

# 在 GxP 系统中使用 AWS 产品的注意事项

**2016 年 1 月**



© 2016, Amazon Web Services, Inc. 或其附属公司。保留所有权利。

## 声明

本文档仅供参考之用。本文档代表截至其发行之日的 AWS 最新产品/服务和实践，如有变更，恕不另行通知。客户负责对本文档中的信息以及对 AWS 产品或服务的任何形式的使用进行独立评估，所有产品或服务均按“原样”提供，不含任何形式的明示或暗示的保证。本文档不形成 AWS 及其附属公司、供应商或许可方的任何保证、主张、合同承诺、条件或担保。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。

## 目录

1	摘要.....	4
2	引言.....	5
2.1.1	关于 AWS.....	5
2.1.2	AWS 客户.....	6
2.1.3	AWS 技术.....	7
2.1.4	AWS 产品.....	8
3	在 GxP 系统中使用 AWS 产品.....	10
3.1	质量体系.....	10
3.1.1	管理责任.....	10
3.1.2	人员.....	11
3.1.3	审计.....	12
3.1.4	采购控制机制.....	13
3.1.5	产品评估.....	14
3.1.6	供应商评估.....	16
3.1.7	供应商协议.....	17
3.1.8	记录和日志.....	19
3.2	系统开发生命周期.....	20
3.2.1	开发.....	21
3.2.2	验证.....	23
3.2.3	运营.....	25
3.3	法规事务.....	28
3.3.1	提交.....	28
3.3.2	检查.....	28
3.3.3	研究参与者的个人数据隐私控制.....	29
4	结论.....	30
5	文档修订.....	30
6	附录.....	31
6.1	数据隐私资源.....	31
6.2	附注的 21 CFR Part 11.....	32
6.3	AWS 协议中的共担责任.....	34

## 1 摘要

2006 年，Amazon Web Services (AWS) 开始以 Web 服务的形式向客户提供 IT 基础设施产品，现在通常称为云计算。如今，AWS 提供高度可靠、可扩展、低成本的基础设施平台，为全球 190 个国家/地区的数十万家企业提供支持。云计算的主要优势包括：让客户可以将前期基础设施资本支出替换为随使用情况增减的较低可变成本，并且可以将更多时间用在核心活动上，减少用于无差别 IT 任务的时间。

借助云，组织不再需要提前数周或数月计划和采购物理设备和 IT 基础设施。相反，他们可以使用自动部署工具和方法立即动用成百上千个虚拟机，这可以更快地交付结果，同时确保控制的一致性更高，人为错误更少。为了获得 AWS 产品带来的优势，具有良好实验室、临床或制造规范 (GxP) 合规性要求的组织及其审核人员需要掌握新技能，并考虑对 GxP 政策和流程进行更改，使 IT 合规性管理更敏捷、自动化程度更高且更关注安全性。

本白皮书提供了在 GxP 环境中使用 AWS 产品的指南，相关内容是与 AWS 药品及医疗设备客户以及当前在经验证的 GxP 系统中使用 AWS 产品的软件合作伙伴协作编写的。为了确保内容的适用性，AWS 还另外邀请了 Lachman Consultant Services Inc.（以下简称“Lachman Consultants”）参与进来，对此白皮书中介绍的方法进行审阅并提供意见。在解答目前影响医药及医疗设备行业的 FDA 和国际法规遵从性问题方面，Lachman Consultants 是最受推崇的咨询公司之一。Lachman Consultants 拥有与诸多公司合作的丰富经验，尤其是在与 GxP 系统的建立和开发有关的事务上，包括支持在云环境中维护受规管数据的 GxP 准则。有关 Lachman Consultants 的更多信息，请访问 [www.lachmanconsultants.com](http://www.lachmanconsultants.com)。

但是，AWS 客户有责任与自己的顾问协商，以确保其 GxP 政策和流程适用于使用 AWS 产品的当前 IT、软件 and 安全性实践。

## 2 引言

Amazon Web Services (AWS) 提供云基础设施软件产品，这些产品越来越多地用于存储和处理世界各地几乎所有行业中的敏感和受监管工作负载。医疗保健和生命科学组织正逐渐意识到 AWS 云的优势，并开始将 AWS 产品用作其受监管 IT 系统的组成部分，包括为适用于医疗器械、药品、生物制品以及其他食品和医疗产品行业的良好实验室规范、良好临床规范和良好生产规范（以下简称“GxP”）提供支持的计算机化系统。

本文档提供的信息旨在协助希望使用 AWS 产品来构建特定计算机化系统的客户，这些系统基于通用 GxP 合规性和数据完整性要求存储或处理电子记录。

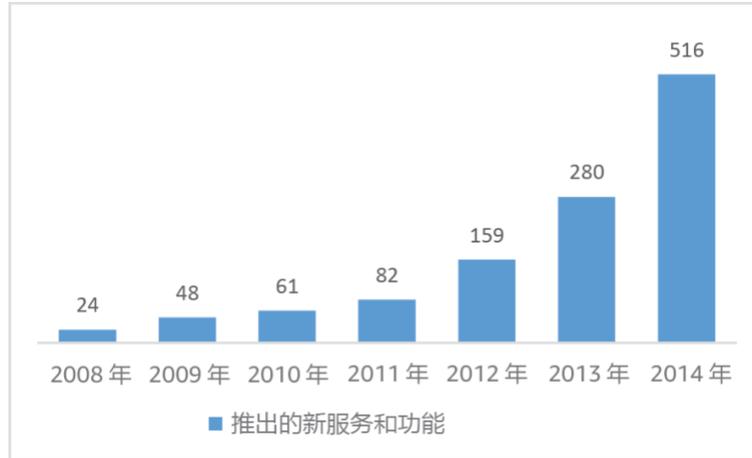
本文档将帮助客户了解：

- AWS 产品的范围和技术基础，
- 客户在使用 AWS 的商用云产品时可能会有的质量体系方面的注意事项，
- 针对纳入 AWS 产品作为组件，并开发、验证和操作 GxP 系统的客户的系统开发生命周期注意事项，以及
- 针对可能向监管机构提交或提供系统相关信息的客户的法规事务注意事项。

有关包含 AWS 产品、隐私和数据保护注意事项的更多具体信息的白皮书，请访问 <https://aws.amazon.com/compliance/>。

### 2.1.1 关于 AWS

Amazon Web Services 由 Amazon.com (NYSE: AMZN) 于 2006 年建立，是一家成熟的云服务提供商，提供诸多基于订阅的基础设施产品，这些产品从美国、澳大利亚、巴西、中国、德国、爱尔兰、日本、韩国和新加坡的数据中心通过互联网按需提供。自成立以来，AWS 致力于通过快速将新产品交付到客户手中，然后根据客户反馈快速迭代和改进这些产品，保持着定义云计算的创新者的身份。创新的节奏和持续的服务改进是越来越多的组织为其关键任务系统选择使用 AWS 产品的原因。



客户痴迷和客户信任是亚马逊团队文化的核心领导原则。客户在使用 AWS 产品时可保留对其数据和系统的所有权和控制权，而 AWS 会通过当前的隐私和数据保护框架保持一致，努力为客户提供信心和透明度。参阅数据隐私附录（第 31 页）了解更多。

- AMZN Corp. 信息：  
<http://phx.corporate-ir.net/phoenix.zhtml?c=97664&p=irhome>
- 领导力原则：  
<http://www.amazon.jobs/principles>
- 分析报告：  
<https://aws.amazon.com/resources/analyst-reports/>

### 2.1.2 AWS 客户

从所有者经营的初创企业和小型企业到全球性企业和政府机构，AWS 在 190 多个国家/地区拥有超过一百万的活跃客户，几乎涵盖了所有行业和组织类型。在我们客户的组织中，AWS 产品的主要用户是构建和维护组织的 IT 基础设施和应用程序的软件开发人员、网络工程师和系统管理员。AWS 在客户成功案例方面有长长的清单，这些案例突出了受益于我们的云产品的行业和市场的广阔范围：<https://aws.amazon.com/solutions/case-studies/all/>。

在自身计算机中使用 AWS 产品的客户中也有许多医疗保健和生命科学组织，AWS Health 网站重点叙述了一些他们的故事：<https://aws.amazon.com/health/>。

### 2.1.3 AWS 技术

Amazon Web Services (AWS) 以所有 AWS 产品、Web 服务中内置的一项核心技术命名。一个 Web 服务是一个自包含、可复用的软件模块，它通过使用标准化消息传递格式（例如 XML<sup>1</sup> 和 JSON<sup>2</sup>）的 Internet 协议使其功能可用于其他软件模块。所有 AWS 产品均可通过自助式管理控制台 <https://aws.amazon.com/account/> 在线获得，它们基于两种类型的 Web 服务，每种类型都有数种接口：

#### Web 服务类型：

- 简单对象访问协议 (SOAP)
- 表征状态转移 (REST)

#### AWS 产品接口：

- 应用程序编程接口 (API)
- 命令行界面 (CLI)
- 图形化用户界面 (GUI)

Web 服务不与任何一种操作系统或编程语言绑定，这意味着使用不同编程语言编写和运行在不同平台上的应用程序可以使用每个 Web 服务接口支持的预定义动作，通过 Internet（或 Intranet）无缝交换数据。Web 服务方法（有时称为面向 Web 的架构）的一个主要优点是，使用 Web 服务的软件应用程序不需要知道 Web 服务的构建方式或基础数据的存储方式，它们只需要知道 Web 服务接口将响应哪些操作即可。只要操作在接口中可用，更改 Web 服务的基础组件或者添加新操作都不会影响应用程序的行为或可靠性。AWS 产品支持的 Web 服务操作列表有完整记录并可以在线获取：<https://aws.amazon.com/documentation/>。

除 Web 服务技术外，软件定义的基础设施技术（例如虚拟化和软件定义的联网 (SDN)）是 AWS 产品的核心。以前只能以专用物理设备提供的基础设施组件，例如网络负载均衡器和防火墙，现在可以以按需软件定义的资源形式提供，这减少了系统开发的时间和成本，同时通过软件自动化实现了更高级别的基础设施标准化和控制。

软件扩展到将传统的物理基础设施组件纳入其中，再加上面向 Web 的架构和现代编程方法的优势，正在推动各行业在 IT SDLC<sup>3</sup>、员工技能和 IT 合规性方面的全球性转变。准备在其 GxP 系统中最大限度利用 AWS 产品的组织是那些认识到并适应这种转变的组织。

<sup>1</sup> 可扩展标记语言

<sup>2</sup> JavaScript 对象标记

<sup>3</sup> 系统开发生命周期

AWS 技术的优势：

- **平台独立和互操作性**：AWS 产品支持以多种编程语言编写的应用程序，并且不将应用程序限制到特定的操作系统或硬件组件。
- **可扩展性**：通过将软件定义的基础设施与使用现代编程方法的 AWS 产品相接合，AWS 客户可以设计其计算机化系统，以根据系统的实际需求快速上扩或收缩资源（及其成本）。
- **容错**：AWS 产品支持 AWS 产品与软件应用程序之间的松散耦合，从而确保即使系统组件或 AWS 产品暂时不可用，客户也可以设计其 GxP 系统以继续正常运行。
- **职责隔离**：将物理基础设施职责与客户虚拟基础设施和软件职责分开，可以确保对 GxP 数据的物理访问与逻辑访问完全隔离，从而提供了关键的数据完整性控制。
- **可审计性**：Web 服务基于消息的互操作性允许客户配置和使用 AWS 产品进行统一记录、监控和审计。
- **专注于核心能力**：AWS 产品的最终益处是我们的客户可以将更少的时间花费在无差别的任务上，而将更多的时间投入为组织增值的核心能力。

#### 2.1.4 AWS 产品

AWS 生产商用云基础设施软件产品和办公生产力应用程序，这些产品本质上是用户可配置且通用的，并依照 ISO、NIST、SOC 等商用 IT 标准交付。这类似于其他通用 IT 产品和服务，例如数据库引擎、操作系统、编程语言、Internet 服务提供商等。许多组织将 AWS 产品归类为商用现成 (COTS) 的基础设施软件产品，这与美国联邦政府通过名为 FedRAMP 的联邦采购计划将 AWS 产品用作 COTS 项相一致。在 FedRAMP（其继承了美国联邦采购法规 (FAR) 的定义）下，COTS 项 1) 基于既定目录在商业市场上以竞争性方式大量提供和销售的产品或服务，2) 提供时未经修改或定制，以及 3) 根据标准商业条款和条件提供。有 GxP 要求的 AWS 客户有责任使用其适用的行业名称对 AWS 产品进行分类，例如适用于受监管的 GxP 环境中计算机系统的“良好自动化生产规范 (GAMP) 类别 1”，或在医疗设备质量框架下的“药品检验合作计划 (PIC/S) 指南”，又或者未知来源软件 (SOUP)、“黑匣子”OTS 组件或通用计算资源。

AWS 提供超过 50 种产品，分为以下几类：

类别	AWS 产品
计算	Amazon EC2、Amazon EC2 Container Service、AWS Elastic Beanstalk、AWS Lambda、Auto Scaling
存储	Amazon S3、Amazon CloudFront、Amazon EBS、Amazon EFS、Amazon Glacier、AWS Storage Gateway、AWS Snowball
数据库	Amazon RDS、Amazon DynamoDB、Amazon ElastiCache、Amazon Redshift
联网	Amazon VPC、AWS Direct Connect、Elastic Load Balancing、Amazon Route 53
开发人员工具	AWS CodeCommit、AWS CodePipeline、AWS CodeDeploy、AWS 工具和软件开发工具包
管理工具	Amazon CloudWatch、AWS CloudFormation、AWS CloudTrail、AWS Config、AWS 管理控制台、AWS OpsWorks、AWS Service Catalog、Trusted Advisor、AWS Tools for Windows PowerShell
安全和身份	Identity & Access Management、AWS Directory Service、Amazon Inspector、AWS CloudHSM、AWS KMS、AWS WAF
分析	Amazon EMR、AWS Data Pipeline、Amazon Elasticsearch Service、Amazon Kinesis、Amazon Kinesis Firehose、Amazon Machine Learning、Amazon QuickSight
移动及物联网 (IOT)	AWS IoT、AWS Mobile Hub、Amazon API Gateway、Amazon Cognito、AWS Device Farm、Amazon Mobile Analytics、AWS Mobile SDK、Amazon SNS
应用程序服务	Amazon API Gateway、Amazon AppStream、Amazon CloudSearch、Amazon Elastic Transcoder、Amazon FPS、Amazon SES、Amazon SNS、Amazon SQS、Amazon SWF
企业生产力应用程序	Amazon WorkSpaces、Amazon WAM、Amazon WorkDocs、Amazon WorkMail

关于 AWS 产品、全球基础设施和客户注册的详细信息和规格可通过以下网址获得：

- <https://aws.amazon.com/account/>
- <https://aws.amazon.com/products/>
- <https://aws.amazon.com/documentation/>

- <https://aws.amazon.com/about-aws/global-infrastructure/>

## 3 在 GxP 系统中使用 AWS 产品

尽管 AWS 产品的交付模型是虚拟的在线产品，而不是实物的本地产品，但是将它们用作 GxP 系统中组件的职责是相似的。在这种成熟的模型下，将商用基础设施产品按 GxP 系统组件进行配置和使用的客户在以下几个关键领域负有责任：

- 质量体系，
- 系统开发生命周期，以及
- 法规事务。

### 3.1 质量体系

寻求在 GxP 系统中使用 AWS 产品的组织应审查并更新其质量系统文档，本节为要考虑的关键领域提供了一些指引。

#### 3.1.1 管理责任

在生产 GxP 系统中使用 AWS 产品之前，客户应考虑如何管理 AWS 账户的创建和维护。由于 AWS 账户创建是自助式的，并且向账户创建者授予了根账户凭据，使其具有对 AWS 产品配置和访问控制的完全控制权，因此在客户组织内具有执行职责的管理层应定义并传达 AWS 账户治理政策，以确保其 GxP 系统中使用的账户得以被跟踪，并且根账户凭据由组织授权的合格人员控制。此外，应将密码政策应用于 AWS 账户，以要求所有账户用户轮换其密码。

客户应考虑更新以下文档以支持其在 GxP 系统中使用 AWS 产品：

- AWS 账户监管政策
- 针对具有组织采购授权的所有员工的备忘录
- AWS 账户创建流程
- AWS 账户用户密码政策

### 3.1.2 人员

AWS 客户有责任确保其人员具有适当的教育水平、经验和接收过适当的培训以执行所分配的工作职能。如果工作职能包括在 GxP 系统中使用 AWS 产品，那么在雇用和/或培训人员时应考虑 AWS 产品的经验水平。系统访问级别和执行的工作职能与确定所需的经验水平相关，并且可能会影响许多工作职能：

- 软件工程师
- 软件测试人员
- 网络工程师
- 系统管理员
- 安全工程师
- 验证工程师
- 采购人员
- 质保人员
- 审计人员
- 注意：GxP 应用程序最终用户通常不直接与 AWS 产品交互，并且可能不需要 AWS 特定的培训

培训可以包括意识培训、培训本身或基于测试的员工资格认证。AWS 和亚马逊合作伙伴网络 (APN) 提供了关于 AWS 产品的一系列初始和进行中培训和认证，包括：

- 在线文档：<https://aws.amazon.com/documentation/>
- 教学视频：[https://aws.amazon.com/training/intro\\_series/](https://aws.amazon.com/training/intro_series/)
- 自主进度动手实验室：<https://aws.amazon.com/training/self-paced-labs/>
- 活动和网络研讨会：<https://aws.amazon.com/about-aws/events/>
- 课程和研讨会：<https://aws.amazon.com/training/course-descriptions/>
- 合作伙伴培训：<https://aws.amazon.com/partners/training/>
- 专业证书：<https://aws.amazon.com/certification/>

客户应考虑更新以下文档以支持其在 GxP 系统中使用 AWS 产品：

- 培训计划和流程
- 工作描述
- 工作申请、履历和简历
- 培训记录
- AWS 产品的证书

### 3.1.3 审计

对于审计在 GxP 系统中使用 AWS 产品的客户，评估系统安全性和数据完整性控制以及 SDLC 的持续有效性非常重要。为了对 AWS 产品的使用情况进行有效的审计，IT 审计人员应熟悉 Web 服务技术、AWS 产品并阅读 JSON 等基本脚本。理想情况下，审计人员可以通过“只读访问策略”直接访问相关的 AWS 账户资源。在 AWS 账户中，审计人员和评估人员应查看相关的产品功能配置和日志记录数据，例如：

- AWS 账户凭据
- 组织合同
- IAM 用户、组和角色
- SAML 和 OpenID Connect 的 IAM 提供商
- Amazon EC2 安全配置
- 其他服务（例如 S3）中的基于资源的政策
- AWS Config 规则
- CloudTrail 中的系统活动日志
- AWS Config 中的更改历史
- 系统支持案例历史

AWS 提供了一系列审计工具和教育资源，以帮助准备审计在 GxP 系统中使用 AWS 产品的审计人员：

- AWS 审计白皮书  
[https://d0.awsstatic.com/whitepapers/compliance/AWS\\_Auditing\\_Security\\_Checklist.pdf](https://d0.awsstatic.com/whitepapers/compliance/AWS_Auditing_Security_Checklist.pdf)
- AWS 运营检查清单白皮书  
[https://s3.amazonaws.com/awsmedia/AWS\\_Operational\\_Checklists.pdf](https://s3.amazonaws.com/awsmedia/AWS_Operational_Checklists.pdf)
- AWS 安全审计指导原则 <https://docs.aws.amazon.com/general/latest/gr/aws-security-audit-guide.html>
- AWS CloudTrail 产品页面 <https://aws.amazon.com/cloudtrail/>
- AWS Config 产品页面 <https://aws.amazon.com/config/>

- AWS Trusted Advisor 页面 <https://aws.amazon.com/premiumsupport/trustedadvisor/>
- 进度自主审计 qwikLAB: <https://www.qwiklab.com/focuses/preview/1250?locale=en>
- 亲身审计人员培训 [awsaudittraining@amazon.com](mailto:awsaudittraining@amazon.com)

客户应当考虑更新以下文档以支持其对 GxP 系统中 AWS 产品的使用：

- IT 设计时间表
- AWS 账户审计流程及检查清单
- AWS 账户审计报告
- IT 审计人员资格证明、简历、AWS 产品的培训记录

### 3.1.4 采购控制机制

传统的 IT 基础设施产品采购涉及实物商品的采购单 (PO) 流程，该流程记为资本支出。但是，对于 AWS 产品，采购涉及对订阅软件产品的进行类似于计量使用量的水电公用服务的计费过程，该过程被记为可变运营费用。许多生命科学组织针对 PO 流程都设定了书面的 GxP IT 产品采购流程，这些过程可能无法满足订购（即按使用量付费）产品定价模型（如 AWS）的购买要求。

使用传统 PO 执行基础设施采购	使用 AWS 的基础设施采购过程
<ol style="list-style-type: none"> <li>1. IT 部给出服务器需求</li> <li>2. IT 部确定匹配服务和 OS 来源</li> <li>3. IT 部提交采购请求</li> <li>4. 采购部向供应商提交 PO</li> <li>5. 供应商发运服务器</li> <li>6. 物材部接收货品</li> <li>7. IT 部安装服务器和 OS</li> <li>8. IT 部配置 OS</li> <li>9. IT 部以人工方式使服务器和 OS 通过资格认定，</li> <li>10. 账户部将硬件资产作为资本费用 (CapEx) 支付费用并折旧</li> </ol>	<ol style="list-style-type: none"> <li>1. IT 部给出服务器需求</li> <li>2. IT 部选择匹配 EC2 实例类型和自带合格的 OS 映像，</li> <li>3. IT 部推出具有合格映像和启用日志自动记录的 EC2 实例，并</li> <li>4. IT 部使用运营成本 (OpEx) 信用卡为计量的 EC2 使用量付款。</li> </ol>

客户在 GxP 系统中使用 AWS 产品应当审核其 IT 采购流程，以确保自身能适应订购定价和在线交付模型。该审核应涉及组织的 IT、采购和质量保证团队，并应纳入订购、接收和付款以及 AWS 账户管理。AWS 提供了文档以帮助组织了解和管理其 AWS 账户账单。

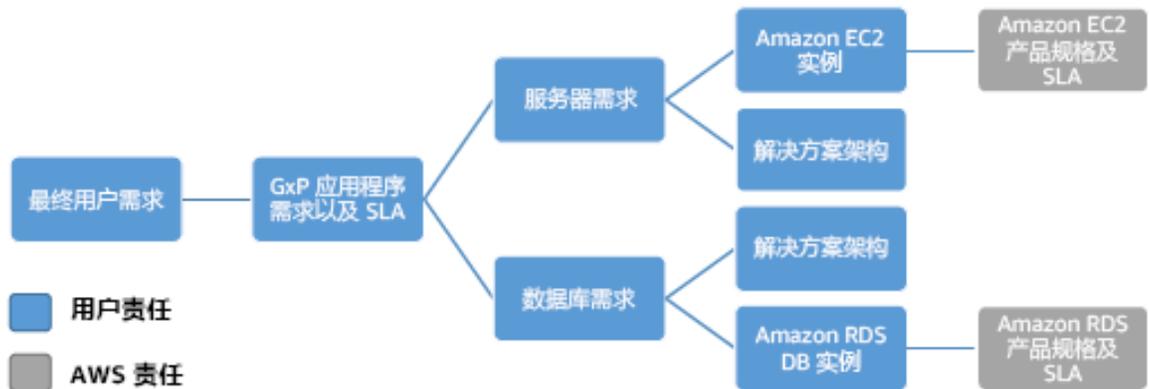
- AWS 账单和成本管理白皮书  
<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/awsaccountbilling-aboutv2.pdf>
- 通过详细的账单报告了解您的使用情况：  
<https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/detailed-billing-reports.html>
- AWS 每月账单简易计算器 <http://calculator.s3.amazonaws.com/index.html>
- 客户应考虑更新以下文档以支持其对 AWS 产品的使用：

客户应考虑更新以下文档以支持其在 GxP 系统中使用 AWS 产品：

- 采购流程
- AWS 详细账单报告
- 以电子邮件发送的 PDF 发票

### 3.1.5 产品评估

确保购买的商品和服务符合指定要求是 GxP 控制的关键要求。对于像 AWS 产品这样的商用基础设施组件，要确保产品规格符合用户要求是很直接的，因为所有 AWS 产品接口规格和协议都已完整记录并可供客户审查。由于 AWS 并未为单个客户定制 AWS 产品或 SLA，因此客户只需将其 GxP 应用程序需求对应至相应的 AWS 产品规范和 SLA。例如，想要使用 AWS 的 Amazon EC2 产品和 Amazon RDS 产品运行 COTS 可配置软件应用程序的客户应首先记录该应用程序的服务器要求（CPU、内存等）和数据库要求，然后转到 Amazon EC2 和 Amazon RDS 产品页面以确定可满足应用程序要求的虚拟服务器系列（即 EC2 实例类型）和数据库类型（即数据库实例类型）。



请务必注意，GxP 系统 SLA 并非单个 AWS 产品 SLA 的直接功能，而是客户配置和使用 AWS 产品（即他们的解决方案架构）的功能。例如，如果 GxP 应用程序需要的可用性级别高于单个 AWS 产品提供的可用性，则客户可以设计其解决方案以实现更高的可用性级别。因此，在评估 AWS 产品对特定 GxP 系统的适用性时，必须考虑整体解决方案架构。

在为自定义（GAMP 类别 5）应用程序或医疗设备评估 AWS 产品时，产品评估将要求 GxP 客户在其 SDLC 计划阶段同时探索系统环境、潜在的架构和设计以及可用的 AWS 产品。为了支持现有客户和潜在客户评估 AWS 产品是否满足其应用程序要求，AWS 在线发布了技术产品文档，并使客户能够在批准其 GxP 系统设计之前试用 AWS 产品。

- AWS 产品文档：<https://aws.amazon.com/documentation/>

客户应考虑更新以下文档以支持其在 GxP 系统中使用 AWS 产品：

- SDLC 流程
- GxP 系统需求及风险评估
- GxP 系统解决方案架构
- AWS 产品评估

### 3.1.6 供应商评估

有 GxP 要求的组织需要根据满足指定要求的能力来评估和选择其潜在的供应商、承包商和顾问。一旦客户执行了产品评估并确定 AWS 产品可以满足其 GxP 系统架构的要求，就可以执行供应商评估，以确保 AWS 可以根据其发布的接口规范和 SLA 可靠地交付 AWS 产品。

AWS 运营行业领先的管理控制框架，该框架符合商业 IT 组织当前的质量、安全性和信任标准。由合格的第三方审计人员定期进行 AWS 控制的合规性评估，并将这些评估中的合规性报告提供给客户，以使它们能够评估 AWS 作为供应商的服务能力。AWS 合规性报告指明了 AWS 产品和评估区域的范围，以及评估者的合规证明。

控制机制	评估条件	审计人员	合规报告
ISO 27001	ISO/IEC 17021 及 27006	EY CertifyPoint	<a href="https://aws.amazon.com/compliance/iso-27001-faqs/">https://aws.amazon.com/compliance/iso-27001-faqs/</a>
ISO 27017	ISO/IEC 17021 及 27006	EY CertifyPoint	<a href="https://aws.amazon.com/compliance/iso-27017-faqs/">https://aws.amazon.com/compliance/iso-27017-faqs/</a>
ISO 9001	ISO/IEC 17021	EY CertifyPoint	<a href="https://aws.amazon.com/compliance/iso-9001-faqs/">https://aws.amazon.com/compliance/iso-9001-faqs/</a>
SOC 1	AT 801 &	EY	<a href="https://aws.amazon.com/compliance/soc-faqs/">https://aws.amazon.com/compliance/soc-faqs/</a>
SOC 2			
SOC 3	AT 101 控制， TSP 100 部分，信 任及证明		
FedRAMP/ NIST 800- 53r4	NIST 800-53a	Veris Group	<a href="https://www.fedramp.gov/marketplace/compliant-systems/amazon-web-services-aws-eastwest-us-public-cloud/">https://www.fedramp.gov/marketplace/compliant-systems/amazon-web-services-aws-eastwest-us-public-cloud/</a>
PCI-DSS v3.1 Level 1	PCI DSS 安全审计 流程	Coalfire	<a href="https://aws.amazon.com/compliance/pci-dss-level-1-faqs/">https://aws.amazon.com/compliance/pci-dss-level-1-faqs/</a>

其他在线资源可用于为客户提供有关 AWS 安全流程以及 AWS 产品当前和过去性能历史的透明度：

- AWS 风险和合规性白皮书，附录 A：CSA 问卷  
[https://d0.awsstatic.com/whitepapers/compliance/AWS\\_Risk\\_and\\_Compliance\\_Whitepaper.pdf](https://d0.awsstatic.com/whitepapers/compliance/AWS_Risk_and_Compliance_Whitepaper.pdf)
- AWS 安全流程白皮书概览  
<https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf>
- AWS 服务运行状况控制面板和状态历史  
<http://status.aws.amazon.com/>

GxP 客户应考虑更新其供应商评估流程，以确保所有供应商类别均可适应 AWS 产品。对于以前在非 GxP 系统中使用过 AWS 产品的 GxP 客户，他们对 AWS 的 GxP 供应商评估还应包括对那些非 GxP 系统的性能历史审查，包括归因于 AWS 且客户无法通过其解决方案架构解决的任何与系统相关的问题。

客户应考虑更新以下文档以支持其在 GxP 系统中使用 AWS 产品：

- GxP 供应商分类和评估流程
- 非 GxP 系统性能审查
- AWS 供应商评估数据，包括供应商问卷
- AWS 供应商审批报告
- AWS 合规性报告和白皮书
- 另请参阅供应商协议（第 17 页）

### 3.1.7 供应商协议

与 IT 供应商的协议对于具有 GxP 系统的组织很重要。这包括明确列出的 IT 供应商对共担责任和承诺的声明，以确保将供应商产品的重大更改通知组织。由于 AWS 产品是标准化的并且对每个客户都是相同的，因此 AWS 产品协议也已经标准化，并且包括 AWS 和客户义务的定义，以及 AWS 产品更改的通知机制。

AWS 协议在下面列出，附录（第 34 页）包含这些 AWS 协议中部分与 GxP 相关的职责的表格。

- 客户协议 <https://aws.amazon.com/agreement/>

- 企业协议 联系 AWS 销售人员
- 安全性附录 联系 AWS 销售人员
- 客户支持 <https://aws.amazon.com/premiumsupport/>
- 服务条款 <https://aws.amazon.com/service-terms/>
- 可接受使用政策 <https://aws.amazon.com/aup/>

产品特定的服务级别协议 (SLA) :

Amazon S3	<a href="https://aws.amazon.com/s3/sla/">https://aws.amazon.com/s3/sla/</a>
Amazon EC2 和 EBS	<a href="https://aws.amazon.com/ec2/sla/">https://aws.amazon.com/ec2/sla/</a>
Amazon RDS	<a href="https://aws.amazon.com/rds/sla/">https://aws.amazon.com/rds/sla/</a>
Route53	<a href="https://aws.amazon.com/route53/sla/">https://aws.amazon.com/route53/sla/</a>
CloudFront	<a href="https://aws.amazon.com/cloudfront/sla/">https://aws.amazon.com/cloudfront/sla/</a>

- 数据处理附录  
<https://aws.amazon.com/compliance/eu-data-protection/>

在 GxP 系统中使用 AWS 产品的客户应仔细考虑他们需要 AWS 的支持级别。AWS 支持分为四层：基本、开发人员、业务和企业，每层都有不同级别的案例严重性等级和响应时间。根据客户的支持场景，例如在进行具有正当理由的法规检查时对系统相关问题进行故障排除（请参阅第 28 页），AWS 支持层将确定客户请求的响应时间。AWS 的许多当前 GxP 客户维持业务级，或企业级的支持以适应这些场景。

客户应审查并在必要时更新其 IT 供应商协议政策，以确保其与 AWS 的标准化运营和协议模型兼容。对于具有使用托管服务提供商、利基 GxP 服务和主机托管提供商的历史的组织而言，这尤其需要，在这些组织中，供应商可以自定义服务并代表客户执行应用程序开发、验证和维护活动。

客户应当考虑更新以下文档以支持其对 GxP 系统中 AWS 产品的使用：

- IT 供应商协议政策
- 适用的协议于上方列出

### 3.1.8 记录和日志

对于每个 GxP 系统，生命科学组织需要标识出作为 GxP 证据所需的可保留记录和日志，并在整个保留期内保持记录的完整性和可用性。在 GxP 系统中使用 AWS 产品时，可保留记录主要包括其 GxP 系统中的客户数据、GxP 系统软件代码和 SDLC 记录，以及客户的 AWS 账户中可用的系统生成的日志和审计跟踪。由于 AWS 产品和现代 SDLC 方法可实现高度自动化，因此许多以前通过手动流程（如基于纸张的安装协议）创建的可保留记录现在通过程序化执行的命令生成。从 GxP 数据角度和 SDLC 角度来看，这种更可靠的记录生成方式可以降低可变性并明显改善数据完整性。

由于与自动化 IT 流程关联的记录类型和格式与手动生成记录的有很大不同，因此 GxP 客户务必应确定需要保留的记录类型和格式，并适当制定其记录保存准则。还应评估 GxP 医疗设备和应用程序中使用的 AWS 产品对设计历史文件 (DHF) 和设备主记录 (DMR) 的记录保存影响。在许多情况下，AWS 产品以程序化方式生成的记录（例如审计跟踪和警报）是完全可迁移的，既能保留在客户的 AWS 账户中，也可以通过将记录传输到其他位置来保留。

客户应考虑更新以下文档以支持其在 GxP 系统中使用 AWS 产品：

- 记录保留时间表
- 记录类型和格式准则
- 记录保留流程
- CloudTrail 日志
- CloudWatch 警报
- S3 和 Glacier 保留政策和生命周期规则
- AWS Support 案例历史

### 3.2 系统开发生命周期

除了对组织的质量体系要求外，每个 GxP 系统还必须具有某些功能和受控的 SDLC 流程来交付它们。适用于每个系统的特定功能和 SDLC 控制取决于多种因素，并由法规派生而出，例如美国的 21 CFR Part 11 和 820，欧盟的 Annex 11 和 93/42/EEC 及其国际等效规定。这些监管制度的总体目的是确保 GxP 系统能够实现其预期用途，并且数据可信赖且可靠，因为它可用于医疗服务的交付，或就诸如人类食品、药物和医疗设备以及动物食品和药物之类的医疗产品的安全性和有效性做出决策。

#### GxP 系统的 SDLC 控制：

- 控制设计和开发，以确保满足指定的要求
- 验证软件应用程序并限定基础设施，以确保准确性、可靠性和一致的预期性能
- 在生产环境中运行的系统的更改控制和更改历史，包括系统用户文档
- 生产环境中的监视系统，以检测和应对不合格情况（即错误）
- 记录和处理与系统有关的投诉和用户支持案例
- 在整个系统生命周期（包括弃用）中保留 SDLC 记录和 GxP 数据

#### GxP 系统需求的功能：

- 能够以人类和机器可读的形式生成准确且完整的 GxP 数据副本
- 数据输入验证和完整性检查
- 用户访问控制和用户操作授权检查
- 用户操作和数据更改的安全、计算机生成且带有时间戳的审计跟踪
- 检查以确认实施步骤的许可排序（即工作流实施）
- 数据传输中和静态加密
- 对数据进行用户授权的操作的电子签名清单
- 电子签名与关联数据之间的链接

用传统的 IT 基础设施模型来满足这些要求是很麻烦的，因为基于软件的应用程序 SDLC 和基于硬件的基础设施 SDLC 完全不同，并且由不同制造商制造的物理基础设施组件需要大量的手动程序控制，以确保维持配置并在可整个基础设施中追溯更改。借助 AWS 产品，公司可以使用一套统一的虚拟化基础设施产品来代替其物理基础设施产品，从而使他们能够将整个基础设施作为软件代码来创建和管理。客户不仅可以使用 Amazon EC2 之类的 AWS 产品从版本控制的映像启动相同的虚拟服务器，还可以使用基于软件的配置模板开发、版本控制和部署其整个基础设施，包括存储、数据库和联网。这种基础设施即代码的方法为整个系统

(包括应用程序和基础设施) 在 SDLC 中提供了前所未有的控制力、统一性和自动化级别。这也意味着, 与传统的 IT 模型相比, 同步开发、测试和生产环境所需的工作量要少得多。

尽管 AWS 产品通常与 SDLC 方法 (如开发运营) 相关联, 但 SDLC (如瀑布和 V 模型) 受到完全支持。本节将使用一个一般化的三阶段 SDLC 示例, 向在 GxP 系统中使用 AWS 产品的客户解释一些注意事项。



### 3.2.1 开发

GxP 系统需要按照记录的流程进行开发, 以确保系统满足其指定要求。在 GxP 系统中使用 AWS 产品的客户对所有 GxP 系统开发活动负全部责任, 包括计划、编程、构建、配置、测试、验证和部署其应用程序, 以及架构设计、预置、配置、编排、部署、资格验证和操作其软件定义基础设施。AWS 不会代表客户设计或开发 GxP 系统, 但是, AWS 产品具有大量的用户文档和白皮书, GxP 系统工程师可以将其用作系统设计和开发活动的输入。

GxP 系统的设计输入要求还应包括网络安全要求, AWS 建议客户遵循公认的安全计划标准 (例如 NIST 特别出版物 800-13) 和任何适用的监管指南文件 (例如 FDA 的医疗设备网络安全管理的上市前提交内容) 制定 GxP 系统安全计划。

尽管客户可以使用 AWS 产品制作多种类型的系统, 但是只有两种基本的开发场景: 1) 购买 COTS 应用程序或 2) 构建自定义应用程序。



在评估与 AWS 产品一起使用的 COTS 软件包时，GxP 客户应在评估中纳入 AWS 合作伙伴网络 (APN) 技术合作伙伴和 AWS Marketplace。AWS 技术合作伙伴提供了托管在 AWS 平台上或与 AWS 平台集成的软件解决方案，而 AWS Marketplace 是一个在线商店，客户可以在其中购买与 AWS 兼容的软件并将其直接部署到其 AWS 账户中。

- APN 技术合作伙伴 <https://aws.amazon.com/partners/technology/>
- AWS Marketplace <https://aws.amazon.com/marketplace/>

AWS 产品还可以与 APN 网络或 AWS Marketplace 外部的商业软件应用程序一起使用，但是，客户需要查看应用程序许可协议并执行产品评估（请参阅前文第 14 页），以确定该应用程序与 AWS 产品的兼容性。APN 咨询合作伙伴也可辅助此等活动 <https://aws.amazon.com/partners/consulting/>。

尽管生命科学组织通常更喜欢购买软件应用程序而不是构建它们，但将 AWS 产品与现代 SDLC 方法结合起来的主要好处是能够快速、重复和可靠地交付定制软件解决方案。如今，由于自动化的工具已经减少或消除了由手动开发活动引起的延迟和错误，许多阻碍组织构建软件的历史性原因（例如从源代码手动构建软件包或手动进行回归测试）已经消失了。AWS OpsWorks、AWS CodeCommit 和 AWS CodePipeline 等 AWS 产品为系统工程师提供了灵活的可配置工具，可帮助他们满足其独特的组织要求，同时还简化了软件开发活动的 SDLC 控制的实施。

在客户完成开发并准备好将其 GxP 系统部署到验证、生产或其他环境中之后，AWS 产品（例如 Amazon 系统映像 (AMI)、AWS CloudFormation、AWS CodeDeploy 和 AWS Elastic Beanstalk）将使一致且受控的部署变得容易且可重复。这些工具还能够创建从网络堆栈到数据库、从存储卷到计算实例的整个系统环境的版本控制副本。可以保留这些版本控制的副本，以用于归档和更改管理，或用于预置新的开发/测试环境以便执行持续的开发或问题排查。

这种持续开发和持续部署的新模型是众多行业中如此多客户使用 AWS 产品创新业务的主要原因之一。为了在其 GxP 系统中利用这些优势，客户可能需要审查并更新其开发方法和流程。

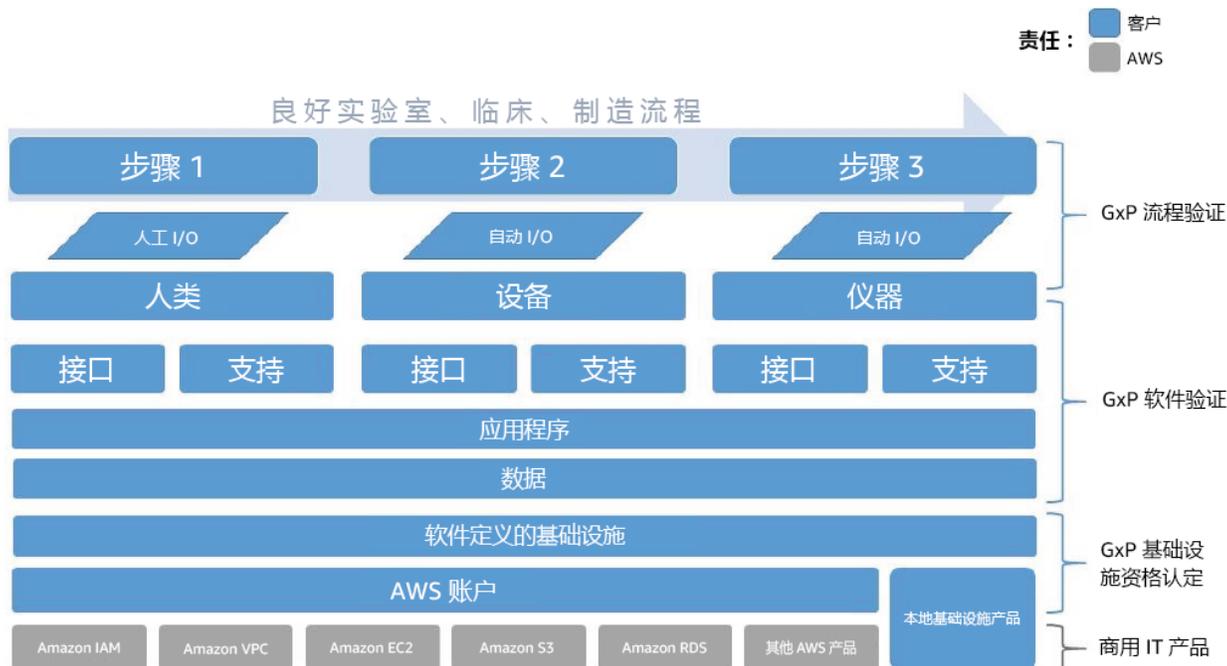
客户应考虑以下文档，以支持其在 GxP 系统中对 AWS 产品的使用：

- SDLC 流程
- 系统设计和开发计划
- 危害评估流程
- 代码检查 SOP
- 用例和用户故事或其他要求规范
- 最终用户 SLA 条件，包括最终用户支持
- 软件架构规范
- 应用程序功能要求
- GxP 医疗和移动应用程序的初步风险（或危害）分析
- AWS CloudTrail 和 Config 日志
- 应用程序源代码
- EC2 AMI 和 CloudFormation 模板
- 代码部署 SOP

### 3.2.2 验证

需要验证 GxP 应用程序以确保软件规格符合用户需求要求，并且需要对运行 GxP 应用程序的软件基础设施进行资格验证，以确保其满足该应用程序的系统要求。由于 AWS 产品是完全基于自助方式提供的，因此在 GxP 系统中使用 AWS 产品的客户应对其 AWS 账户中的所有软件验证和基础设施资格认证活动完全负责。由于 AWS 不代表客户开发或管理应用程序，也不预置

或配置特定于客户的基础设施，因此 AWS 无法代表客户执行 GxP 验证或资格认证活动。AWS 负责确保 AWS 产品符合 AWS 产品规格、SLA 和商业 IT 标准，GxP 客户负责验证其使用 AWS 产品构建的 GxP 系统。



与传统的物理基础设施和安装介质相比，AWS 产品的应用程序和基础设施的安装、实例化和部署有着根本性的差异。在物理基础设施硬件时代，安装活动是高度手动和协议驱动的。协议通常是针对每个系统组件分别开发和预先批准的，然后由操作员手动执行，同时有验证员待命在旁以确保正确完成每个步骤。完成后，该协议将由质量代表进行审核和批准。随着 IT SDLC 的成熟和服务器虚拟化的普及，尽管仍然是高度手动的，但验证活动已从协议驱动活动转变为流程驱动活动。一些组织会使用协议创建合格的“黄金映像”，然后按照流程使用合格的映像创建虚拟服务器。



在基础设施由软件定义的云时代，GxP 系统工程师能够使用版本控制的基础设施模板对整个系统堆栈进行版本控制并自动进行部署。AWS 客户之间的常见做法之一是创建合格的系统模板，并将其与自动部署工具结合使用以预置单独的资源，以及整个开发、测试和验证环境。每个 AWS 产品中都内置的 Web 服务 API 技术还允许利用第三方 API 验证工具（例如 RunScope 和 SoapUI），来比以前手动定期验证更频繁地对预期的系统行为进行资格认定和验证。

由于这种从时间点手动活动到连续自动活动的范式转换，许多生命科学组织在传统硬件基础设施上遵循的 GxP 更改控制和验证实践应进行审查和更新，以解决使用 AWS 的商业云产品作为 GxP 系统组件时，自动化基础设施模型的问题。

客户应考虑以下文档，以支持其在 GxP 系统中对 AWS 产品的使用：

- SDLC 流程
- 验证流程
- IT 资格认定流程
- 自动化部署流程
- AWS CloudTrail 和 Config 日志
- 应用程序源代码
- EC2 AMI 和 CloudFormation 模板

### 3.2.3 运营

在生产操作中开发、执行、控制和监视 GxP 系统对于确保它们持续符合规范非常重要。当最终用户出现问题或系统出现偏差时，具有 GxP 系统的组织还需要维护一个响应、纠正和预防这些问题的过程。尽管可以利用 AWS 产品执行这些活动，但是 AWS 不会代表客户执行 GxP 系统的操作和监视活动。

GxP 系统原则	要求总结	注意事项
<b>更改控制</b>	生产中对 GxP 系统的更改应得到验证或确认，以确保系统满足定义的用户要求。	客户：定义系统用户要求并配置和认证 AWS 产品以满足这些要求的是客户。客户负责核查和验证他们对用户需求和产品配置实施的更改。

GxP 系统原则	要求总结	注意事项
		AWS：AWS 无法控制客户需求或产品配置。因此，AWS 无法代表客户核查或验证 GxP 系统更改。但 AWS 会验证对 AWS 产品的更改，以确保满足产品规格和 SLA。
<b>服务等级协议</b>	GxP 系统用户与维护 GxP 系统的任何第三方（包括 IT 部门）之间必须达成正式协议。	<p>客户：客户定义 GXP 系统的服务级别协议，并且必须配置和使用 AWS 产品来满足 SLA。</p> <p>AWS：AWS 产品 SLA 与 GxP 系统 SLA 不同，AWS 无法控制或了解客户为系统建立的 SLA。</p> <p>请参阅附录 4.3，AWS 协议中的共担责任</p>
<b>最终用户支持</b>	GxP 系统所有者应建立向最终用户提供支持的流程。	<p>客户：客户负责为 GxP 系统最终用户提供支持。</p> <p>AWS：AWS 不为 GxP 系统最终用户提供任何支持或服务。</p>
<b>备份和恢复</b>	应定期备份 GxP 数据，并且应包括数据完整性和可恢复性的验证。	<p>客户：客户负责配置和使用 AWS 产品来维护适当的数据安全性、保护和备份。</p> <p>AWS：AWS 无法控制客户的产品配置，AWS 无法洞悉客户的内容（即数据）。因此，AWS 不会代表客户备份客户内容。</p>
<b>事件响应</b>	GxP 系统事件应进行报告、评估和记录。	<p>客户：客户负责从其最终用户和系统管理员接收事件报告，并评估和归档这些报告。如果事件需要 AWS 支持，则客户可以使用与其支持协议一致的方法提交支持案例。</p> <p>AWS：AWS 无法洞悉 GxP 系统事件，但是，将根据客户的支持级别协议评估和调查提交给 AWS 的与 AWS 产品相关的客户支持案例。客户支持案例历史记录在案，并可以在线提供给客户。</p>
<b>纠正和预防措施</b>	GxP 系统应具有纠正和预	客户：客户控制 GxP 系统不符合项的识别和

GxP 系统原则	要求总结	注意事项
	防系统不合格项的流程。	跟踪，并负责实施所需的纠正和预防措施。  AWS：AWS 无法洞悉系统操作和不合格之处，因此无法对系统实施纠正和预防措施。但 AWS 会维护针对 AWS 产品的持续改进计划，并且该计划已包含在质量和安全性证明的范围内。

Web 服务技术与现代的自动部署实践相结合，可以通过允许单个系统组件的更新（系统停机时间极短，通常不需要停机）或打破依赖关系来进行更新，从而提高进行连续开发的系统的速度和弹性。只要 API 接口规范没有更改，客户就可以与系统交互并相信（但需要验证）正在使用的功能将可用。使用 AWS 产品的客户可以受益于 Web 服务 API 的各个方面，尽管客户仍必须构建其系统以应对 API 中断。基于 API 的系统还可以与更改控制系统（例如 Remedy、ServiceNow、Sparta Systems 和其他更改管理跟踪系统）集成在一起，从而提供具有 GxP 质量署名的软件开发和部署管道的完全集成。

为了使 GxP 客户获得这些运营优势，他们应该审查并在需要时更新其运营文档和记录，以使其与 AWS 产品保持一致。

客户应考虑以下文档，以支持其在 GxP 系统中对 AWS 产品的使用：

- 更改控制流程
- 配置管理流程
- 发布到生产流程
- 监控流程
- AWS CloudTrail 和 Config 日志
- 应用程序源代码
- EC2 AMI 和 CloudFormation 模板
- 客户支持案例历史

### 3.3 法规事务

在 GxP 监管的行业中，法规事务专业人员使用 GxP 系统中的数据向监管卫生当局和伦理委员会提交备案和注册文件。他们还制定和维护托管监管机构检查的流程，并在其组织寻求分发 GxP 产品的区域内跟踪不断变化的立法。当 GxP 客户在其 GxP 系统中使用 AWS 产品时，他们的 IT、质量和法规事务团队应讨论产品可能对法规实践造成什么影响（若有），包括

- 监管提交和
- 卫生当局检查，以及任何
- 审查委员会和伦理委员会要求。

#### 3.3.1 提交

使用 GxP 系统进行监管提交并不是什么新鲜事，并且已经有了基于云的软件应用程序来生成、跟踪和发送监管提交。实际上，FDA 使用 AWS 产品，通过 openFDA.gov 平台发布监管提交的数据。GxP 客户需要考虑的新问题是，监管提交内容中是否应包括他们的 GxP 系统，如果是，则客户的监管团队将如何处理 AWS 产品的使用。

例如，医疗设备软件应用程序（例如图片存档和通信系统 (PACS)）可能需要完成 510k 提交才能获得 FDA 批准。如果将 PACS 设计为可在与 AWS 的 Amazon EC2 产品兼容的通用 x86 服务器上运行，则 PACS 的 510k 可能没有特别提及 AWS 产品，而只是声明：“该软件应用程序是与通用计算服务器一起使用的 PACS。”

将 AWS 产品包括在法规提交中的决定是 GxP 客户的责任，如果有任何与提交相关的问题，AWS 建议 GxP 客户寻求合格的法规事务专业人士的建议。

#### 3.3.2 检查

卫生当局可以随时检查生命科学组织及其 GxP 系统。尽管 COTS IT 产品在接受机构检查的 GxP 系统中具有悠久的历史，但是在 GxP 系统中使用 AWS 之类的 COTS 云产品提供商尚属新鲜事物，并且机构现场检查人员可能不熟悉 AWS 产品或其用法。为了确保使用 AWS 产品的 GxP 系统获得令人满意的检查结果，AWS 建议 GxP 客户建立并维护包括以下要素的检查就绪计划：

- 识别客户组织内熟悉 GxP 系统中 AWS 产品的配置和使用的关键人员，
- 确保在进行 FDA 检查时通知那些关键人物并使其可参与其中的流程，以及
- 每个 GxP 系统的概要演示，以快速准确地将关键系统要素传达给 FDA 或卫生当局的检查员。客户应考虑在其演示材料中包括以下元素：
  - 系统标识，包括系统名称、版本（如果适用）和系统分类
  - 系统说明，包括对依赖系统的关键 GxP 活动和/或工作角色的简明概述；还应确定与其他系统的接口
  - 网络或架构图表，包括相关职责
  - 系统操作，包括访问系统的物理位置、最终用户数、接口和产品
  - 应用程序 SOP 列表，包括业务部门、技术或公司流程
  - 责任摘要，包括最终用户业务部门的名称、技术和管理责任、安全操作等

如果系统相关调查需要 AWS 提供产品问题排查支持，则客户选择的 AWS 支持层将确定提交支持请求的渠道以及 AWS 的预期响应时间。

客户应考虑以下文档，以支持其在 GxP 系统中对 AWS 产品的使用：

- 检查就绪计划
- GxP 系统概述演示
- 系统文档索引

### 3.3.3 研究参与者的个人数据隐私控制

临床研究中使用的 GxP 系统还可能需个人数据隐私控制，以保护由系统存储、处理或传输其个人可识别信息 (PII) 和受保护的健康信息 (PHI) 的个人的机密性。示例可能包括：

- 研究招募工具，
- 电子数据记录 (EC) 系统，
- 数据存储和归档，
- 诊断医疗设备应用程序，和
- 移动医疗设备应用程序。

机构审查委员会 (IRB)、独立道德委员会 (IEC) 和/或数据访问委员会 (DAC) 可能会要求使用涉及 AWS 产品的 GxP 系统进行人类研究的赞助者和研究者提供有关该系统如何保护研究参与者个人信息的信息，包括执行的所有系统安全性审查和安全性操作控制，例如描述不再需要时撤消系统访问的流程。在包含 PII 的 GxP 系统中使用 AWS 产品的客户应确保了解数据位置要求，并在必要时描述运行该系统的 AWS 产品中实施的安全性和数据位置控制措施。有关 AWS 产品中数据位置控制的其他信息，可在线访问

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html>。

客户应考虑以下文档，以支持其在 GxP 系统中对 AWS 产品的使用：

- PII 保护政策
- 数据位置控制计划
- GxP 系统的系统安全计划

## 4 结论

尽管 AWS 产品交付是通过 Internet 而非以物理方式进行的，但 GxP 客户仍对使用产品（包括他们使用 AWS 产品开发、验证和运营的应用程序和虚拟化基础设施）承担责任。使用本白皮书中的建议，GxP 公司可以评估其质量体系、SDLC 控制和法规事务计划，以证明对纳入 AWS 产品作为组件的 GxP 系统的有效控制。

## 5 文档修订

下表显示了此白皮书的完整修订历史记录。

日期	说明
2016 年 1 月	最初发布

## 6 附录

### 6.1 数据隐私资源

在 AWS，数据保护始终具有最高优先级。客户在使用 AWS 产品时可保留对数据的所有权和控制，AWS 也会努力为客户提供额外的隐私保证和透明度。本附录列出了 AWS 提供给客户的一些关键数据隐私资源。

- AWS 数据隐私常见问题  
<https://aws.amazon.com/compliance/data-privacy-faq/>
- Amazon 企业半年信息请求报告  
[http://d0.awsstatic.com/certifications/Information\\_Request\\_Report.pdf](http://d0.awsstatic.com/certifications/Information_Request_Report.pdf)
- AWS 第三方访问列表  
<http://aws.amazon.com/compliance/third-party-access/>
- 美国-欧洲安全港  
<https://safeharbor.export.gov/companyinfo.aspx?id=27379>
- 欧盟指令 95/46/EC 常见问题和模型条款  
<https://aws.amazon.com/compliance/eu-data-protection/>  
<http://www.cnpd.public.lu/en/actualites/international/2015/03/AWS/index.html>
- 美国基因型和表型数据库  
[https://d0.awsstatic.com/whitepapers/compliance/AWS\\_dBGaP\\_Genomics\\_on\\_AWS\\_Best\\_Practices.pdf](https://d0.awsstatic.com/whitepapers/compliance/AWS_dBGaP_Genomics_on_AWS_Best_Practices.pdf)
- US HIPAA 商业伙伴常见问题  
<https://aws.amazon.com/compliance/hipaa-compliance/>

## 6.2 附注的 21 CFR Part 11

本附录重点介绍了一些客户可以使用 AWS 产品来满足 21 CFR Part 11 法规的电子记录和电子签名要求的方式。

- **访问控制**：客户可以将 GxP 系统和数据访问限制为授权人员。客户可以使用 AWS 产品（例如 Amazon Identity and Access Management (IAM) 和 AWS Directory Service）实施访问控制。AWS 客户还可以将其账户访问控制配置为与现有的本地目录（例如 Microsoft Active Directory）一起使用，以创建用于混合云部署的无缝访问控制环境。
- **GxP 系统验证**：可以在 AWS 中部署和验证应用程序。客户可以根据其组织政策和流程来验证其 GxP 系统。
- **数据可回收性**：在整个记录保留期内，AWS 客户可以随时从其 AWS 账户生成和取回准确完整的记录副本。由于 AWS 客户保留对其 AWS 账户、系统和数据的根管理访问权限，因此只要客户启用 AWS 审计追踪产品和服务，他们就可以随时独立获取其数据或审计追踪。
- **审计追踪**：可以根据客户定义的政策来生成、监视、下载和保留安全、计算机生成的、带时间戳的审计跟踪。像 AWS CloudTrail 和 Amazon CloudWatch 这样的 AWS 产品使客户能够开发和操作日志记录系统，以满足从单个文件对象级别到应用程序级别的最高水平的数据和系统审核要求。
- **workflow 环境**：AWS 客户完全控制针对 GxP workflow 活动的操作系统检查，包括他们为 GxP 系统维护的 SDLC 流程。
- **用户授权**：权限检查可以在 AWS 账户及应用程序中使用基础设施级别的角色和权限组，从而可确保仅授权人员可以使用系统，或由 AWS 客户对数据采取行动。诸如 Amazon IAM 之类的产品使客户可以定义基础设施用户账户以及机器对机器服务账户所需的角色、安全级别和交易策略。
- **输入输出验证**：输入检查和不可否认性控制高度依赖于创建和更新 GxP 数据的人员、流程和技术。如果将 GxP 数据手动输入到 Web 或移动应用程序中，则 AWS 客户可以使用一系列手动流程来培训和验证其用户，然后再授予他们对该应用程序的访问权限。一旦被授予访问权限，应用程序级别控制措施就可以自动执行所需的输入检查。客户账户中的 AWS 产品可用于监视和控制工作站或移动设备等联网资源的连接。如果 GxP 数据是从本地仪器、设备传感器或应用程序计算过程自动生成的，则可以使用各种 AWS 产品（例如 Amazon Simple Queue Service (SQS) 和 Amazon Kinesis），以及支持用户和服务级别访问控

制的身份和访问管理工具，来启用和控制从客户本地环境到其 AWS 账户的数据排队和传输。

- **人员培训**：AWS 客户在其 AWS 账户内开发、维护和使用 GxP 数据和系统，这意味着他们可以遵循现有的政策和流程来确定其员工是否具有适当的教育水平和经验以及经过适当的培训来执行所分配的 GxP 任务。AWS 提供了广泛的技术文档和客户培训计划，以帮助客户 IT 工程人员实现其 AWS 学习目标，而广泛的 AWS 合作伙伴生态系统包括具有医疗保健和生命科学能力的第三方系统集成商和咨询合作伙伴。
- **系统文档**：客户可以使用他们现有的受控文档流程和系统来实现对系统文档的适当控制。可以使用适当的 URL 以及客户需要的任何特定于版本的信息来引用 AWS 技术文档。此外，由于每个客户在 AWS 中的虚拟基础设施本质上都是软件定义的基础设施，因此客户可以版本控制和存档用于定义其账户中 AWS 资源的整套代码和模板（请参阅合格的基础设施）。
- **安全控制**：客户可以使用其现有的客户端加密解决方案或 AWS 广泛的安全产品线（例如 Amazon Key Management Service (KMS)）和服务器端加密（诸如 Amazon Simple Storage Service (S3)、Amazon Relational Database Service (RDS) 和 Amazon Elastic Load Balancer (ELB) 之类产品中的透明数据加密 (TDS) 和安全套接字层 (SSL) 功能），实施诸如数据静态加密和传输中加密等其他措施。Amazon Virtual Private Cloud (VPC) 这种产品可让客户控制其虚拟联网环境并在其内部数据中心和 Amazon VPC 之间创建加密的硬件虚拟私有网络 (VPN) 连接，以便他们可以将云作为其现有网络的扩展。
- **电子签名**：对电子签名表现形式、签名/记录链接以及电子签名组件和控制措施的要求，通常在客户用于生成和维护其 GxP 数据的经过验证的应用程序中予以满足。客户应通过其 AWS 账户中的虚拟网络评估现有电子签名应用程序的适用性，或者通过自己开发自定义原生云应用程序的一部分来满足电子签名要求。当使用 AWS 产品满足密码控制等要求时，Amazon IAM 密码政策等开箱即用功能可允许客户根据其具体要求创建自己的密码复杂性和过期策略。
- **数据保留**：每个客户的 GxP 数据生命周期和保留要求的流程和政策都存在很大差异，具体取决于客户的组织和适用于它们的特定要求。在其 AWS 账户中设计和开发 GxP 数据管理解决方案时，客户应注意指定其机密性、完整性和可用性要求，包括对原始数据、衍生数据和元数据的所有记录保留政策。

### 6.3 AWS 协议中的共担责任

该表是对 AWS 标准协议中职责的辅助性总结，并不具有权威性。本部分中的职责概述仅适用于单个 AWS 产品，并且不包括 AWS 客户及其最终用户之间的 SLA 职责。

主题	责任	客户	AWS
联系人	维护与 AWS 账户关联的有效电子邮件地址 (客户协议 1.2)	x	
更改	通知客户 AWS 产品的重大更改或停用 (客户协议 2.1)		x
更改	支持早前版本的 AWS 产品 API，持续 12 个月 (客户协议 2.2)		x
更改	根据需要执行安全更新，以确保 AWS 产品的机密性、完整性和可用性 <a href="https://aws.amazon.com/security/security-bulletins/">https://aws.amazon.com/security/security-bulletins/</a>		x
内容	内容的制定、要旨、操作、维护和使用（即 GxP 记录和应用程序） (客户协议 4.1)	x	
内容	内容的安全性、保护和备份 (客户协议 4.2)	x	
支持	提供对 GxP 系统最终用户的支持 (客户协议 4.2)	x	
支持	对客户的基本支持 ( <a href="https://aws.amazon.com/premiumsupport/">https://aws.amazon.com/premiumsupport/</a> )		x
隐私	控制数据所在的地理区域	x	