# AWS Certifications, Programs, Reports, and Third-Party Attestations

*March 2017*

We welcome your feedback. Please share your thoughts at this link.

# 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.

# Contents

# Abstract

AWS engages with external certifying bodies and independent auditors to provide customers with considerable information regarding the policies, processes, and controls established and operated by AWS.

# CJIS

AWS complies with the FBI's Criminal Justice Information Services (CJIS) standard. We sign CJIS security agreements with our customers, including allowing or performing any required employee background checks according to the CJIS Security Policy.

Law enforcement customers (and partners who manage CJI) are taking advantage of AWS services to improve the security and protection of CJI data, using the advanced security services and features of AWS, such as activity logging (AWS CloudTrail), encryption of data in motion and at rest (S3's Server-Side Encryption with the option to bring your own key), comprehensive key management and protection (AWS Key Management Service and CloudHSM), and integrated permission management (IAM federated identity management, multi-factor authentication).

AWS has created a Criminal Justice Information Services (CJIS) Workbook in a security plan template format aligned to the CJIS Policy Areas. Additionally, a CJIS Whitepaper has been developed to help guide customers in their journey to cloud adoption.

Visit the CJIS Hub Page at https://aws.amazon.com/compliance/cjis/.

# CSA

In 2011, the Cloud Security Alliance (CSA) launched STAR, an initiative to encourage transparency of security practices within cloud providers. The CSA Security, Trust & Assurance Registry (STAR) is a free, publicly accessible registry that documents the security controls provided by various cloud computing offerings, thereby helping users assess the security of cloud providers they currently use or are considering contracting with. AWS is a CSA STAR registrant and has completed the Cloud Security Alliance (CSA) Consensus Assessments Initiative Questionnaire (CAIQ). This CAIQ published by the CSA provides a way to reference and document what security controls exist in AWS' Infrastructure as a Service offerings. The CAIQ provides 298 questions a cloud consumer and cloud auditor may wish to ask of a cloud provider.

See CSA Consensus Assessments Initiative Questionnaire.

# Cyber Essentials Plus

Cyber Essentials Plus is a UK Government-backed, industry-supported certification scheme introduced in the UK to help organizations demonstrate operational security against common cyber-attacks.

It demonstrates the baseline controls AWS implements to mitigate the risk from common Internet-based threats, within the context of the UK Government's "10 Steps to Cyber Security". It is backed by industry, including the Federation of Small Businesses, the Confederation of British Industry and a number of insurance organizations that offer incentives for businesses holding this certification.

Cyber Essentials sets out the necessary technical controls; the related assurance framework shows how the independent assurance process works for Cyber Essentials Plus certification through an annual external assessment conducted by an accredited assessor. Due to the regional nature of the certification, the certification scope is limited to EU (Ireland) region.

# DoD SRG Levels 2 and 4

The Department of Defense (DoD) Cloud Security Model (SRG) provides a formalized assessment and authorization process for cloud service providers (CSPs) to gain a DoD Provisional Authorization, which can subsequently be leveraged by DoD customers. A Provisional Authorization under the SRG provides a reusable certification that attests to our compliance with DoD standards, reducing the time necessary for a DoD mission owner to assess and authorize one of their systems for operation on AWS. AWS currently holds provisional authorizations at Levels 2 and 4 of the SRG.

Additional information of the security control baselines defined for Levels 2, 4, 5, and 6 can be found at http://iase.disa.mil/cloud_security/Pages/index.aspx.

Visit the DoD Hub Page at https://aws.amazon.com/compliance/dod/.

# FedRAMPsm

AWS is a Federal Risk and Authorization Management Program (FedRAMPsm) Compliant Cloud Service Provider. AWS has completed the testing performed by a FedRAMPsm accredited Third-Party Assessment Organization (3PAO) and has been granted two Agency Authority to Operate (ATOs) by the US Department of Health and Human Services (HHS) after demonstrating compliance with FedRAMPsm requirements at the Moderate impact level. All U.S. government agencies can leverage the AWS Agency ATO packages stored in the FedRAMPsm repository to evaluate AWS for their applications and workloads, provide authorizations to use AWS, and transition workloads into the AWS environment. The two FedRAMPsm Agency ATOs encompass all U.S. regions (the AWS GovCloud (US) region and the AWS US East/West regions).

For a complete list of the services that are in the accreditation boundary for the regions stated above, see the AWS Services in Scope by Compliance Program page (https://aws.amazon.com/compliance/services-in-scope/).

For more information on AWS FedRAMPsm compliance please see the AWS FedRAMPsm FAQs at https://aws.amazon.com/compliance/fedramp/.

# FERPA

The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when he or she reaches the age of 18, or attends a school beyond the high school level. Students to whom the rights have transferred are "eligible students."

AWS enables covered entities and their business associates subject to FERPA to leverage the secure AWS environment to process, maintain, and store protected education information.

AWS also offers a FERPA-focused whitepaper for customers interested in learning more about how they can leverage AWS for the processing and storage of educational data.

The FERPA Compliance on AWS whitepaper outlines how companies can use AWS to process systems that facilitate FERPA compliance:

# FIPS 140-2

The Federal Information Processing Standard (FIPS) Publication 140-2 is a US government security standard that specifies the security requirements for cryptographic modules protecting sensitive information. To support customers with FIPS 140-2 requirements, SSL terminations in AWS GovCloud (US) operate using FIPS 140-2 validated hardware. AWS works with AWS GovCloud (US) customers to provide the information they need to help manage compliance when using the AWS GovCloud (US) environment.

# FISMA and DIACAP

AWS enables US government agencies to achieve and sustain compliance with the Federal Information Security Management Act (FISMA). The AWS infrastructure has been evaluated by independent assessors for a variety of government systems as part of their system owners' approval process. Numerous Federal Civilian and Department of Defense (DoD) organizations have successfully achieved security authorizations for systems hosted on AWS in accordance with the Risk Management Framework (RMF) process defined in NIST 800-37 and DoD Information Assurance Certification and Accreditation Process (DIACAP).

# GxP

GxP is an acronym that refers to the regulations and guidelines applicable to life sciences organizations that make food and medical products such as drugs, medical devices, and medical software applications. The overall intent of GxP requirements is to ensure that food and medical products are safe for consumers and to ensure the integrity of data used to make product-related safety decisions.

AWS offers a GxP whitepaper, which details a comprehensive approach for using AWS for GxP systems. 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.

For more information on the GxP, on AWS please contact AWS Sales and Business Development.

For additional information please see our GxP Compliance FAQs at https://aws.amazon.com/compliance/gxp-part-11-annex-11/.

# HIPAA

AWS enables covered entities and their business associates subject to the U.S. Health Insurance Portability and Accountability Act (HIPAA) to leverage the secure AWS environment to process, maintain, and store protected health information and AWS will be signing business associate agreements with such customers. AWS also offers a HIPAA-focused whitepaper for customers interested in learning more about how they can leverage AWS for the processing and storage of health information. The Architecting for HIPAA Security and Compliance on Amazon Web Services whitepaper outlines how companies can use AWS to process systems that facilitate HIPAA and Health Information Technology for Economic and Clinical Health (HITECH) compliance.

Customers who execute an AWS BAA may use any AWS service in an account designated as a HIPAA Account, but they may only process, store and transmit PHI using the HIPAA-eligible services defined in the AWS BAA. For a complete list of these services, see the HIPAA Eligible Services Reference page (https://aws.amazon.com/compliance/hipaa-eligible-services-reference/).

AWS maintains a standards-based risk management program to ensure that the HIPAA-eligible services specifically support the administrative, technical, and physical safeguards required under HIPAA. Using these services to store, process, and transmit PHI allows our customers and AWS to address the HIPAA requirements applicable to the AWS utility-based operating model.

For additional information please see our HIPAA Compliance FAQs and Architecting for HIPAA Security and Compliance on Amazon Web Services.

# IRAP

The Information Security Registered Assessors Program (IRAP) enables Australian government customers to validate that appropriate controls are in place and determine the appropriate responsibility model for addressing the needs of the Australian Signals Directorate (ASD) Information Security Manual (ISM).

Amazon Web Services has completed an independent assessment that has determined all applicable ISM controls are in place relating to the processing, storage and transmission of Unclassified (DLM) for the AWS Sydney Region.

For more information, see the IRAP Compliance FAQs at https://aws.amazon.com/compliance/irap/ and AWS alignment with the Australian Signals Directorate (ASD) Cloud Computing Security Considerations.

# ISO 9001

AWS has achieved ISO 9001 certification, AWS' ISO 9001 certification directly supports customers who develop, migrate and operate their quality-controlled IT systems in the AWS cloud. Customers can leverage AWS' compliance reports as evidence for their own ISO 9001 programs and industry-specific quality programs, such as GxP in life sciences, ISO 13485 in medical devices, AS9100 in aerospace, and ISO/TS 16949 in automotive. AWS customers who don't have quality system requirements will still benefit from the additional assurance and transparency that an ISO 9001 certification provides.

The ISO 9001 certification covers the quality management system over a specified scope of AWS services and Regions of operations. For a complete list of services, see the AWS Services in Scope by Compliance Program page (https://aws.amazon.com/compliance/services-in-scope/).

ISO 9001:2008 is a global standard for managing the quality of products and services. The 9001 standard outlines a quality management system based on eight principles defined by the International Organization for Standardization (ISO) Technical Committee for Quality Management and Quality Assurance. They include:

- Customer focus

- Leadership
- Involvement of people
- Process approach
- System approach to management
- Continual Improvement
- Factual approach to decision-making
- Mutually beneficial supplier relationships

The AWS ISO 9001 certification can be downloaded at https://d0.awsstatic.com/certifications/iso_9001_certification.pdf.

AWS provides additional information and frequently asked questions about its ISO 9001 certification at: https://aws.amazon.com/compliance/iso-9001-faqs/.

# ISO 27001

AWS has achieved ISO 27001 certification of our Information Security Management System (ISMS) covering AWS infrastructure, data centers, and services. For a complete list of services, see the AWS Services in Scope by Compliance Program page (https://aws.amazon.com/compliance/services-in-scope/).

ISO 27001/27002 is a widely-adopted global security standard that sets out requirements and best practices for a systematic approach to managing company and customer information that's based on periodic risk assessments appropriate to ever-changing threat scenarios. In order to achieve the certification, a company must show it has a systematic and ongoing approach to managing information security risks that affect the confidentiality, integrity, and availability of company and customer information. This certification reinforces Amazon's commitment to providing significant information regarding our security controls and practices.

The AWS ISO 27001 certification can be downloaded at https://d0.awsstatic.com/certifications/iso_27001_global_certification.pdf.

AWS provides additional information and frequently asked questions about its ISO 27001 certification at: https://aws.amazon.com/compliance/iso-27001-faqs/.

# ISO 27017

ISO 27017 is the newest code of practice released by the International Organization for Standardization (ISO). It provides implementation guidance on information security controls that specifically relate to cloud services.

AWS has achieved ISO 27017 certification of our Information Security Management System (ISMS) covering AWS infrastructure, data centers, and services. For a complete list of services, see the AWS Services in Scope by Compliance Program page (https://aws.amazon.com/compliance/services-in-scope/).

The AWS ISO 27017 certification can be downloaded at https://d0.awsstatic.com/certifications/iso_27017_certification.pdf.

AWS provides additional information and frequently asked questions about its ISO 27017 certification at https://aws.amazon.com/compliance/iso-27017-faqs/.

# ISO 27018

ISO 27018 is the first International code of practice that focuses on protection of personal data in the cloud. It is based on ISO information security standard 27002 and provides implementation guidance on ISO 27002 controls applicable to public cloud Personally Identifiable Information (PII). It also provides a set of additional controls and associated guidance intended to address public cloud PII protection requirements not addressed by the existing ISO 27002 control set.

AWS has achieved ISO 27018 certification of our Information Security Management System (ISMS) covering AWS infrastructure, data centers, and services. For a complete list of services, see the AWS Services in Scope by Compliance Program page (https://aws.amazon.com/compliance/services-in-scope/).

The AWS ISO 27018 certification can be downloaded at https://d0.awsstatic.com/certifications/iso_27018_certification.pdf.

AWS provides additional information and frequently asked questions about its ISO 27018 certification at https://aws.amazon.com/compliance/iso-27018-faqs/.

# ITAR

The AWS GovCloud (US) region supports US International Traffic in Arms Regulations (ITAR) compliance. As a part of managing a comprehensive ITAR compliance program, companies subject to ITAR export regulations must control unintended exports by restricting access to protected data to US Persons and restricting physical location of that data to the US. AWS GovCloud (US) provides an environment physically located in the US and where access by AWS Personnel is limited to US Persons, thereby allowing qualified companies to transmit, process, and store protected articles and data subject to ITAR restrictions. The AWS GovCloud (US) environment has been audited by an independent third-party to validate the proper controls are in place to support customer export compliance programs for this requirement.

# MPAA

The Motion Picture Association of America (MPAA) has established a set of best practices for securely storing, processing and delivering protected media and content (http://www.fightfilmtheft.org/facility-security-program.html). Media companies use these best practices as a way to assess risk and security of their content and infrastructure. AWS has demonstrated alignment with the MPAA best practices and the AWS infrastructure is compliant with all applicable MPAA infrastructure controls. While the MPAA does not offer a "certification," media industry customers can use the AWS MPAA documentation to augment their risk assessment and evaluation of MPAA-type content on AWS.

See the AWS Compliance MPAA hub page for additional details at https://aws.amazon.com/compliance/mpaa/.

# MTCS Tier 3 Certification

The Multi-Tier Cloud Security (MTCS) is an operational Singapore security management Standard (SPRING SS 584:2013), based on ISO 27001/02 Information Security Management System (ISMS) standards. The certification assessment requires us to:

- Systematically evaluate our information security risks, taking into account the impact of company threats and vulnerabilities
- Design and implement a comprehensive suite of information security controls and other forms of risk management to address company and architecture security risks
- Adopt an overarching management process to ensure that the information security controls meet the our information security needs on an ongoing basis

View the MTCS Hub Page at https://aws.amazon.com/compliance/aws-multitiered-cloud-security-standard-certification/.

# NIST

In June 2015 The National Institute of Standards and Technology (NIST) released guidelines 800-171, "Final Guidelines for Protecting Sensitive Government Information Held by Contractors". This guidance is applicable to the protection of Controlled Unclassified Information (CUI) on nonfederal systems.

AWS is already compliant with these guidelines, and customers can effectively comply with NIST 800-171 immediately. NIST 800-171 outlines a subset of the NIST 800-53 requirements, a guideline under which AWS has already been audited under the FedRAMP program. The FedRAMP Moderate security control baseline is more rigorous than the recommended requirements established in Chapter 3 of 800-171, and includes a significant number of security controls above and beyond those required of FISMA Moderate systems that protect CUI data. A detailed mapping is available in the NIST Special Publication 800-171, starting on page D2 (which is page 37 in the PDF).

# PCI DSS Level 1

AWS is Level 1 compliant under the Payment Card Industry (PCI) Data Security Standard (DSS). Customers can run applications on our PCI-compliant technology infrastructure for storing, processing, and transmitting credit card information in the cloud. In February 2013, the PCI Security Standards Council released PCI DSS Cloud Computing Guidelines. These guidelines provide customers who are managing a cardholder data environment with considerations for maintaining PCI DSS controls in the cloud. AWS has incorporated the PCI DSS Cloud Computing Guidelines into the AWS PCI Compliance Package for customers. The AWS PCI Compliance Package includes the AWS PCI Attestation of Compliance (AoC), which shows that AWS has been successfully validated against standards applicable to a Level 1 service provider under PCI DSS Version 3.1, and the AWS PCI Responsibility Summary, which explains how compliance responsibilities are shared between AWS and our customers in the cloud.

For a complete list of services in scope for PCI DSS Level 1, see the AWS Services in Scope by Compliance Program page (https://aws.amazon.com/compliance/services-in-scope/).

For more information, see https://aws.amazon.com/compliance/pci-dss-level-1-faqs/.

# SOC 1/ISAE 3402

Amazon Web Services publishes a Service Organization Controls 1 (SOC 1), Type II report. The audit for this report is conducted in accordance with American Institute of Certified Public Accountants (AICPA): AT 801 (formerly SSAE 16) and the International Standards for Assurance Engagements No. 3402 (ISAE 3402). This dual-standard report is intended to meet a broad range of financial auditing requirements for U.S. and international auditing bodies. The SOC 1 report audit attests that AWS' control objectives are appropriately designed and that the individual controls defined to safeguard customer data are operating effectively. This report is the replacement of the Statement on Auditing Standards No. 70 (SAS 70) Type II Audit report.

The AWS SOC 1 control objectives are provided here. The report itself identifies the control activities that support each of these objectives and the independent auditor's results of their testing procedures of each control.

| Objective Area | Objective Description |
|---|---|
| **Security Organization** | Controls provide reasonable assurance that information security policies have been implemented and communicated throughout the organization. |
| **Employee User Access** | Controls provide reasonable assurance that procedures have been established so that Amazon employee user accounts are added, modified and deleted in a timely manner and reviewed on a periodic basis. |
| **Logical Security** | Controls provide reasonable assurance that policies and mechanisms are in place to appropriately restrict unauthorized internal and external access to data and customer data is appropriately segregated from other customers. |
| **Secure Data Handling** | Controls provide reasonable assurance that data handling between the customer's point of initiation to an AWS storage location is secured and mapped accurately. |
| **Physical Security and Environmental Protection** | Controls provide reasonable assurance that physical access to data centers is restricted to authorized personnel and that mechanisms are in place to minimize the effect of a malfunction or physical disaster to data center facilities. |
| **Change Management** | Controls provide reasonable assurance that changes (including emergency / non-routine and configuration) to existing IT resources are logged, authorized, tested, approved and documented. |
| **Data Integrity, Availability and Redundancy** | Controls provide reasonable assurance that data integrity is maintained through all phases including transmission, storage and processing. |

| Objective Area | Objective Description |
|---|---|
| **Incident Handling** | Controls provide reasonable assurance that system incidents are recorded, analyzed, and resolved. |

The SOC 1 reports are designed to focus on controls at a service organization that are likely to be relevant to an audit of a user entity's financial statements. As AWS' customer base is broad, and the use of AWS services is equally as broad, the applicability of controls to customer financial statements varies by customer. Therefore, the AWS SOC 1 report is designed to cover specific key controls likely to be required during a financial audit, as well as covering a broad range of IT general controls to accommodate a wide range of usage and audit scenarios. This allows customers to leverage the AWS infrastructure to store and process critical data, including that which is integral to the financial reporting process. AWS periodically reassesses the selection of these controls to consider customer feedback and usage of this important audit report.

AWS' commitment to the SOC 1 report is ongoing, and AWS will continue the process of periodic audits. For the current scope of the SOC 1 report, see the AWS Services in Scope by Compliance Program page (https://aws.amazon.com/compliance/services-in-scope/).

# SOC 2

In addition to the SOC 1 report, AWS publishes a Service Organization Controls 2 (SOC 2), Type II report. Similar to the SOC 1 in the evaluation of controls, the SOC 2 report is an attestation report that expands the evaluation of controls to the criteria set forth by the American Institute of Certified Public Accountants (AICPA) Trust Services Principles. These principles define leading practice controls relevant to security, availability, processing integrity, confidentiality, and privacy applicable to service organizations such as AWS. The AWS SOC 2 is an evaluation of the design and operating effectiveness of controls that meet the criteria for the security and availability principles set forth in the AICPA's Trust Services Principles criteria. This report provides additional transparency into AWS security and availability based on a pre-defined industry standard of leading practices and further demonstrates AWS' commitment to protecting

customer data. The SOC 2 report scope covers the same services covered in the SOC 1 report. See the SOC 1 description above for the in-scope services.

# SOC 3

AWS publishes a Service Organization Controls 3 (SOC 3) report. The SOC 3 report is a publically-available summary of the AWS SOC 2 report. The report includes the external auditor's opinion of the operation of controls (based on the AICPA's Security Trust Principles included in the SOC 2 report), the assertion from AWS management regarding the effectiveness of controls, and an overview of AWS Infrastructure and Services. The AWS SOC 3 report includes all AWS data centers worldwide that support in-scope services. This is a great resource for customers to validate that AWS has obtained external auditor assurance without going through the process to request a SOC 2 report. The SOC 3 report scope covers the same services covered in the SOC 1 report. See the SOC 1 description above for the in-scope services. View the AWS SOC 3 report here.

# Further Reading

For additional information, see the following sources:

- AWS Risk and Compliance Overview
- AWS Answers to Key Compliance Questions
- CSA Consensus Assessments Initiative Questionnaire

# Document Revisions

| Date | Description |
|---|---|
| **March 2017** | Updated in scope services. |
| **January 2017** | Migrated to new template. |
| **January 2016** | First publication |