？(例如，加密密钥、密码、SNMP 社区字符串等)	
	IVS-12.3	是否已制定相关策略和程序并实施了相关机制，以保护无线网络环境并检测是否存在未授权 (流氓) 网络设备，以即时从网络断开连接？	

控制组	CID	一致性评估问题	AWS 的回答
基础设施和虚拟化安全 *网络架构*	IVS-13.1	您的网络架构图是否清楚地规定了高风险环境和具有合法合规影响的数据流程？	AWS 客户有责任根据其定义的要求对其网络进行隔离。 在内部，AWS 网络隔离操作符合 ISO 27001 标准。AWS 已通过独立审计师的验证和认证，确认符合 ISO 27001 认证标准。
	IVS-13.2	您是否实施了技术措施并应用了纵深防御技术 (如数据包深度分析、流量限制和黑洞防御)，以检测并及时响应基于网络的异常入口/出口流量模式 (如 MAC 欺骗和 ARP 病毒攻击) 和/或分布式拒绝服务 (DDoS) 攻击？	AWS 安全会定期扫描所有面向 Internet 的服务终端节点 IP 地址，检查是否存在安全漏洞 (扫描范围不包括用户实例)。AWS 安全会通知相关方修复发现的任何安全漏洞。另外，独立的安全公司会定期执行外部漏洞威胁评估。然后，将从这些评估中发现的问题以及相关建议进行归类并提交给 AWS 领导层。 另外，AWS 控制环境还接受内外风险评估机构的定期评估。AWS 邀请外部认证机构和独立审计师审查并测试 AWS 的总体控制环境。 在审核我们的 SOC、PCI DSS、ISO 27001 和 FedRAMP 合规性期间，独立的外部审计师将审核 AWS 安全控制体系。
互操作性和可移植性 *API*	IPY-01	您是否发布服务中可用的所有 API 的列表并注明哪些是标准 API、哪些是自定义 API？	有关 AWS API 的详细信息，请访问 AWS 网站：https://aws.amazon.com/documentation/。 为了达到 ISO 27001 标准，AWS 已制定正式的策略和程序，以描述对 AWS 资源进行逻辑访问的最低标准。AWS SOC 报告概述了管理 AWS 资源访问权限配置的现有控制体系。 有关更多信息，请参阅 AWS 云安全白皮书：http://aws.amazon.com/security。
互操作性和可移植性 *数据请求*	IPY-02	对于非结构化的客户数据，能否根据要求提供行业标准格式 (如 .doc、.xls 或 .pdf)？	
互操作性和可移植性 *政策和法律*	IPY-03.1	是否提供管理 API 用法的策略和程序 (即服务等级协议)，以实现服务与第三方应用程序的互操作？	
	IPY-03.2	是否提供管理应用程序数据迁入/迁出服务的策略和程序 (即服务等级协议)？	客户保留控制和拥有其内容的权利。客户可以自行决定如何将其应用程序和内容迁入/迁出 AWS 平台。
互操作性和可移植性 *标准网络协议*	IPY-04.1	能否通过安全的 (如非明文和身份验证)、业界公认的标准网络协议进行数据导入、数据导出和服务管理操作？	AWS 支持客户按照需要移动 AWS 存储上的数据。有关存储选项的更多信息，请参阅 http://aws.amazon.com/choosing-a-cloud-platform。

控制组	CID	一致性评估问题	AWS 的回答
	IPY-04.2	您是否为消费者 (租户) 提供详细介绍所涉及的相关互操作性和可移植性网络协议标准的文档？	
互操作性和可移植性 *虚拟化*	IPY-05.1	您是否采用业界公认的虚拟化平台和标准虚拟化格式 (如 OVF) 来帮助确保实现互操作性？	Amazon EC2 目前采用高度自定义版 Xen 管理程序。内部和外部防窃取团队会定期评估该管理程序的新旧漏洞和攻击载体，非常适合维护虚拟客户机间的强隔离状态。在评估和审计期间，AWS Xen 管理程序安全由独立审计师定期评估。有关更多信息，请参阅 AWS 云安全白皮书：http://aws.amazon.com/security。
	IPY-05.2	您是否记录了对任意在用的管理程序所做的自定义更改以及可用的特定于解决方案的虚拟化绑定，以供客户审查？	
移动安全 *反恶意软件*	MOS-01	您是否在信息安全意识培训中提供针对特定移动设备的反恶意软件培训？	AWS 用于管理防病毒/恶意软件的程序、流程、过程均符合 ISO 27001 标准。请参阅 ISO 27001 标准、附录 A、域 12 了解更多信息。
移动安全 *应用程序商店*	MOS-02	您是否记录和公开供移动设备访问或存储公司数据和/或公司系统的已批准的应用程序存储的列表？	AWS 已建立了信息安全框架和策略，并根据 ISO 27002 控制体系、美国注册公开会计师协会 (AICPA) 信托服务原则、PCI DSS V3.1 和美国国家标准与技术研究院 (NIST) 刊物 800-53 (即：《联邦信息系统安全控制推荐》) 有效地集成了 ISO 27001 可认证框架。 客户保留对其数据和相关媒体资产的控制权和责任。管理移动安全设备和客户内容访问权限是客户的责任。
移动安全 *已批准的应用程序*	MOS-03	您是否具备策略执行功能 (如 XACML) 以确保只将已批准的应用程序和来自已批准应用程序存储的应用程序加载到移动设备上？	
移动安全 *已批准可用于 BYOD 的应用程序*	MOS-04	您的 BYOD 策略和培训是否明确声明哪些应用程序和应用程序存储已获批准可在 BYOD 设备上使用？	
移动安全 *认知和培训*	MOS-05	您的员工培训是否包含成文的移动设备策略，并明确规定移动设备和可接受的移动设备用法及要求？	

控制组	CID	一致性评估问题	AWS 的回答
移动安全 *基于云的服务*	MOS-06	您是否记录了经过预先批准、允许通过移动设备使用和存储公司业务数据的基于云的服务的列表？	
移动安全 *兼容性*	MOS-07	您是否有用于测试设备、操作系统和应用程序兼容性问题的成文应用程序验证流程？	
移动安全 *设备资格*	MOS-08	您是否有相关的 BYOD 策略对可用于 BYOD 目的的设备和资格要求进行规定？	
移动安全 *设备清单*	MOS-09	您是否维护有存储和访问公司数据 (包括设备状态，即操作系统和补丁级别、丢失或报废、设备受让人) 的所有移动设备的清单？	
移动安全 *设备管理*	MOS-10	您是否在允许存储、传输或处理公司数据的所有移动设备上部署了集中式移动设备管理解决方案？	
移动安全 *加密*	MOS-11	您的移动设备策略是否通过对所有移动设备进行技术控制来要求对整个设备或识别为具有敏感强制执行效力的数据使用加密？	
移动安全 *破解和攫权*	MOS-12.1	您的移动设备策略是否禁止规避移动设备上的内置安全控制体系 (如破解或攫权)？	
	MOS-12.2	您是否在设备上设有侦测和预防控制措施或通过集中式设备管理系统禁止规避内置安全控制体系的行为？	

控制组	CID	一致性评估问题	AWS 的回答
移动安全 *法律*	MOS-13.1	您的 BYOD 策略是否明确规定了对隐私权、诉讼要求、电子取证和法律保留的预期？	客户保留对其数据和相关媒体资产的控制权和责任。管理移动安全设备和客户内容访问权限是客户的责任。
	MOS-13.2	您是否在设备上设有侦测和预防控制措施或通过集中式设备管理系统禁止规避内置安全控制体系的行为？	
移动安全 *锁定屏幕*	MOS-14	您是否要求和强制通过技术措施使 BYOD 及公司所有设备进行自动锁屏？	
移动安全 *操作系统*	MOS-15	您是否通过公司的变更管理流程管理对移动设备操作系统、补丁级别和应用程序的所有更改？	
移动安全 *密码*	MOS-16.1	您是否设有面向企业发放的移动设备和/或 BYOD 移动设备的密码策略？	
	MOS-16.2	您是否通过技术控制手段 (即 MDM) 强制实施密码策略？	
	MOS-16.3	您的密码策略是否禁止通过移动设备变更身份验证要求 (即密码/PIN 长度)？	
移动安全 *策略*	MOS-17.1	您是否设有要求 BYOD 用户对特定公司数据执行备份的策略？	
	MOS-17.2	您是否设有要求 BYOD 用户禁止使用未批准应用程序存储的策略？	
	MOS-17.3	您是否设有要求 BYOD 用户使用反恶意软件 (如支持) 的策略？	

控制组	CID	一致性评估问题	AWS 的回答
移动安全 *远程擦除*	MOS-18.1	您的 IT 部门是否为所有公司接受的 BYOD 设备提供远程擦除或公司数据擦除服务？	
	MOS-18.2	您的 IT 部门是否为所有公司分配的移动设备提供远程擦除或公司数据擦除服务？	
移动安全 *安全补丁*	MOS-19.1	设备制造商或运营商一旦发布通用版本，您是否就会在公司的移动设备上安装最新的安全相关补丁？	
	MOS-19.2	您的移动设备是否允许公司 IT 人员进行远程验证以下载最新安全补丁？	
移动安全 *用户*	MOS-20.1	您的 BYOD 策略是否明确规定了允许在 BYOD 设备上使用或访问的系统和服务器？	
	MOS-20.2	您的 BYOD 策略是否明确规定了允许通过 BYOD 设备访问的用户角色？	
安全事故管理、电子取证和云取证 *联络/授权维护*	SEF-01.1	您是否按照合同和相关法规保持与地方当局的联络人和联络地点？	AWS 按照 ISO 27001 标准的要求，与行业机构、风险和合规性组织、当地政府、监管机构保持联系。 AWS 已通过独立审计师的验证和认证，确认符合 ISO 27001 认证标准。

控制组	CID	一致性评估问题	AWS 的回答
安全事故管理、电子取证和云取证 *事故管理*	SEF-02.1	您是否已制定安全事故响应计划	AWS 已根据 ISO 27001 标准制定了事故响应计划和程序。AWS 已通过独立审计师的验证和认证，确认符合 ISO 27001 认证标准。 AWS SOC 报告提供了 AWS 执行的具体控制活动的进一步信息。由 AWS 代表客户存储的所有数据均享有强大的租户隔离安全和控制保护。 有关更多信息，请参阅 AWS 云安全白皮书 (http://aws.amazon.com/security)。
	SEF-02.2	您是否将自定义租户要求集成到您的安全事故响应计划？	
	SEF-02.3	您是否已发布角色与责任相关文档，详细说明在安全事故期间您和您的租户各自担负的责任？	
	SEF-02.4	您去年是否测试了安全事故响应计划？	
安全事故管理、电子取证和云取证 *事故报告*	SEF-03.1	您的安全信息和事件管理 (SIEM) 系统是否会合并数据源 (应用日志、防火墙日志、IDS 日志、物理访问日志等)，以供粒度分析和报警使用？	
	SEF-03.2	您的记录和监视框架是否支持将事故隔离到特定租户？	
安全事故管理、电子取证和云取证 *事故响应法务准备*	SEF-04.1	您的事故响应计划是否符合监管链管理流程与控制体系方面的法定行业标准？	
	SEF-04.2	您的事故响应能力是否包括使用合法的电子取证数据收集和分析技术？	
	SEF-04.3	您是否有能力支持针对特定租户的诉讼保留 (即冻结从特定时间点开始的数据)，而无需冻结其他的租户数据？	
	SEF-04.4	因响应法律传票而产生数据时，您是否强制执行和验证租户数据隔离？	

控制组	CID	一致性评估问题	AWS 的回答
安全事故管理、电子取证和云取证 *事故响应指标*	SEF-05.1	您是否监视并量化所有信息安全事故的类型、数量和影响？	AWS 安全度量是根据 ISO 27001 标准进行监视和分析的。请参阅 ISO 27001 附录 A、域 16 了解进一步详情。AWS 已通过独立审计师的验证和认证，确认符合 ISO 27001 认证标准。
	SEF-05.2	您是否一经请求即与租户分享安全事故统计信息数据？	
供应链管理、透明度和问责制 *数据质量和完整性*	STA-01.1	您是否检查和负责数据质量错误及相关风险，并与云供应链合作伙伴联手纠正它们？	客户保留对其数据质量和通过使用 AWS 服务可能导致的任意质量错误的控制权和所有权。 有关数据完整性和访问管理 (包括最少访问权限) 的特定详情，请参阅 AWS SOC 报告
	STA-01.2	您是否设计和实施控制措施以通过适当的职责分离、基于角色的访问和为供应链中的所有人员分配最少的访问权限来降低和遏制数据安全风险？	
供应链管理、透明度和问责制 *事故报告*	STA-02.1	您是否通过电子方式 (如门户) 定期向所有受影响的客户和提供商传达安全事故信息？	AWS 已根据 ISO 27001 标准制定了事故响应计划和程序。AWS SOC 报告提供了 AWS 执行的具体控制活动的进一步信息。 有关更多信息，请参阅 AWS 云安全白皮书 (http://aws.amazon.com/security)。
供应链管理、透明度和问责制 *网络/基础设施服务*	STA-03.1	您是否为云服务产品的所有相关组件收集容量和数据使用方面的信息？	AWS 根据 ISO 27001 标准来管理容量和数据使用。AWS 已通过独立审计师的验证和认证，确认符合 ISO 27001 认证标准。
	STA-03.2	您是否会向租户提供容量计划和使用报告？	
供应链管理、透明度和问责制 *提供商内部评估*	STA-04.1	您是否每年对自己的政策、程序、配套措施及指标的合规性和有效性实施内部评估？	AWS 采购和供应团队会与所有 AWS 供应商保持联系。 请参阅 ISO 27001 标准；附录 A、域 15 以了解更多详情。AWS 已通过独立审计师的验证和认证，确认符合 ISO 27001 认证标准。

控制组	CID	一致性评估问题	AWS 的回答
供应链管理、透明度和问责制 *第三方协议*	STA-05.1	您是否根据处理、存储和传送数据的国家/地区的法律选择和监视外包服务提供商？	在 AWS 的父组织 (Amazon.com) 和相应第三方提供商之间的相互保密协议中确立支持 AWS 系统和设备的第三方提供商的人员安全要求。Amazon 法律顾问和 AWS 采购团队在与第三方提供商签订的合同协议中定义 AWS 第三方提供商人员安全要求。处理 AWS 信息的所有人员必须至少符合雇佣前背景调查的筛选流程，并在获得 AWS 信息访问权之前已签订保密协议 (NDA)。 AWS 一般不会将 AWS 服务的开发外包给分包商。
	STA-05.2	您是否根据数据起源地的国家/地区的法律选择并监视外包服务提供商？	
	STA-05.3	法律顾问是否会审查所有第三方协议？	
	STA-05.4	第三方协议是否包括为信息和资产提供安全和保护？	
	STA-05.5	您是否为客户提供所有子处理协议的列表和副本并不断更新？	
供应链管理、透明度和问责制 *供应链治理审查*	STA-06.1	您是否审查合作伙伴的风险管理和治理流程，以担负来自该合作伙伴供应链的其他成员的风险？	AWS 维护与关键的第三方供应商的正式协议，并依照其与该企业的关系实施适当的关系管理机制。作为 AWS 持续遵守 SOC 和 ISO 27001 工作的一部分，AWS 的第三方管理流程经过独立审计师的审查。
供应链管理、透明度和问责制 *供应链指标*	STA-07.1	是否制订了策略和程序并实施了支持业务流程和技术措施，以维护提供商与客户 (租户) 之间完整、准确和有针对性的协议 (如 SLA 等)？	
	STA-07.2	您能否衡量和解决整个供应链 (上游/下游) 的规定和/或条款的不合规之处？	
	STA-07.3	您能否管理不同的供应商关系导致的服务水平冲突或不一致之处？	
	STA-07.4	您是否至少每年审查全部协议、策略和流程一次？	

控制组	CID	一致性评估问题	AWS 的回答
供应链管理、透明度和问责制 *第三方评估*	STA-08.1	您能否通过执行每年审查来确保在整个信息供应链提供合理的信息安全？	
	STA-8.2	您的每年审查是否包括您的信息供应链依赖的所有合作伙伴/第三方提供商？	
供应链管理、透明度和问责制 *第三方审计*	STA-09.1	是否支持租户独立执行漏洞评估？	客户可以申请支持对其云基础架构执行扫描，前提是这些扫描只限于客户自己的实例，并且不违反 AWS 可接受的使用政策。通过提交 AWS 漏洞/渗透测试申请表可启动对这些类型扫描的预先核准。 AWS 安全定期邀请独立的安全公司参与执行外部漏洞威胁评估。AWS SOC 报告提供了与 AWS 执行的特定控制活动有关的更多详情。
	STA-09.2	您是否请第三方服务对您的应用程序和网络执行漏洞扫描和定期渗透测试？	
威胁和漏洞管理 *病毒/恶意软件*	TVM-01.1	您是否在所有系统上安装了支持或连接您的云服务产品的防恶意软件程序？	AWS 用于管理防病毒/恶意软件的程序、流程、过程均符合 ISO 27001 标准。请参阅 AWS SOC 报告，其中提供了进一步详情。 此外，可参阅 ISO 27001 标准、附录 A、域 12 以了解更多详情。AWS 已通过独立审计师的验证和认证，确认符合 ISO 27001 认证标准。
	TVM-01.2	您是否确定，已采用行业接受的时间表来更新所有基础设施组件上的使用签名、列表或行为模式的安全威胁检测系统？	
威胁和漏洞管理 *漏洞/补丁管理*	TVM-02.1	您是否按照行业最佳实践中的描述，定期执行网络层漏洞扫描？	客户保留对其客户操作系统、软件和应用程序的控制权，并负责执行其系统漏洞扫描和修补。客户可以申请支持对其云基础架构执行扫描，前提是这些扫描只限于客户自己的实例，并且不违反 AWS 可接受的使用政策。AWS 安全定期扫描所有面向网络的服务终端节点 IP 地址以查找漏洞。AWS 安全会通知相关方修复发现的任何安全漏洞。AWS 自身的维护和系统修补一般不会影响到客户。 有关更多信息，请参阅 AWS 云安全白皮书：http://aws.amazon.com/security。请参阅 ISO 27001 标准、附录 A、域 12 了解更多详情。AWS 已通过独立审计师的验证和认证，确认符合 ISO 27001 认证标准。
	TVM-02.2	您是否按照行业最佳实践中的描述，定期执行应用层漏洞扫描？	
	TVM-02.3	您是否根据行业最佳实践中的描述，定期执行本地操作系统层漏洞扫描？	
	TVM-02.4	如果租户要求，您是否会向其提供漏洞扫描的结果？	

控制组	CID	一致性评估问题	AWS 的回答
	TVM-02.5	您是否能够迅速修补所有计算设备、应用程序和系统上的漏洞？	
	TVM-02.6	您是否会一经要求即向租户提供根据风险制定的系统修补时间表？	
威胁和漏洞管理 *移动代码*	TVM-03.1	移动代码是否在安装和使用前获得授权？是否检查了移动代码的配置，确保根据清楚定义的安全策略运行该授权移动代码？	AWS 支持客户根据自身需要管理客户端和移动应用程序。
	TVM-03.2	是否阻止执行所有未授权的移动代码？	

延伸阅读

有关更多信息，请参阅以下资源：

- AWS 风险和合规性概述
- AWS 认证、计划、报告和第三方鉴证
- AWS Answers to Key Compliance Questions

文档修订

日期	描述
2017 年 1 月	迁移到了新模板。
2016 年 1 月	首次发布