AWS 风险和合规性概述

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

本文提供信息来帮助客户将 AWS 集成到其现有控制框架内，包括评估 AWS 控制机制的基本方法。

介绍

AWS 与客户共同控制 IT 环境。AWS 承担的分担责任部分包括在高度安全和受控制的平台上提供服务，并提供大量安全功能供客户使用。客户的责任包括以安全且受控制的方式配置 IT 环境，以满足自身需要。当客户不告知 AWS 其使用方式和配置细节时，AWS 会将与客户相关的安全与控制环境传达给客户。AWS 通过采取以下措施达到与客户交流传达的目的：

- 获取行业资质证书和本文档中描述的独立第三方的认证
- 在白皮书和网站内容中发布有关 AWS 安全与控制实践的信息
- 根据保密协议，直接向 AWS 客户提供证书、报告、和其他文档 (根据需要)

有关 AWS 安全性的详细描述，请参阅 AWS 安全中心。

有关 AWS 合规性的详细描述，请参阅 AWS 合规性页面。

此外，AWS 安全过程概述白皮书阐述了 AWS 的一般安全控制机制和专门针对服务的安全措施。

责任共担环境

将 IT 基础设施迁移到 AWS 服务的行为在客户与 AWS 之间建立了责任共享的模型。该共享模型可以帮助缓解客户操作负担，因为 AWS 会操作、管理并控制各个方面的组件，从主机操作系统和虚拟化层至运行服务的设施的物理安全，全权负责。客户负责管理来宾操作系统 (包括更新和安全补丁)、其他关联应用程序软件以及 AWS 提供的安全组防火墙的配置。客户应慎重选择服务，因为他们所承担的责任因他们使用的服务、服务与其 IT 环境的集成以及适用法律法规而各异。客户可以利用诸如基于主机的防火墙、基于主机的入侵检测/防护、加密和密钥管理之类的技术，来增强安全性能和/或满足更加严格的合规性要求。这种共同责任的本质还赋予了客户足够的灵活性和控制能力，使部署的解决方案能够达到行业特定的认证要求。

客户/AWS 分担责任模型还扩展到 IT 控制体系方面。正如 AWS 与客户共同行使控制 IT 环境的责任一样，管理、运营和验证 IT 控制体系的责任也是由双方共同承担。AWS 可帮助客户缓解管理控制体系的负担，方式是接手管理之前可能由客户管理、部署在 AWS 环境中的物理基础设施相关的控制体系。因为每个客户在 AWS 中的部署均不相同，所以客户可以藉此将管理特定 IT 控制体系的责任移交到 AWS，从而形成一个新型分布式控制环境。然后客户可以使用 AWS 控制和合规性文档 (如 AWS 认证和第三方鉴证中所述) 来根据需要执行控制评估与验证程序。

强合规性管理

AWS 始终要求客户不断维持对整个 IT 控制环境的足够管控能力，无论其 IT 部署方式如何。主要实践包括：了解必要的合规性目标和要求 (从相关来源)、制定满足这些目标和要求的控制环境，理解基于组织的风险承受能力的验证需要，以及验证其控制环境的运行效率。在 AWS 云中部署，为企业应用各种类型的控制体系和验证方法，提供多种选择。

严格的客户合规性与管理可能包括以下基本方法：

1. 核查来自 AWS 和其他来源的信息，尽可能了解整个 IT 环境，然后记录其全部合规性要求。
2. 设计并实施控制目标，以满足企业的合规性要求。
3. 识别并记录外部各方拥有的控制体系。
4. 验证所有控制目标是否均已达到，以及全部密钥控制体系是否已设计并行之有效。

以这种方式进行合规性管理，将帮助企业更好地了解其控制环境，有助于清晰说明要执行的验证活动。

评估并集成 AWS 控制体系

AWS 通过白皮书、报告、认证和其他第三方鉴证向客户提供了各种有关其 IT 控制环境的信息。本文档帮助客户理解与其所用 AWS 服务相关的现有控制体系，以及这些控制体系已经历的验证方式。客户还能借助这些信息得以阐释和验证，证明控制目前正在其扩展 IT 环境中有效工作。

按照传统做法，控制目标和控制体系的设计与运行效率由内部和/或外部审计师通过流程预排和证据评估进行验证。直接观察/验证 (由客户或客户的外部审计师执行) 一般用于验证控制体系。在企业使用服务提供商的情况下，如 AWS，就需要第三方认证并评估资质证书，以便就控制目标和控制体系的设计与运行效率获得合理的保证。因此，尽管客户的关键控制体系可能由 AWS 管理，但是控制环境可能仍然是统一的框架，所有控制体系在这种框架中均有记述，且验证为行之有效。第三方认证和 AWS 资质证书不仅提供更高级别的控制环境认证，还可以让客户免于在 AWS 云中为其 IT 环境执行特定的验证。

AWS IT 控制信息

AWS 通过以下方式向客户提供 IT 控制信息：

特定的控制定义。AWS 客户能够识别由 AWS 管理的关键控制体系。关键控制体系对客户的控制环境至关重要，需要对它们的运行效率执行外部认证，以便符合各种合规性要求，例如年度财务审计。为此，AWS 在其 Service Organization Controls 1 (服务性机构控制体系鉴证 1，SOC 1) II 类报告中公布了各种具体的 IT 控制体系。SOC 1 报告的前称是 Statement on Auditing Standards (SAS) No. 70 Service Organizations 报告，是广泛认可的审计标准，由美国会计师协会 (AICPA) 制定。SOC 1 审计是对 AWS 定义的控制目标和控制活动的设计与运营效率的彻底深度的设计，其中包括对 AWS 管理部分的控制目标和控制或的审计。“II 类”代表该报告中描述的每个控制体系不仅经历了设计充裕度评估，还由外部审计师测试了运行效率。鉴于 AWS 外部审计师的独立性和胜任能力，该报告中经过鉴定的控制体系可提供客户对 AWS 控制环境的高度信任。AWS 控制体系可以说是专为应对许多合规性目的和确保运行效率而设计，包括 Sarbanes-Oxley (SOX) Section 404 财务报表审计。一般而言，可以支持其他外部认证机构使用 SOC 1 II 类报告 (例如，ISO 27001 审计师可能需要 SOC 1 II 类报告来完成对客户的评估)。

其他特定控制活动涉及到 AWS 支付卡行业 (PCI) 和 Federal Information Security Management Act (联邦信息安全管理法案，FISMA) 合规性要求。AWS 遵从 FISMA Moderate 标准和 PCI 数据安全标准。这些 PCI 和 FISMA 标准非常规范，要求独立验证 AWS 是否遵守已发布的标准。

一般控制标准合规性。如果 AWS 客户要求达到广泛的控制目标，可能需要对 AWS 行业资质证书执行评估。为了达到 AWS ISO 27001 认证标准，AWS 遵守广泛、全面的安全标准，并遵从维护安全环境方面的最佳实践。而通过 PCI 数据安全标准 (PCI DSS)，AWS 遵守了一组对处理信用信息的公司非常重要的控制体系。通过遵从 FISMA 标准的 AWS，AWS 遵守了美国政府部门要求的各种控制体系。遵从这些一般标准可为客户提供有关现有控制体系和安全流程的全面信息，以便在管理合规性问题时加以考虑。

AWS 全球区域

数据中心在全球多个地区组成集群，其中包括：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 (法兰克福)、欧洲 (爱尔兰)、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) 和南美洲 (圣保罗)。

有关区域的完整列表，请访问 AWS 全球基础设施页面。

AWS 风险和合规性计划

AWS 提供有关风险和合规性计划的信息，以便客户能够将 AWS 控制体系融入其管理框架中。该信息可帮助客户将完整的控制和管理框架 (包括 AWS) 当作该框架的重要组成部分。

风险管理

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。

另外，AWS 控制环境还接受各种内外风险评估机构的评估。AWS 合规性和安全团队已基于 Control Objectives for Information and related Technology (信息系统和技术控制目标，COBIT) 框架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 Rev 3 (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。AWS 坚持该安全策略、为员工提供安全培训和执行应用程序安全审查。这些审查会评估数据的保密性、完整性、可用性以及与信息安全策略的一致性。

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。这些扫描是针对底层 AWS 基础设施的运作状况和可行性执行的，不能用以取代客户满足自身特定合规性要求所需的漏洞扫描。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。

控制环境

AWS 全面管理控制环境，其中包括策略、流程和利用 Amazon 的总体控制环境各个方面的控制活动。该控制环境已针对 AWS 服务产品的安全交付布置到位。建立和维护一个可支持 AWS 控制框架的运行效率的环境所需的人力、过程和技术包含在这种集合型控制环境中。AWS 已将经过主要的云计算行业实体验证的适用云控制体系集成到 AWS 控制框架。AWS 持续跟踪这些行业集团的动态，以便获得可借以实施先进方法的创意，从而更好地帮助客户管理其控制环境。

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。为每名员工提供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。

AWS 的组织结构提供了可用于计划、执行和控制商业运营的架构。组织结构分配了角色和责任，以提供足够的人力、运营效率和明确责任分工。管理还为关键员工建立了授权和相应的报告制度。公司招聘验证流程部分包括：教育、工作经验，在某些情况下，在法律法规允许的范围内根据员工的职位以及该职位可访问 AWS 设施的级别对员工进行的背景调查。公司还按照既定的入职流程，帮助新员工熟悉 Amazon 工具、流程、系统、策略和程序。

信息安全

AWS 已实施正式信息安全计划，旨在保护客户系统和数据的机密性、完整性和可用性。AWS 在公共网站上发布安全白皮书，说明 AWS 如何帮助客户保护数据安全。

AWS 联系信息

客户可以申请获取由第三方审计师发布的报告和认证，也可以申请查阅有关 AWS 合规性的更多信息，方法是联系 AWS 销售和业务开发部。该代表会根据客户问题的性质将客户引荐交给合适的团队。有关 AWS 合规性的其他信息，请参阅 AWS 合规性网站或将问题直接发送到 awscompliance@amazon.com。

延伸阅读

有关更多信息，请参阅以下资源：

- CSA 一致性评估倡议问卷
- AWS 认证、计划、报告和第三方鉴证
- AWS 对重要合规性问题的回答

文档修订

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