aws

Unable to locate subtitle

Amazon Web Services：风险与合规性

Amazon Web Services：风险与合规性: ***Unable to locate subtitle***

Table of Contents

Amazon Web Services：风险与合规性

发布日期：2021 年 3 月 11 日 (文档修订)

摘要

AWS 为各种客户（包括受监管行业的客户）提供服务。通过我们的责任共担模式，我们让客户能够在 IT 环境中有效且高效地管理风险，并通过按照广为认可的既定框架和计划来保证有效的风险管理。本白皮书概括介绍了 AWS 实施的在责任共担的 AWS 一方管理风险的机制，以及客户可用于确保这些机制得到有效实施的工具。

引言

AWS 与客户共同控制 IT 环境。因此，安全性是一项共同承担的责任。在管理 AWS 云中的安全性与合规性方面，各方都有各自的责任。客户的责任取决于他们使用的服务。但是，一般来说，客户有责任以符合其特定安全性与合规性要求的方式构建其 IT 环境。

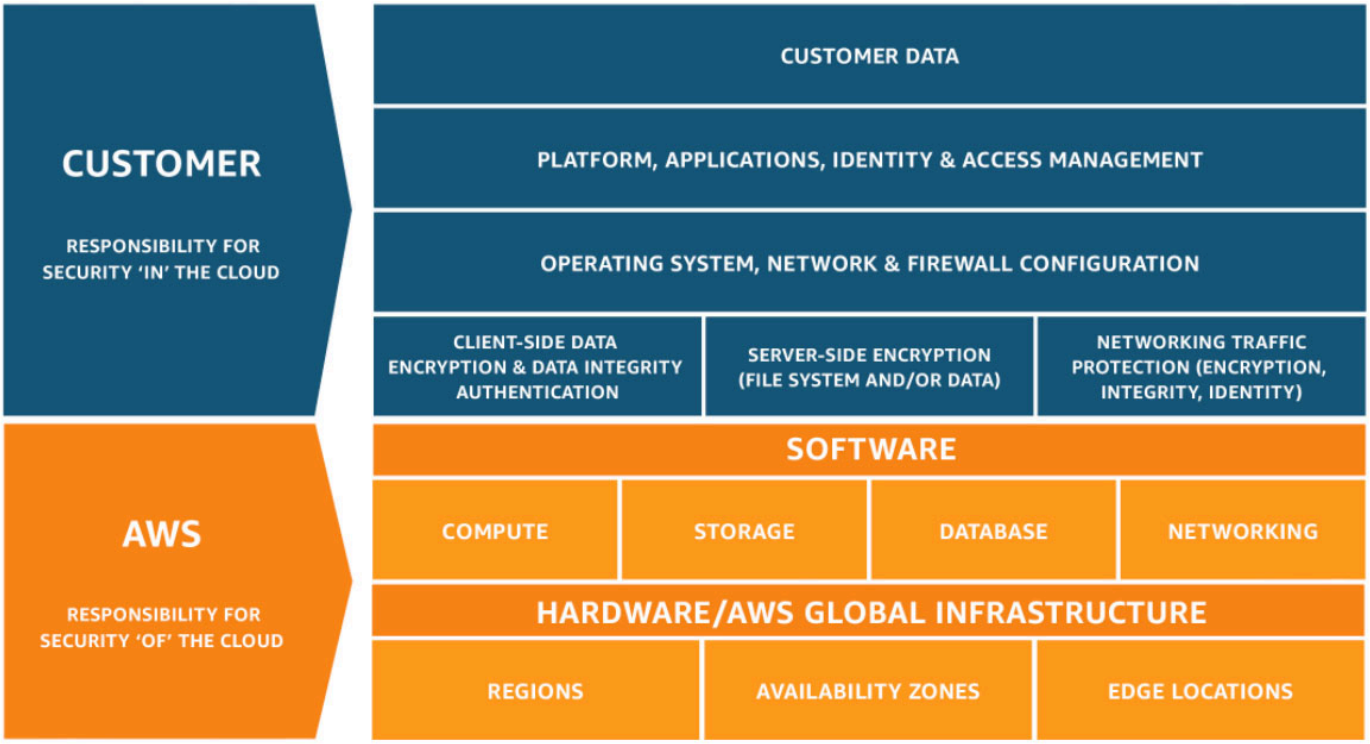
本白皮书详细介绍了各方的安全责任以及客户可通过哪些方式从 AWS 风险与合规性计划中受益。

责任共担模式

安全性与合规性是 AWS 和客户的共同责任。这种共担模式有助于减轻客户的运营负担，具体取决于部署的服务。这是因为，AWS 运营、管理和控制各种组件，从主机操作系统和虚拟化层，一直到运营各种服务的设施的物理安全性，面面俱到。除了 AWS 提供的安全组防火墙的配置外，客户还承担来宾操作系统（包括更新和安全补丁）和其他相关应用程序软件的责任和管理工作。

我们建议客户慎重考虑他们选择的服务，因为他们所承担的责任因他们使用的服务、这些服务与其 IT 环境的集成以及适用的法律法规而各不相同。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和防护、加密和密钥管理之类的技术，来增强其安全性能和/或满足其更加严格的合规性要求。

这种责任共担的性质也提供了灵活性和客户控制，让客户能够部署满足行业特定认证要求的解决方案。



这种责任分担模式还扩展到了 IT 控制体系方面。正如 AWS 与客户共同承担运营 IT 环境的责任一样，管理、运营和验证 IT 控制体系的责任也由双方共同承担。AWS 可通过管理与 AWS 环境中部署的物理基础设施相关的控制体系来帮助客户。然后，客户可以使用提供给他们的 AWS 控制和合规性文档，根据需要执行控制体系评估和验证流程。如需如何在 AWS 与其客户之间分担某些控制责任的示例，请参阅 AWS 责任共担模式。

评估并集成 AWS 控制体系

AWS 通过技术文献、报告、认证和其他第三方鉴证向客户提供有关其 IT 控制环境的各种信息。本文档帮助客户了解与其所用 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。这些信息还有助于客户说明和验证其扩展 IT 环境中的控制体系是否有效运行。

按照传统做法，内部和/或外部审计人员通过流程预排和证据评估来验证控制体系的设计与运行有效性。这种类型的直接观察和验证通常由客户或客户的外部审计人员执行，为的是验证传统内部部署中的控制体系。

在使用服务提供商（例如 AWS）的情况下，客户可以请求和评估第三方鉴证和认证。这些鉴证和认证可以帮助客户确保由合格的独立第三方验证的控制目标和控制体系的设计和运行有效性。因此，尽管某些控制体系可能由 AWS 管理，但控制环境仍然可以是一个统一的框架，客户可以在其中说明并验证控制体系是否正在有效运行，并加快合规性审核流程。

AWS 的第三方鉴证和认证为客户提供了控制环境的可见性和独立验证。借助此类鉴证和认证，客户无需自己在 AWS 云中为其 IT 环境执行某些验证工作。

AWS 风险和合规性计划

AWS 已在整个组织中集成风险和合规性计划。该计划旨在管理所有服务设计和部署阶段的风险，并不断改进和重新评估组织中的风险相关活动。以下各节将更详细地讨论 AWS 集成风险与合规性计划的组成部分。

AWS 业务风险管理

AWS 制定了业务风险管理 (BRM) 计划，AWS 业务部门可借助该计划向 AWS 董事会和 AWS 高层领导提供 AWS 面临的主要风险的整体情况。BRM 计划表明我们能够对 AWS 功能进行独立风险监督。具体来说，BRM 计划执行以下操作：

- 对关键 AWS 功能领域执行风险评估和风险监控
- 识别并推动风险补救
- 维护已知风险登记

为了推动风险补救，BRM 计划会报告其工作结果，并在必要时向整个企业的董事和副总裁上报问题，以便为业务决策提供信息。

运营和业务管理

AWS 组合使用每周、每月和每季度会议及报告，以确保风险管理流程所有组成部分之间的风险沟通。此外，AWS 还实施了上报流程，从而让管理层能够了解整个组织的高优先级风险。这些工作结合起来，有助于确保风险管理与 AWS 业务模式的复杂性保持一致。

此外，通过 Cascading 责任结构，副总裁（业务所有者）负责监督其业务。为此，AWS 每周都会召开会议，以审核运营指标，并在影响业务之前确定关键趋势和风险。

公司的管理层和高级领导层在建立 AWS 的基调和核心价值观方面起着重要作用。每名员工都会收到公司发放的《商业行为和道德准则》，并且需要定期接受培训。执行合规性审计，使员工了解并遵从既定政策。

AWS 的组织结构提供了可用于计划、执行和控制商业运营的框架。组织结构包括角色和责任，以提供足够的人力、运营效率并明确责任分工。管理层还为关键员工建立了相应的报告制度。公司的招聘调查过程包括调查教育背景、先前的工作经历，以及在某些情况下根据招聘职位以及该职位可访问 AWS

设施的级别进行法律法规允许的员工背景调查。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。

控制环境和自动化

AWS 将安全控制措施作为管理整个组织风险的基本要素予以实施。AWS 控制环境由标准、流程和结构组成，它们为在整个 AWS 中实施一套最低安全要求奠定了基础。

虽然 AWS 控制环境中包含的流程和标准是独立的，但是 AWS 还利用了 Amazon 整体控制环境的各个方面。利用的工具包括：

- 适用于所有 Amazon 业务的工具，例如用于管理职责分离的工具
- 整个 Amazon 范围内的某些企业职能，如法律、人力资源和财务

在 AWS 利用 Amazon 整体控制环境的情况下，管理这些机制的标准和流程专为 AWS 业务量身定制。这意味着，在 AWS 控制环境中使用和应用它们的期望可能不同于在整个 Amazon 环境中使用和应用它们的期望。AWS 控制环境最终充当安全交付 AWS 服务产品的基础。

在构成 AWS 控制环境的某些重复性流程中，控制自动化是 AWS 减少人为干预的一种方式。它是有效实施信息安全控制以及进行相关风险管理的关键。控制自动化旨在主动地最大限度减少流程执行中的潜在不一致问题，执行重复过程的人员本质上的缺陷便可能引起这样的不一致。通过控制自动化，潜在的过程偏差得以消除。这为按设计实施控制提供了更高保证。

AWS 跨安全职能的工程团队负责设计 AWS 控制环境，以尽可能支持更高级别的控制自动化。AWS 的自动化控制措施包括如下示例：

- 治理和监督：政策版本控制和批准
- 人员管理：自动提供培训、快速解雇员工
- 开发和配置管理：代码部署管道、代码扫描、代码备份、集成部署测试
- 身份和访问管理：自动分离职责、访问审核、权限管理
- 监控和日志记录：自动收集和关联日志、报警
- 物理安全：与 AWS 数据中心相关的自动化流程，包括硬件管理、数据中心安全培训、访问报警和物理访问管理
- 扫描和补丁管理：自动扫描漏洞、补丁管理和部署

控制评估和持续监控

AWS 会在服务部署前后开展各种活动，以进一步降低 AWS 环境中的风险。这些活动在每项 AWS 服务的设计和开发过程中都集成了安全性和合规性要求，然后验证服务在投入生产（启动）后能否安全运行。

风险管理和合规性活动包括两项启动前活动和两项启动后活动。启动前活动包括：

- AWS 应用程序安全性风险管理审核，以验证是否已识别并缓解安全风险
- 架构就绪性审核，以帮助客户确保符合各项法规要求

在部署时，我们将根据详细的安全要求对服务进行严格评估，以满足 AWS 的高安全性标准。启动后活动包括：

- AWS 应用程序安全性持续审核，以帮助确保服务安全态势得以维持
- 持续漏洞管理扫描

通过这些控制评估和持续监控，受到监管的客户便能够放心地在 AWS 服务上构建合规的解决方案。有关各种合规性计划范围内的服务列表，请参阅 AWS 范围内服务网页。

AWS 认证、计划、报告和第三方鉴证

AWS 定期接受独立的第三方鉴证审计，以确保控制活动按预期运行。更具体地说，需要根据各地区和行业的各种全球和区域安全框架对 AWS 进行审计。AWS 参与了 50 多项不同的审计计划。

这些审计的结果由评估机构记录，并通过 AWS Artifact 提供给所有 AWS 客户。AWS Artifact 是一个免费的自助服务门户，用于按需访问 AWS 合规性报告。当新报告发布时，它们会在 AWS Artifact 中提供，让客户能够立即访问新报告，根据报告结果持续监控 AWS 的安全性与合规性。

根据国家/地区或行业的本地法规或合同要求，AWS 可能还需直接接受客户或政府审计人员的审计。这些审计提供对 AWS 控制环境的额外监督，以确保客户有工具帮助他们放心、合规且以基于风险的方式使用 AWS 服务开展运营。

有关 AWS 认证计划、报告和第三方鉴证计划的更多详细信息，请访问 AWS 合规性计划网页。还可以访问AWS 范围内服务网页，了解服务特定信息。

云安全联盟

AWS 参与了自发性云安全联盟 (CSA) 安全、信任和保证注册表 (STAR) 自我评估，以记录我们对 CSA 发布的最佳实践的遵守情况。CSA 是“一个全球领先组织，致力于定义和提高大家对最佳实践的认识，从而帮助确保云计算环境安全”。CSA 一致性评估倡议问卷 (CAIQ) 提供 CSA 预期云客户和/或云审计人员会向云提供商提出的一系列问题。它包含一系列安全、控制和流程问题，用途广泛，包括云提供商选择和安全评估。

有两个资源可供客户使用，它们记录了 AWS 与 CSA CAIQ 的一致性。第一个是 CSA CAIQ 白皮书，第二个是与我们的 SOC-2 控制体系的更详细的控制映射，可通过 AWS Artifact 获得。有关 AWS 参与 CSA CAIQ 的更多信息，请参阅 AWS CSA 网站。

客户云合规性治理

无论 IT 部署方式或位置如何，AWS 客户都有责任对其整个 IT 控制环境保持充分的治理。主要实践包括：

- 了解所需的合规性目标和要求（从相关来源）
- 建立满足这些目标和要求的控制环境
- 了解基于组织的风险承受能力所需的验证
- 验证其控制环境的运行有效性

在 AWS 云中部署，为企业应用各种类型的控制措施和验证方法提供了多种选择。

强客户合规性与治理可能包括以下基本方法：

1. 检查 AWS 责任共担模式、AWS 安全性文档、AWS 合规性报告和 AWS 提供的其他信息，以及其他客户特定文档。尝试尽可能多地了解整个 IT 环境，然后将所有合规性要求记录到一个全面的云控制框架中。
2. 设计并实施控制目标，以满足 AWS 责任共担模式中规定的企业合规性要求。
3. 识别并记录外部各方拥有的控制体系。
4. 验证是否所有控制目标均已达到，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治理将帮助客户更好地了解其控制环境，并且有助于清晰说明要执行的验证活动。

总结

为我们的客户提供高度安全和弹性的基础设施和服务是 AWS 的首要任务。我们对客户的承诺是重点关注不断赢得客户的信任，并确保客户对在 AWS 上安全运行其工作负载一直保持信心。为实现这一目标，AWS 集成了风险和合规性机制，其中包括：

- 实施范围广泛的各种安全控制措施和自动化工具
- 持续监控和评估安全控制措施，以帮助确保 AWS 的运营有效性及严格遵守合规性制度
- 按 AWS 业务风险管理计划进行的独立风险评估
- 运营和业务管理机制

此外，AWS 还会定期接受独立的第三方审计，以确保控制活动按预期运行。这些审计以及 AWS 获得的许多认证为使客户受益的 AWS 控制环境提供了更高级别的验证。

结合客户管理的安全控制措施，这些工作让 AWS 能够代表客户进行安全创新，并帮助客户在 AWS 上进行构建时改善其安全状况。

贡献者

本文档的贡献者包括：

- Marta Taggart，AWS 安全部门高级项目经理
- Bradley Roach，AWS 业务风险管理部门风险经理
- Patrick Woods，AWS 安全高级部门安全专家

延伸阅读

AWS 通过以下方式向客户提供有关其安全和控制环境的信息：

- 获取和维护 AWS 合规性计划页面上列出的行业认证和独立第三方鉴证。
- 不断在白皮书和 Web 内容（如 AWS 安全博客）中发布有关 AWS 安全和控制实践的信息。
- AWS Builders Library 中深入介绍了 AWS 如何大规模利用自动化技术管理我们的服务基础设施。
- 通过名为 AWS Artifact 的自助服务门户直接向 AWS 客户提供合规性证书、报告和其他文档，从而提高透明度。
- 提供 AWS 合规性资源，并在 AWS 合规性常见问题解答网页上持续记录和发布问询的答案。
- 客户可以关注 AWS Well-Architected Framework 中的设计原则，获取有关如何对基于 AWS 构建的工作负载进行高于一般标准配置的指导。

文档修订

要获得有关此白皮书的更新通知，请订阅 RSS 源。

更新-历史记录-更改	更新-历史记录-描述	更新-历史记录-日期
次要更新	已审核技术准确性	2021 年 3 月 10 日
已更新白皮书	此版本包含重大更改，包括删除了有关合规性计划和方案的参考信息，因为这些信息可在 AWS 合规性计划和合规性计划范围内的 AWS 服务网页上找到。此外，我们还删除了涵盖常见合规性问题的部分，因为这些信息现已在 AWS 合规性常见问题解答网页上提供。	2020 年 11 月 1 日
初次发布	Amazon Web Services：风险与合规性白皮书已发布	2011 年 5 月 1 日

声明

客户有责任对本文档中的信息，进行独立评估。本文档：(a) 仅供参考；(b) 代表当前提供的 AWS 产品和实践，如有更改，恕不另行通知；并且 (c) AWS 及其附属机构、供应商或许可方不做任何承诺或保证。AWS 产品或服务“按原样”提供，不提供任何形式的保证、陈述或条件，无论是明示还是暗示。AWS 对其客户的责任和义务由 AWS 协议决定，本文档与 AWS 和客户之间签订的任何协议无关，亦不影响任何此类协议。