Considerations for Using AWS Products in GxP Systems

January 2016

Notices

This document is provided for informational purposes only. It represents AWS's current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS's products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

Table of Contents

1 ABSTRACT

In 2006, Amazon Web Services (AWS) began offering IT infrastructure products to customers in the form of web services, now commonly known as cloud computing. Today, AWS provides a highly reliable, scalable, and low-cost infrastructure platform that powers hundreds of thousands of businesses in 190 countries around the world. Some of the key benefits of cloud computing are the opportunity to replace up-front capital infrastructure expenses with low variable costs that scale with usage and allow customers to spend more time on their core activities and less time on undifferentiated IT tasks.

With the cloud, organizations no longer need to plan for and procure physical devices and IT infrastructure weeks or months in advance. Instead they can instantly spin up hundreds or thousands of virtual machines using automated deployment tools and methods that deliver results faster while ensuring more consistency of controls and less manual errors. In order to benefit from adopting AWS Products, organizations with Good Laboratory, Clinical, or Manufacturing Practices (GxP) compliance requirements and their auditors will need to acquire new skills and consider changes to GxP policies and procedures that focus on making IT compliance more agile, automated, and security-oriented.

This whitepaper provides guidance for using AWS Products in the context of GxP and the content has been developed in conjunction with AWS pharmaceutical and medical device customers, as well as software partners, who are currently using AWS Products in their validated GxP systems. In order to ensure the suitability of the content, AWS took the additional step of engaging Lachman Consultant Services Inc. (Lachman Consultants) to review and contribute to the approach outlined in this whitepaper. Lachman Consultants is one of the most highly respected consulting firms on FDA and international regulatory compliance issues affecting the pharmaceutical and medical device industry today. Lachman Consultants has extensive experience working with companies specifically on matters pertaining to the establishment and development of GxP systems, including GxP guidelines in support of maintaining regulated data in a cloud environment. For further information on Lachman Consultants, visit www.lachmanconsultants.com.

Nevertheless, it remains incumbent upon AWS customers to consult with their own advisors to ensure that their GxP policies and procedures are suitable for current IT, software, and security practices using AWS Products.

2 INTRODUCTION

Amazon Web Services (AWS) provides cloud infrastructure software products that are increasingly used to store and process sensitive and regulated workloads in virtually every industry across the world. Healthcare and life science organizations are realizing the benefits of the AWS cloud and are leveraging AWS products as components of their regulated IT systems, including computerized systems that support Good Laboratory Practices, Good Clinical Practices, and Good Manufacturing Practices ("GxP") for medical devices, pharmaceuticals, biologics, and other food and medical product industries.

This document provides information to assist customers who want to use AWS Products to build computerized systems that store or process electronic records in the content of common GxP compliance and data integrity considerations.

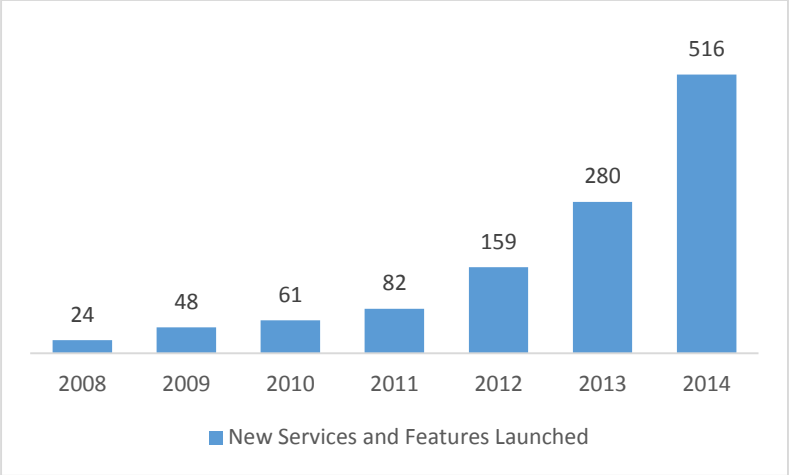
It will help customers understand:

- The scope and technological basis of AWS Products,
- The Quality System considerations customers may take into account when using AWS's commercial cloud products,
- The System Development Life Cycle considerations for customers who develop, validate and operate GxP systems that incorporate AWS Products as a component, and
- The Regulatory Affairs considerations for customers who may submit or provide their system-related information to regulatory agencies.

Whitepapers containing more specific information about AWS Products, privacy and data protection considerations are available at https://aws.amazon.com/compliance/.

2.1.1 About AWS

Founded in 2006 by Amazon.com (NYSE: AMZN), Amazon Web Services is a well-established cloud services provider offering a catalog of subscription-based infrastructure products that are delivered on-demand over the Internet from data center locations in the US, Australia, Brazil, China, Germany, Ireland, Japan, Korea, and Singapore. Since its inception, AWS has been an innovator in defining cloud computing by working to get new products in the hands of customers quickly, and then rapidly iterating and improving on those products based on customer feedback. The pace of innovation and continuous service improvements are a major reason why more and more organizations are choosing to use AWS Products for their mission-critical systems.



Customer obsession and customer trust are core leadership principles of Amazonian team culture. While customers retain ownership and control of their data and systems when using AWS Products, AWS works vigorously to provide assurance and transparency to customers by aligning with current privacy and data protection frameworks. See Data Privacy Appendix (page 31) for more.

- AMZN Corp. Info: http://phx.corporate-ir.net/phoenix.zhtml?c=97664&p=irol-irhome
- Leadership Principles: http://www.amazon.jobs/principles
- Analyst Reports: https://aws.amazon.com/resources/analyst-reports/

2.1.2 AWS Customers

AWS has more than one million active customers in over 190 countries representing virtually every industry and organization type, from owner-operated startups and small businesses to global enterprises and government agencies. Within our customer organizations, the primary users of AWS Products are software developers, network engineers, and system administrators who build and maintain the organization's IT infrastructure and applications. AWS has an extensive list of customer success stories that highlight the broad range of industries and markets that are benefiting from our cloud products, https://aws.amazon.com/solutions/case-studies/all/.

Healthcare and life sciences organizations are among those using AWS Products in their computerized systems, and the AWS Health website highlights some of their stories, https://aws.amazon.com/health/.

2.1.3 AWS Technology

Amazon Web Services (AWS) is named after a core technology built into all AWS Products, web services. A web service is a self-contained, reusable software module that makes its functionality available to other software modules over Internet protocols using

standardized messaging formats like XML[1] and JSON[2]. AWS Products, which are all available online through the self-service management console, https://aws.amazon.com/account/, are based on two types of web services, each with several types of interfaces:

Types of Web Services:

- Simple Object Access Protocol (SOAP)
- Representational State Transfer (REST)

AWS Product Interfaces:

- Application Programming Interface (API)
- Command Line Interface (CLI)
- Graphical User Interface (GUI)

Web services are not tied to any one operating system or programming language, which means that applications written in different programming languages and running on different platforms can seamlessly exchange data over the Internet (or intranet) using the pre-defined actions supported by each web service interface. A major advantage of the web service approach, sometimes called web oriented architecture, is that software applications that use web services do not need to know how the web service is built or how the underlying data is stored, they only need to know which actions the web service interface will respond to. As long as the actions are available in the interface, changes to the underlying components of a web service or the addition of new actions do not affect the behavior or reliability of the application. The list of web service actions supported by AWS Products are fully documented and available online, https://aws.amazon.com/documentation/.

In addition to web service technology, software defined infrastructure technologies like virtualization and software-defined networking (SDN) are core to AWS Products. Infrastructure components that were once only available as specialized physical equipment, such as network load balancers and firewalls, are now available as on-demand software-defined resources, which reduces system development timelines and expenses while enabling a higher level of infrastructure standardization and control through software automation.

The expansion of software to include traditionally physical infrastructure components combined with the benefits of web oriented architecture and modern programming methodologies are driving a global transition in IT SDLCs[3], staff skills, and IT compliance in every industry. The organizations that are poised to best leverage AWS Products in their GxP systems are those who recognize and adapt to this transition.

[1] eXtensible Markup Language
[2] JavaScript Object Notation
[3] System Development Life Cycle

Advantages of AWS Technology:

- **Platform Independence and Interoperability:** AWS Products support applications written in many programming languages and do not restrict applications to specific operating systems or hardware components.
- **Scalability:** Combining software defined infrastructure with AWS Products with modern programming methods lets AWS customers design their computerized systems to rapidly scale resources (and their costs) up or down based on actual demands on the system.
- **Fault Tolerance:** AWS Products support loose coupling between AWS Products and software applications, which ensures that customers can architect their GxP systems to continue operating properly even if a system component or AWS Product is temporarily unavailable.
- **Segregation of Duties:** Separating physical infrastructure responsibilities from customer virtual infrastructure and software responsibilities provides a critical data integrity control by ensuring that those with physical access are completely isolated from those with logical access to GxP data.
- **Auditability:** The message-based interoperability of web services allows customer configuration and use of AWS Products to be uniformly logged, monitored, and audited.
- **Focus on Core Competencies:** The ultimate benefit of AWS Products is that our customers can spend less time doing undifferentiated tasks and more time focusing on their core competencies that add value to their organization.

2.1.4 AWS Products

AWS makes commercial cloud infrastructure software products and office productivity applications that are user-configurable, general purpose in nature, and delivered to commercial IT standards like ISO, NIST, SOC and others. This is similar to other general purpose IT products and services such as database engines, operating systems, programming languages, internet service providers, etc. Many organizations categorize AWS products as commercial-off-the-shelf (COTS) infrastructure software products, which is consistent with the US federal government's use of AWS Products as a COTS item through a federal procurement program called FedRAMP. Under FedRAMP, which inherits definitions from the US Federal Acquisition Regulation (FAR), COTS items are 1) products or services that are offered and sold competitively in substantial quantities in the commercial marketplace based on an established catalog, 2) offered without modification or customization, and 3) offered under standard commercial terms and conditions. AWS customers with GxP requirements are responsible for categorizing AWS products using their applicable industry designations such as Category 1 under Good Automated Manufacturing Practices (GAMP) and Pharmaceutical Inspection Co-operation Scheme (PIC/S) guides for computerized systems in regulated GxP environments or, under medical device quality frameworks, Software of Unknown Provenance (SOUP), "black box" OTS components, or general purpose computing resources.

AWS offers over 50 products falling to several groups:

Group	AWS Products
Compute	Amazon EC2, Amazon EC2 Container Service, AWS Elastic Beanstalk, AWS Lambda, Auto Scaling
Storage	Amazon S3, Amazon CloudFront, Amazon EBS, Amazon EFS, Amazon Glacier, AWS Storage Gateway, AWS Snowball
Database	Amazon RDS, Amazon DynamoDB, Amazon ElastiCache, Amazon Redshift
Networking	Amazon VPC, AWS Direct Connect, Elastic Load Balancing, Amazon Route 53
Developer Tools	AWS CodeCommit, AWS CodePipeline, AWS CodeDeploy, AWS Tools & SDKs
Management Tools	Amazon CloudWatch, AWS CloudFormation, AWS CloudTrail, AWS Config, AWS Management Console, AWS OpsWorks, AWS Service Catalog, Trusted Advisor, AWS Tools for Windows PowerShell
Security and Identity	Identity & Access Management, AWS Directory Service, Amazon Inspector, AWS CloudHSM, AWS KMS, AWS WAF
Analytics	Amazon EMR, AWS Data Pipeline, Amazon Elastisearch Service, Amazon Kinesis, Amazon Kinesis Firehose, Amazon Machine Learning, Amazon QuickSight
Mobile and Internet of Things (IOT)	AWS IoT, AWS Mobile Hub, Amazon API Gateway, Amazon Cognito, AWS Device Farm, Amazon Mobile Analytics, AWS Mobile SDKs, Amazon SNS
Application Services	Amazon API Gateway, Amazon AppStream, Amazon CloudSearch, Amazon Elastic Transcoder, Amazon FPS, Amazon SES, Amazon, SNS, Amazon SQS, Amazon SWF
Enterprise Productivity Applications	Amazon WorkSpaces, Amazon WAM, Amazon WorkDocs, Amazon WorkMail

Details and specifications for AWS Products, global infrastructure and customer sign-up are available online:

- https://aws.amazon.com/account/
- https://aws.amazon.com/products/
- https://aws.amazon.com/documentation/
- https://aws.amazon.com/about-aws/global-infrastructure/

3 USING AWS PRODUCTS IN GXP SYSTEMS

Although the delivery model for AWS Products is virtual online products instead of physical on-premises products, the responsibilities for using them as components in GxP systems are similar. Under this well-established model, customers who configure and use commercial infrastructure products as components in their GxP systems have responsibilities in several key areas:

- Quality Systems,
- System Development Life Cycle, and
- Regulatory Affairs.

3.1 Quality Systems

Organizations seeking to use AWS Products in GxP systems should review and update their quality system documentation and this section provides guidance on some of the key areas to consider.

3.1.1 Management Responsibility

Before using AWS Products in production GxP Systems, customers should consider how they will manage the creation and maintenance of their AWS accounts. Since AWS account creation is self-service and account creators are granted root account credentials with full control of AWS Product configurations and access controls, management with executive responsibility within the customer organization should define and communicate an AWS account governance policy to ensure that their account(s) used in GxP Systems are tracked and that root account credentials are controlled by qualified individuals who are authorized by the organization. Additionally, a password policy should be applied to the AWS account to require all account users to rotate their passwords.

Customers should consider updating the following documents to support their use of AWS Products in GxP Systems:

- AWS Account Governance Policy
- Memo to All Staff with Purchasing Authority for the Organization
- AWS Account Creation Procedure
- AWS Account User Password Policy

3.1.2 Personnel

AWS customers are responsible for ensuring their personnel have the education, training, and experience to perform their assigned job functions. When job functions include using AWS Products in GxP systems, then experience level with AWS Products should be taken into consideration when hiring and/or training personnel. The level of system access and job functions performed are relevant for determining the experience level required, and there a number of job functions that may be impacted:

- Software engineers
- Software testers
- Network engineers
- System administrators
- Security engineers
- Validation engineers
- Purchasing staff
- Quality Assurance staff
- Auditors
- Note: GxP application end users generally do not interact directly with AWS Products and likely don't need AWS-specific training

Training may consist of awareness training, training *per se*, or test-based employee qualification. AWS and the Amazon Partner Network (APN) provide an array of initial and ongoing training and certifications with AWS Products, including:

- Online Documentation: https://aws.amazon.com/documentation/
- Instructional Videos: https://aws.amazon.com/training/intro_series/
- Self-paced Labs: https://aws.amazon.com/training/self-paced-labs/
- Events and Webinars: https://aws.amazon.com/about-aws/events/
- Classes and Workshops: https://aws.amazon.com/training/course-descriptions/
- Partner Training: https://aws.amazon.com/partners/training/
- Professional Certifications: https://aws.amazon.com/certification/

Customers should consider updating the following documents to support their use of AWS Products in GxP Systems:

- Training plans and procedures
- Job descriptions
- Job applications, resumes and CVs
- Training records
- Certifications with AWS Products

3.1.3 Audits

For customers auditing their use of AWS Products in GxP Systems, it is important to assess the ongoing effectiveness of the system security and data integrity controls, and the SDLC. In order to conduct effective audits of AWS Product usage, IT auditors should familiarize themselves with web service technology, AWS Products and reading basic

scripts such as JSON. Ideally, auditors would have direct access to the relevant AWS account resources through Read Only Access Policies. Within the AWS account, auditors and assessors should review the relevant product feature configurations and logging data, such as:

- AWS account credentials
- Organizational contacts
- IAM users, groups and roles
- IAM providers for SAML and OpenID Connect
- Amazon EC2 security configurations
- Resource-based policies in other services like S3
- AWS Config Rules
- System activity logs in CloudTrail
- Change history in AWS Config
- System support case histories

AWS offers a range of auditing tools and educational resources to assist auditors who are preparing to audit the use of AWS Products in GxP Systems:

- AWS Auditing Whitepaper: https://do.awsstatic.com/whitepapers/compliance/AWS_Auditing_Security_Checklist.pdf
- AWS Operational Checklists Whitepaper: https://s3.amazonaws.com/awsmedia/AWS_Operational_Checklists.pdf
- AWS Security Audit Guidelines: https://docs.aws.amazon.com/general/latest/gr/aws-security-audit-guide.html
- AWS CloudTrail Product page: https://aws.amazon.com/cloudtrail/
- AWS Config Product page: https://aws.amazon.com/config/
- AWS Trusted Advisor page: https://aws.amazon.com/premiumsupport/trustedadvisor/
- Self-paced Auditing qwikLAB: https://www.qwiklab.com/focuses/preview/1250?locale=en
- In-person Auditor Training: awsauditttraining@amazon.com

Customers should consider updating the following documents to support their use of AWS Products in GxP Systems:

- IT audit schedule
- AWS account audit procedures and checklists
- AWS account audit reports
- IT auditor qualifications, CV, training records for AWS Products

3.1.4 Purchasing Controls

Traditional IT infrastructure product purchasing involves a purchase order (PO) process for physical goods that are booked as a capital expense. With AWS Products, however, purchasing requires a metered utility-like billing process for subscription software products that are booked as a variable operating expense. Many life sciences organizations have GxP IT product purchasing procedures written for a PO process that

may not accommodate purchase of a subscription, pay-as-you-go product pricing model like AWS.

Infrastructure Purchasing Using Traditional POs

1. IT specifies server requirements
2. IT sources matching server and OS
3. IT submit request to Purchasing
4. Purchasing submits PO to Supplier
5. Supplier ships server
6. Materials Dept. receives shipment
7. IT installs server and OS
8. IT configures OS
9. IT manually qualifies server and OS,
10. Account Dept pays for and depreciates hardware asset as a Capital Expense (CapEx)

Infrastructure Purchasing Process Using AWS

1. IT specifies server requirements
2. IT selects matching EC2 Instance Type and brings-their-own qualified OS image,
3. IT launches EC2 instance with qualified image and automatic logging enabled, and
4. IT pays for metered usage of EC2 using an operating expense (OpEx) credit card.

Customers using AWS Products in GxP Systems should review their IT purchasing procedures to ensure they can accommodate subscription pricing and an online delivery model. This review should involve the organization's IT, purchasing, and quality assurance teams, and should encompass ordering, receiving, and payments, as well as AWS account management. AWS provides documentation to assist organizations in understanding and managing their AWS account billing.

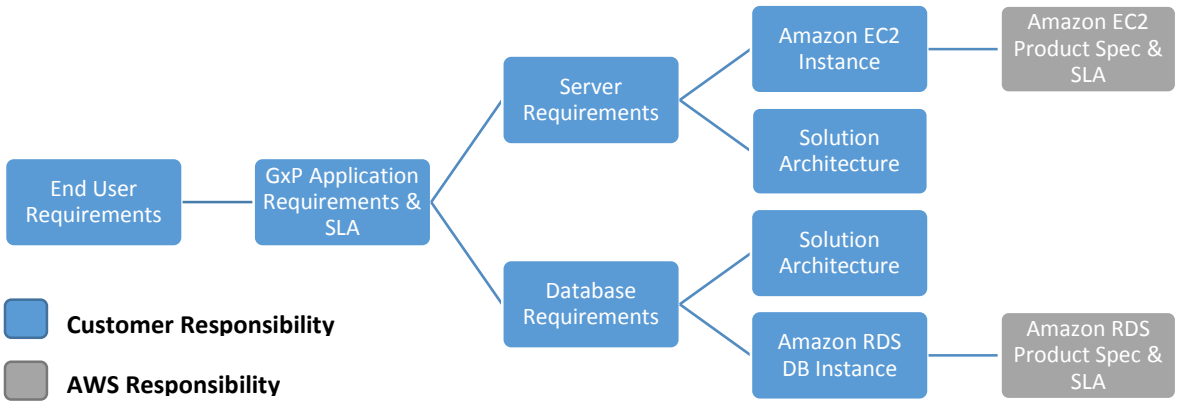
- AWS Billing and Cost Management Whitepaper: https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/awsaccountbilling-aboutv2.pdf
- Understanding Your Usage with Detailed Billing Reports: https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/detailed-billing-reports.html
- AWS Simply Monthly Billing Calculator http://calculator.s3.amazonaws.com/index.html
- Customers should consider updating the following documents to support their use of AWS Products:

Customers should consider updating the following documents to support their use of AWS Products in GxP Systems:

- Purchasing procedures
- AWS detailed billing reports
- PDF invoice by email

3.1.5 Product Assessment

Ensuring that purchased goods and services conform to specified requirements is a key requirement of GxP controls. In the case of commercially available infrastructure components like AWS Products, ensuring that product specifications match user requirements is straight-forward because all AWS Product interface specifications and agreements are fully documented and available for customer review. Since AWS does not customize AWS Products or SLAs for individual customers, customers can simply map their GxP application requirements to the corresponding AWS Products specifications and SLAs. For example, a customer wanting to run a COTS configurable software application using AWS's Amazon EC2 Product and Amazon RDS Product should first document the application's server requirements (CPU, memory, etc) and database requirements, and then go to the Amazon EC2 and Amazon RDS product pages to identify the virtual server family (i.e. EC2 instance type) and database type (i.e DB instance type) that will meet the application requirements.



It's important to note that the GxP System SLA are not a direct function of the individual AWS Product SLAs; rather, the GxP system SLA is a function of the customer's configuration and use of AWS Products (i.e. their solution architecture). For example, if a GxP application needs a higher level of availability than provided by the individual AWS Product(s), the customer can architect their solution to achieve that higher level of availability. Therefore, when assessing the suitability of AWS Products for a particular GxP System, the overall solution architecture must be taken into account.

When evaluating AWS Products for custom (GAMP category 5) applications or medical devices, then the product assessment will require GxP customers to simultaneously explore the system context, potential architectures and design, and available AWS Products during their SDLC planning phase. In order to support both existing and prospective customers in assessing whether AWS Products meet their application requirements, AWS publishes technical product documentation online and provides

customers with the ability to try AWS Products before approving their GxP system design.

- AWS Product Documentation: https://aws.amazon.com/documentation/

Customers should consider updating the following documents to support their use of AWS Products in GxP Systems:

- SDLC Procedure(s)
- GxP System Requirements & Risk Assessment
- GxP System Solution Architecture
- AWS Product Assessment

3.1.6 Supplier Evaluation

Organizations with GxP requirements need to evaluate and select their potential suppliers, contractors, and consultants on the basis of their ability to meet specified requirements. Once a customer has performed a product assessment and determined that AWS Products can meet the requirements of their GxP system architecture, a supplier evaluation can be performed to establish that AWS can reliably deliver the AWS Products according to their published interface specifications and SLAs.

AWS operates an industry-leading management control framework that conforms to current quality, security, and trust standards for commercial IT organizations. Compliance assessments of AWS controls are conducted on a recurring basis by qualified third-party auditors, and compliance reports from these assessments are made available to customers to enable them to evaluate AWS as a supplier. The AWS Compliance Reports identify the scope of AWS products and regions assessed, as well the assessor's attestation of conformance.

Controls	Assessment Criteria	Auditor	Compliance Report
ISO 27001	ISO/IEC 17021 & 27006	EY CertifyPoint	https://aws.amazon.com/compliance/iso-27001-faqs/
ISO 27017	ISO/IEC 17021 & 27006	EY CertifyPoint	https://aws.amazon.com/compliance/iso-27017-faqs/
ISO 9001	ISO/IEC 17021	EY CertifyPoint	https://aws.amazon.com/compliance/iso-9001-faqs/
SOC 1 SOC 2	AT 801 &	EY	https://aws.amazon.com/compliance/soc-faqs/

Controls	Assessment Criteria	Auditor	Compliance Report
SOC 3	AT 101 Controls , TSP Sec. 100 Trust & Attestation		
FedRAMP/NIST 800-53r4	NIST 800-53a	Veris Group	https://www.fedramp.gov/marketplace/compliant-systems/amazon-web-services-aws-eastwest-us-public-cloud/
PCI-DSS v3.1 Level 1	PCI DSS Security Audit Procedure	Coalfire	https://aws.amazon.com/compliance/pci-dss-level-1-faqs/

Additional online resources are available to provide customers transparency about AWS security processes and the current and past performance history of AWS Products:

- AWS Risk and Compliance Whitepaper, Appendix A: CSA Questionnaire https://do.awsstatic.com/whitepapers/compliance/AWS_Risk_and_Compliance_Whitepaper.pdf
- Overview of AWS Security Processes Whitepaper https://do.awsstatic.com/whitepapers/aws-security-whitepaper.pdf
- AWS Service Health Dashboard and Status History http://status.aws.amazon.com/

GxP Customers should consider updating their supplier evaluation procedures to ensure that any supplier categories can accommodate AWS Products. For GxP Customers who have a prior experience using AWS Products in their non-GxP systems, their GxP supplier evaluation of AWS should also include a performance history review of those non-GxP systems including any system-related issues that were attributable to AWS *and* were not addressable by the customer through their solution architecture.

Customers should consider updating the following documents to support their use of AWS Products in GxP Systems:

- GxP Supplier Classification & Evaluation Procedure
- Non-GxP System Performance Review
- AWS Supplier Evaluation Data, including Supplier Questionnaires
- AWS Supplier Approval Report
- AWS Compliance Reports and Whitepapers
- See also Supplier Agreements (page 17)

3.1.7 Supplier Agreement

Agreements with IT suppliers are important for organizations with GxP systems. This includes documented, clear statements of shared responsibilities and commitments from the IT supplier to notify the organization of material changes to the supplier's product. Since AWS Products are standardized and identical for every customer, AWS Product agreements are also standardized and include definitions of both AWS and customer obligations, as well as notification mechanisms for changes to AWS Products.

AWS agreements are listed below and appendix (page 34) includes a table of some GxP-relevant responsibilities found in these AWS agreements.

- Customer Agreement https://aws.amazon.com/agreement/
- Enterprise Agreement contact AWS sales
- Security Addendum contact AWS sales
- Customer Support https://aws.amazon.com/premiumsupport/
- Service Terms https://aws.amazon.com/service-terms/
- Acceptable Use Policy https://aws.amazon.com/aup/
- Product-specific Service Level Agreements (SLAs):

Amazon S3	https://aws.amazon.com/s3/sla/
Amazon EC2 and EBS	https://aws.amazon.com/ec2/sla/
Amazon RDS	https://aws.amazon.com/rds/sla/
Route53	https://aws.amazon.com/route53/sla/
CloudFront	https://aws.amazon.com/cloudfront/sla/

- Data Processing Addendum
  https://aws.amazon.com/compliance/eu-data-protection/

Customers using AWS Products in GxP systems should carefully consider the level of support they require from AWS. There are four tiers of AWS support, Basic, Developer, Business and Enterprise, each with a differing level of case severity rankings and response times. Depending on the customer's support scenarios, such as troubleshooting a system-related issue in the event of a for-cause regulatory inspection (see page 28), the AWS support tier will determine the response times for the customer's request. Many of AWS's current GxP customers maintain Business- or Enterprise-level support to accommodate these scenarios.

Customers should review and, if necessary, update their IT supplier agreement policies to ensure they are compatible with AWS's standardized operating and agreement model. This is particularly needed for organizations with a prior history of using managed service providers, niche GxP services, and co-location providers in which the suppliers customize their services and performed application development, validation, and maintenance activities on their customer's behalf.

Customers should consider updating the following documents to support their use of AWS Products in GxP Systems:

- IT supplier agreement policy
- Applicable agreements listed above

3.1.8 Records & Logs

For each GxP system, life sciences organizations are required to identify the retainable records and logs needed as GxP evidence and to maintain the integrity and availability of the records throughout their retention period. When using AWS Products in GxP Systems, the retainable records primarily consist of the customer data within their GxP System, the GxP system software code and SDLC records, and the system-generated logs and audit trails available within the customer's AWS account. Due to the high levels of automation achievable with AWS Products and modern SDLC methodologies, many of the retainable records that were once created through manual processes, such as paper-based installation protocols, are now generated through programmatically executed commands. This more reliable way to generate records reduces variability and demonstrably improves data integrity, both from a GxP data perspective and from the perspective of the SDLC.

Since the record types and formats associated with automated IT processes are quite different from manually-generated records, GxP customers should make sure to identify the record types and formats they need to retain and to develop their recordkeeping guidelines appropriately. AWS Products used in GxP medical devices and applications should also be evaluated for recordkeeping impact to the Design History File (DHF) and Device Master Record (DMR). In many cases, records that are programmatically generated by AWS Products, such as audit trails and alarms, are fully portable and retainable either within the customer's AWS account or by transmitting the record for retention to an alternate location.

Customers should consider updating the following documents to support their use of AWS Products in GxP Systems:

- Record Retention Schedule
- Record Type and Format Guidelines
- Recordkeeping Procedures
- CloudTrail logs
- CloudWatch alarms
- S3 and Glacier retention policies and life cycle rules
- AWS support case histories

3.2 System Development Life Cycle

In addition to quality system requirements for the organization, each GxP system must have certain features and a controlled SDLC process for delivering them. The specific features and SDLC controls that apply to each system depend on a variety of factors and are derived from regulations like 21 CFR Parts 11 and 820 in the US, Annex 11 and 93/42/EEC in the EU, and their international equivalents. The overall intent of these regulatory regimes is to ensure that the GxP system fulfills its intended use and that the data is trustworthy and reliable, as it may be used in the delivery of medical care or to make decisions about the safety and efficacy of medicinal products such as human foods, drugs, and medical devices, as well as animal food and drugs.

SDLC Controls for GxP Systems:

- Control the design and development to ensure specified requirements are met
- Validate software applications and qualify infrastructure to ensure accuracy, reliability, and consistent intended performance
- Change control and change history for systems operating in production environment, including system user documentation
- Monitoring system in the production environment to detect and respond to nonconformance (i.e. errors)
- Document and process system-related complaints and user support cases
- Preservation of SDLC records and GxP data throughout the system lifecycle, including deprecation

Features Needed in GxP Systems:

- Ability to generate accurate and complete copies of GxP data in human- and machine-readable form
- Data input validation and data integrity checks
- User access controls and authorization checks for user actions
- Secure, computer-generated, time-stamped audit trails of user actions and changes to data
- Checks to enforce permitted sequencing of steps (i.e. workflow enforcement)
- Encryption of data in transit and at rest
- Electronic signature manifests for user-authorized actions to data
- Linking between electronic signature and the associated data

Meeting these requirements with the traditional IT infrastructure model is cumbersome because the software-based application SDLC and hardware-based infrastructure SDLC are quite different and the nature of physical infrastructure components made by various manufacturers requires a number of manual, procedural controls to ensure configurations are maintained and changes are traceable across the infrastructure. With AWS Products, companies replace their physical infrastructure products with a harmonized suite of virtualized infrastructure products, allowing them to create and manage their entire infrastructure as software code. Not only can customers use AWS Products like Amazon EC2 to launch identical virtual servers from version-controlled images, their entire infrastructure including storage, database, and networking can be developed, version-controlled and deployed using software-based configuration templates. This infrastructure-as-code approach delivers an unprecedented level of

control, uniformity, and automation across the SDLC for the entire system, including application and infrastructure. It also means that synchronizing Dev, Test and Production environments requires much less effort than the traditional models of IT.

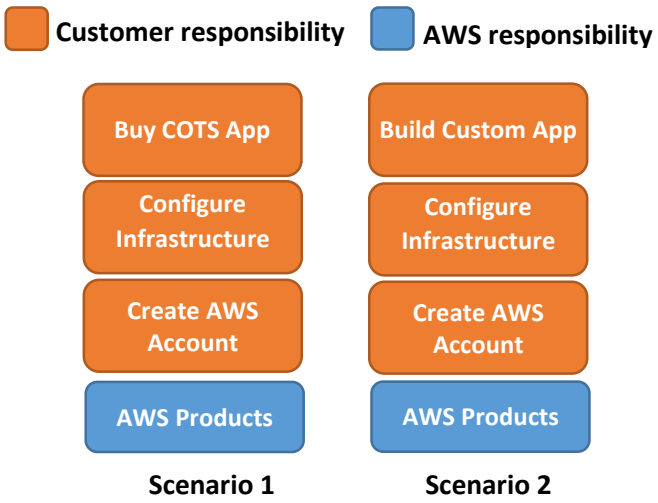
Although AWS Products are generally associated with SDLC methodologies like DevOps, SDLCs like Waterfall and V-model are fully supported. This section will use a generalized three-phase SDLC example to explain some of the considerations for customers using AWS Products in GxP Systems.

3.2.1 Develop

GxP systems need to be developed following documented procedures that ensure the systems meets its specified requirements. Customers using AWS Products in GxP systems are fully responsible for all GxP system development activities including, planning, coding, building, configuring, testing, validating and deploying their applications, as well as architecting, provisioning, configuring, orchestrating, deploying, qualifying and operating their software-defined infrastructure. AWS does not design or develop GxP systems on behalf of customers, however, AWS Products have extensive user documentation and whitepapers that GxP system engineers can use as inputs into their system design and development activities.

The design input requirements for GxP systems should also include cybersecurity requirements, and AWS recommends that customers develop a GxP system security plan following a recognized security planning standard such as NIST Special Publication 800-13 and any applicable regulatory guidance documents such as Content of Premarket Submissions for Management of Cybersecurity in Medical Devices from the FDA.

Although customers can make many types of systems using AWS Products, there are two basic development scenarios: 1) buying a COTS application or 2) building a custom application.



When evaluating COTS software packages for use with AWS Products, GxP Customers should include the AWS Partner Network (APN) Technology Partners and the AWS Marketplace in their evaluation. AWS Technology Partners offer software solutions that are either hosted on, or integrated with the AWS platform and the AWS Marketplace is an online store where customers can purchase and deploy AWS-compatible software directly into their AWS account.

- APN Technology Partners https://aws.amazon.com/partners/technology/
- The AWS Marketplace https://aws.amazon.com/marketplace/

AWS Products may also be used with commercial software applications from outside the APN Network or AWS Marketplace, however, customers need to review the application licensing agreements and perform a Product Assessment (see page 14 above) to determine the application's compatibility with AWS Products. APN Consulting Partners are available to assist with this activity as well, https://aws.amazon.com/partners/consulting/.

Although life sciences organizations have generally preferred to buy their software applications rather than build them, a major benefit of combining AWS Products with modern SDLC methodologies is the ability to deliver custom software solutions rapidly, repeatedly, and reliably. Many of the historic reasons that discouraged organizations from building their software, like building software packages manually from source code or manually conducting regression tests, are gone now that fully automated tools have reduced or eliminated the delays and errors cause by manual development activities. AWS Products like AWS OpsWorks, AWS CodeCommit, and AWS CodePipeline are providing system engineers with flexible, configurable tools that help them meet their unique organizational requirements, while also streamlining the implementation of SDLC controls for their software development activities.

Once a customer has developed and is ready to deploy their GxP system to a validation, production or other environment, AWS Products like Amazon Machine Images (AMI), AWS CloudFormation, AWS CodeDeploy, and AWS Elastic Beanstalk make consistent and controlled deployment easy and repeatable. These tools also enable the ability to create version controlled copies of the entire system environment from the network stack to the database and storage volumes to the compute instances. These version controlled copies can be retained for archiving and change management or for provisioning new Dev/Test environments for continued development or troubleshooting.

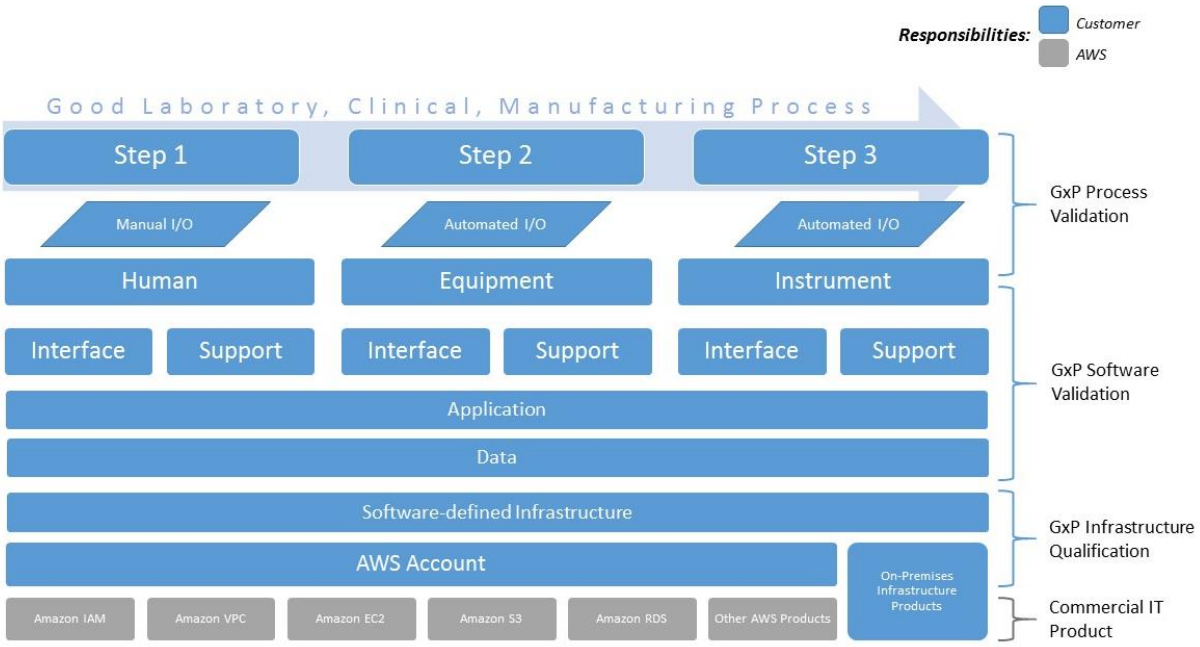
This new model of continuous development and continuous deployment is one of the main reasons why so many customers in so many industries are innovating their business using AWS Products. In order to leverage these benefits in their GxP systems, customers may need to review and update their development methodologies and procedures.

Customers should consider the following documentation to support their use of AWS Products in GxP Systems:

- SDLC Procedure
- System Design and Development Plan
- Hazards Assessment Procedure
- Code Inspection SOP
- Use cases and user stories or other requirements specification
- End user SLA criteria, including end user support
- Software Architecture Specifications
- Application functional requirements
- Preliminary Risk (or Hazards) Analysis for GxP medical and mobile applications
- AWS CloudTrail and Config logs
- Application Source Code
- EC2 AMIs and CloudFormation Templates
- Code Deployment SOP

3.2.2 Validate

GxP applications need to be validated to ensure that software specifications conform to user needs requirements, and the software infrastructure that GxP application runs on needs to be qualified to ensure that it meets the system requirements for the application. Since AWS Products are provided on an entirely self-service basis, customers using AWS Products in GxP systems are fully responsible for all software validation and infrastructure qualification activities within their AWS account. Since AWS does not develop or manage applications on behalf of customers, nor does AWS provision or configure customer-specific infrastructure, AWS cannot perform GxP validation or qualification activities on behalf of customers. AWS is responsible for ensuring AWS Products conform to AWS product specifications, SLAs and commercial IT standards, and GxP customers are responsible for validating the GxP systems they build with AWS Products.



The installation, instantiation, and deployment of applications and infrastructure are fundamentally different with AWS Products than with traditional physical infrastructure and installation media. In the era of physical infrastructure hardware, installation activities were highly manual and protocol-driven. Protocols were typically developed and pre-approved individually for each system component and then manually executed by an operator while a verifier stood by to ensure each step was completed correctly. Once completed, the protocol would be review and approved by a quality representative. As IT SDLCs matured and server virtualization popularized, validation activities shifted from protocol- to procedure-driven activities, although the activities were still highly manual. Some organizations would create a qualified "gold image" using a protocol and then subsequently use of the qualified image to create a virtual server following a procedure.

In the cloud era where infrastructure is software-defined, GxP system engineers have the ability to version control the entire system stack and automate deployment using

version-controlled infrastructure templates. One of the common practices among AWS customers is creating qualified system templates and using them in combination with automated deployment tools to provision individual resources, as well as entire development, test and validation environments. The web service API technology that's built into every AWS Product also allows third-party API verification tools like RunScope and SoapUI to be leveraged as a way to qualify and validate expected system behavior much more frequently than previously achievable with manual, periodic validation.

Because of this paradigm shift from point-in-time manual activities to continuous automatic activities, the GxP change control and validation practices that many life sciences organizations follow for their traditional hardware infrastructure should be reviewed and updated to address the automated infrastructure model when using AWS's commercial cloud products as components of GxP systems.

Customers should consider the following documentation to support their use of AWS Products in GxP Systems:

- SDLC Procedure
- Validation Procedure
- IT Qualification Procedure
- Automated Deployment Procedure
- AWS CloudTrail and Config logs
- Application Source Code
- EC2 AMIs and CloudFormation Templates

3.2.3 Operate

Developing, conducting, controlling and monitoring GxP systems in production operations is important to ensure that they continue to conform to specifications. When end user issues or system deviations occur, organizations with GxP systems also need to maintain a process for responding, correcting and preventing those issues. Although AWS Products can be leveraged for these activities, AWS does not perform GxP systems operations and monitoring activities of GxP systems on behalf of customers.

GxP System Principle	Summary of Requirement	Considerations
Change Control	Changes to GxP systems in production should be verified or validated to ensure the system meets the defined user requirements.	Customer: It is the customer who defines their system user requirements and configures and qualifies AWS products to meet those requirements. Customers are responsible for verifying and validating the changes they implement to user requirements and product configurations.

GxP System Principle	Summary of Requirement	Considerations
		AWS: AWS has no control over the customer requirements or product configurations. Accordingly, AWS cannot verify or validate GxP system changes on behalf of customers. AWS does verify changes to AWS Products to ensure product specifications and SLAs are satisfied.
Service level agreement	Formal agreements must exist between GxP system users and any third parties, including IT departments, who maintain the GxP system.	Customer: The customer defines the service level agreement of the GXP system and must configure and use AWS products to meet the SLA. AWS: AWS Product SLAs are distinct from GxP system SLAs and AWS has no control or insight over the SLAs the customer establishes for the system. See Appendix 4.3, Shared Responsibilities in AWS Agreements
End User Support	GxP system owners should establish procedures for providing support to end users.	Customer: Customers are responsible for providing support to GxP system end users. AWS: AWS does not provide any support or services to GxP system end users.
Backup and Recovery	Regular backups of GxP data should be done and should include verification of data integrity and restorability.	Customer: The customer is responsible for configuring and using AWS Products to maintain appropriate security, protection and backup of data. AWS: AWS has no control over customer configuration of products and AWS has no insight into the customer content (i.e. data). Consequently, AWS does not backup customer content on behalf of customers.
Incident response	GxP system incidents should be reported, assessed, and documented.	Customer: The customer is responsible for receiving incident reports from their end users and system administrators, as well as assessing and documenting these reports. If an incident requires AWS support, customer

GxP System Principle	Summary of Requirement	Considerations
		may file a support case using a method consistent with their support agreement. AWS: AWS does not have insight into GxP system incidents, however, customer support cases submitted to AWS that pertain to an issue with AWS Products will be assessed and investigated according to the customer's support level agreement. Customer support case histories are documented and available to customers online.
Corrective and preventive actions	GxP systems should have procedures for correcting and preventing system nonconformities.	Customer: The customer controls the identification and tracking of GxP system nonconformities and is responsible for implementing the needed corrective and preventive actions. AWS: AWS has no insight into the system operations and nonconformities and is unable to implement corrective and preventive actions for the system. AWS does maintain a continuous improvement program for AWS Products and this program is included in the scope of quality and security attestations.

Web service technology combined with modern automated deployment practices permits the increased speed and resilience of systems undergoing continuous development by allowing individual system components to be updated with minimal, often no, downtime of the system or breaking of dependencies. As long as the API interface specification has not changed, the customer may interact with the system and trust (but verify) that features in use will be available. Customers using AWS Products benefit from aspects of web service APIs, although customers still must architect their systems for resilience against API outages. API-based systems can also be integrated with change control systems such as Remedy, ServiceNow, Sparta Systems and other change management tracking systems, providing for full integration of the software development and deployment pipeline with GxP quality signoffs

In order for GxP customers to achieve these operational benefits, they should review and, if needed, update their operations documents and records to align them with AWS Products.

Customers should consider the following documentation to support their use of AWS Products in GxP Systems:

- Change Control Procedure
- Configuration Management Procedure
- Release to Production Procedure
- Monitoring Procedures
- AWS CloudTrail and Config logs
- Application Source Code
- EC2 AMIs and CloudFormation Templates
- Customer Support Case Histories

3.3 Regulatory Affairs

Within GxP-regulated industries, regulatory affairs professionals use data from GxP systems to submit filings and registration documents to regulatory health authorities and ethics committees. They also develop and maintain procedures for hosting regulatory agency inspections and keep track of the ever-changing legislation in the regions in which their organization seeks to distribute its GxP products. When a GxP Customer uses AWS Products in their GxP Systems, their IT, quality, and regulatory affairs team should discuss what, if any, impact there maybe to their regulatory practices, including

- Regulatory submissions and
- Healthy authority inspections, as well as any
- Review board and ethics committee requirements.

3.3.1 Submissions

Using GxP systems for regulatory submissions is not new and there are already cloud-based software applications for generating, tracking, and sending regulatory submissions. In fact, FDA uses AWS Products to publish data from regulatory submissions using the openFDA.gov platform. What's new and requires consideration by GxP customers is whether or not their GxP System should be included in the content of regulatory submission and, if so, how the customer's regulatory team will address the use of AWS Products.

For example, a medical device software application, such as a Picture Archiving and Communication System (PACS), may require a 510k submission for FDA clearance. If the PACS is architected to run on a common x86 server that's compatible with AWS's Amazon EC2 Product, the PACS' 510k may not specifically mention AWS Products but simply state, "The software application is a PACS used with general purpose computing servers."

The decision to include AWS Products in regulatory submissions is the responsibility of GxP customers and AWS advises GxP customers to seek the advice of a qualified regulatory affairs professional if there are any submission-related questions.

3.3.2 Inspections

Health authorities may inspect life sciences organizations and their GxP systems at any time. Although COTS IT products have a long history of use in GxP Systems that have undergone agency inspections, the use of COTS cloud product providers like AWS in GxP systems is relatively new and agency field inspection staff may not be familiar with AWS Products or their usage. In order to ensure a successful inspection outcome for GxP systems that use AWS Products, AWS recommends that GxP customers establish and maintain an inspection readiness plan that includes several elements:

- Identification of the key individuals within the customer's organization who are familiar with the configuration and use of AWS Products in the GxP system,
- Procedures to ensure those key individuals are notified and available in the event of an FDA inspection, and
- A general overview presentation for each GxP system to quickly and accurately convey the key system elements to the FDA or Health Authority inspector. Customers should consider including the following elements in their presentation materials:
    - System Identification including system name, version (if applicable), and system classification
    - System Description including a high-level overview of the key GxP activities and or job roles that rely on the system; interfaces with other systems should also be identified
    - Network or Architecture Diagram including any related responsibilities
    - System Operations including physical locations where the system is accessed, number of end users, interfaces and products
    - List of Application SOPs including any business unit, technical or corporate procedures
    - Responsibility Summary including the names of the end user business unit(s), technical and administrative responsibility, security operations, etc.

In the event of a system-related investigation requiring product troubleshooting support from AWS, the AWS support tier the customer has selected with determine the channel for submitting support requests and AWS's expected response time.

Customers should consider the following documentation to support their use of AWS Products in GxP Systems:

- Inspection readiness plan
- GxP system overview presentation
- System documentation index

3.3.3 Personal Data Privacy Controls for Research Participants

GxP systems used in clinical research may also require personal data privacy controls to protect the confidentiality of individuals whose personally identifiable information (PII) and protected health information (PHI) are stored, processes or transmitted by the system. Examples may include:

- Research Recruiting tools,
- Electronic Data Capture (EC) Systems,
- Data Storage and Archiving,
- Diagnostic medical device applications, and
- Mobile medical device applications.

Sponsors and investigators conducting human research studies using GxP systems that involve AWS Products may be asked by Institutional Review Boards (IRB), Independent Ethics Committees (IEC), and/or Data Access Committees (DAC) to provide information about how the system secures personal information of study participants, including any system security reviews performed and security operations controls such as describing the procedures for revoking system access when it is no longer required. Customers who are using AWS Products in GxP systems that contain PII should make sure to understand the data locality requirements and, if necessary, describe the security and data locality controls implemented in the AWS Products the system is running on. Additional information on data locality controls in AWS Products is available online, https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html .

Customers should consider the following documentation to support their use of AWS Products in GxP Systems:

- Policy for PII protection
- Data locality control plan
- System security plan for GxP systems

4 CONCLUSION

Although AWS Product delivery is over the Internet rather than physical, GxP customers retain accountability and responsibility for their use of the products, including the applications and virtualized infrastructure they develop, validate and operate using AWS Products. Using the recommendations in this whitepaper, GxP companies can evaluate their quality systems, SDLC controls and regulatory affairs plans in order to demonstrate effective control of GxP systems that incorporate AWS Products as a component.

5 DOCUMENT REVISIONS

The table below shows the complete revision history of this whitepaper.

Date	Description
January 2016	Initial Release

6 APPENDICES

6.1 Data Privacy Resources

At AWS, data protection is always a top priority. While customers retain ownership and control of their data when using AWS products, AWS works hard to provide additional privacy assurances and transparency to customers. This appendix lists some of the key data privacy resources that AWS makes available to customers.

- AWS Data Privacy FAQ
  https://aws.amazon.com/compliance/data-privacy-faq/
- Amazon Corporate Bi-annual Information Request Report
  http://d0.awsstatic.com/certifications/Information_Request_Report.pdf
- AWS Third Party Access List
  http://aws.amazon.com/compliance/third-party-access/
- U.S.-EU SAFE HARBOR
  https://safeharbor.export.gov/companyinfo.aspx?id=27379
- EU Directive 95/46/EC FAQ and Model Clauses
  https://aws.amazon.com/compliance/eu-data-protection/
  http://www.cnpd.public.lu/en/actualites/international/2015/03/AWS/index.html
- US Database of Genotypes and Phenotypes
  https://d0.awsstatic.com/whitepapers/compliance/AWS_dBGaP_Genomics_on_AWS_Best_Practices.pdf
- US HIPAA Business Associate FAQ
  https://aws.amazon.com/compliance/hipaa-compliance/

6.2 Annotated 21 CFR Part 11

This appendix highlights some of the ways in which customers can use AWS Products to satisfy the electronic record and electronic signature requirements of 21 CFR Part 11 regulations.

- **Access Controls:** GxP systems and data access can be limited by customers to authorized individuals. Customers can use AWS Products such as Amazon Identity and Access Management (IAM) and AWS Directory Service to implement access controls. AWS customers can also configure their account access controls to work with existing, on-premises directories like Microsoft Active Directory to create a seamless access control environment for hybrid cloud deployments.
- **GxP System Validation:** Applications can be deployed and validated in AWS. Customers can validate their GxP systems according to their organizational policies and procedures.
- **Data Retrievability:** Accurate and complete copies of records can be generated and retrieved by AWS customers from their AWS account at any time throughout the record retention period. Because AWS customers retain root administrative access to their AWS account, systems and data, they can independently retrieve their data or audit trails at any time, so long as the customer enables the AWS audit trail products and features.
- **Audit Trails:** Secure, computer-generated, time-stamped audit trails can be generated, monitored, downloaded, and retained according to customer-defined policies. AWS products like AWS CloudTrail and Amazon CloudWatch allow customers to develop and operate logging systems to meet the highest levels of data and system auditing from the individual file object level on up to the application level.
- **Workflow Enforcement:** Operational system checks for GxP workflow activities are fully controlled by AWS customers, including the SDLC processes they maintain for the GxP system.
- **User Authorization:** Authority checks to ensure that only authorized individuals can use the system or take action on data can be implemented by AWS customers using infrastructure-level roles and permission groups within their AWS account and within their applications. Products like Amazon IAM allow customers to define the roles, security levels, and transactional policies they need for infrastructure user accounts as well as for machine-to-machine service accounts.
- **Input Output Verification:** Input checks and nonrepudiation controls are highly dependent on the people, processes, and technologies that create and update the GxP data. If GxP data is entered manually into a web or mobile application, AWS customers can employ a combination of manual processes to train and verify their users before they're granted access to the app. Once granted access, the application level controls can automatically enforce the required input checks. The AWS Products within the customer's account can be used to monitor and control the connectivity of networked resources such as workstations or mobile devices. If GxP data is generated automatically from local instruments, device sensors, or application computing processes, the queuing and transport of data from the customer's local environment to their AWS account can enabled and controlled using a variety of

AWS Products like Amazon Simple Queue Service (SQS) and Amazon Kinesis, as well as the identity and access management tools that enable user- and service-level access controls.

- **Personnel Training:** AWS customers develop, maintain, and use the GxP data and systems within their AWS account, which means they can follow their existing policies and procedures for determining whether their staff have the education, training and experience to perform their assigned GxP tasks. AWS offers extensive technical documentation and customer training programs to help customer IT engineering staff achieve their AWS learning goals, and the extensive AWS partner ecosystem includes third-party system integrators and consulting partners with competencies in healthcare and life sciences.
- **System Documentation:** Use of appropriate controls over systems documentation can be achieved by customers using their existing controlled document procedures and systems. AWS technical documentation can be referenced using the appropriate URL and any version specific information the customer requires. Additionally, since each customer's virtual infrastructure in AWS is by nature a software-defined infrastructure, customers can version control and archive the complete set of code and templates they use to define the AWS resources in their account (see Qualified Infrastructure).
- **Security Controls:** Additional measures such as encryption of data at-rest and in-transit can be implemented by customers using their existing client-side encryption solutions or AWS's extensive line of security products such Amazon Key Management Service (KMS) as well as server-side encryption, transparent data encryption (TDS), and Secure Socket Layer (SSL) features in products like Amazon Simple Storage Service (S3), Amazon Relational Database Service (RDS) and Amazon Elastic Load Balancer (ELB). Amazon Virtual Private Cloud (VPC) is a product that lets customers control their virtual networking environment and create encrypted Hardware Virtual Private Network (VPN) connections between their on-premises datacenter and their Amazon VPC so they can leverage the cloud as an extension of their existing networks.
- **Electronic Signatures:** Requirements for electronic signature manifestations, signature/record linking, and electronic signature components and controls are typically satisfied as part of the validated applications that customers use to generate and maintain their GxP data. Customers should evaluate the suitability of their existing electronic signature applications with the virtual network in their AWS account, or they can also address the electronic signature requirements as part of the custom, cloud-native applications they develop themselves. When AWS products are used to address requirements such as password controls, out-of-the-box features like Amazon IAM Password Policies can allow customers to create their own password complexity and aging policies according to their specific requirements.
- **Data Retention:** The procedures and policies for each customer's GxP data lifecycle and retention requirements are highly variable depending on the customer's organization and the particular requirements that apply to them. When designing and developing GxP data management solutions in their AWS account, customers should take care to specify their confidentiality, integrity and availability requirements, including any record retention policies for raw data, derived data, and metadata.

6.3 Shared Responsibilities in AWS Agreements

This table is meant as a helpful summary of responsibilities found in AWS standard agreements and is not authoritative. The responsibilities outline in this section are for the individual AWS Products only and do not include the SLA responsibilities between AWS customers and their end users.

Topic	Responsibilities	Customer	AWS
Contacts	Maintain valid e-mail address associated with AWS account (customer agreement 1.2)	x	
Changes	Notify customers of material change or discontinuation of AWS Product (customer agreement 2.1)		x
Changes	Support previous versions of AWS Product APIs for 12 months (customer agreement 2.2)		x
Changes	Perform security updates as needed to ensure confidentiality, integrity and availability of AWS products https://aws.amazon.com/security/security-bulletins/		x
Content	Development, contents, operation, maintenance and use of Content (i.e. GxP records and applications) (customer agreement 4.1)	X	
Content	Security, protection, and backup of your content (customer agreement 4.2)	x	
Support	Provide support of GxP system end users (customer agreement 4.2)	x	
Support	Basic support to customer (https://aws.amazon.com/premiumsupport/)		x
Privacy	Control of geographic regions where data resides	x	