

AWS Customer Compliance Guides

June 2024



TERMS OF USE

Customers are responsible for making their own independent assessment of the information in this CCG. This CCG: (a) is provided for informational purposes only, (b) represents current AWS product offerings and practices at the time of publication, which are subject to change without notice, and (c) does not create any commitments or assurances from AWS and its affiliates, suppliers or licensors.

This CCG does not constitute legal or compliance advice. This CCG is provided “as is” and AWS disclaims all warranties, representations, or conditions of any kind, whether express, implied, statutory, or otherwise relating to this CCG. AWS specifically disclaims all implied warranties of merchantability, fitness for a particular purpose, title, and non-infringement, and all warranties arising from course of dealing, usage, or trade practice with respect to all use of this CCG. For avoidance of doubt, AWS does not warrant that any information contained in this CCG, or any use of or any results of the use of this CCG, will meet customer’s or any other person’s requirements or objectives, achieve any intended result, or be accurate, complete, or error free. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements. This document is not part of and does not modify any agreement between AWS and its customers.

In no event will AWS be liable in connection with any use of this CCG under any legal or equitable theory, including breach of contract, tort (including negligence), strict liability, and otherwise, including without limitation for any (a) consequential, incidental, indirect, exemplary, special, enhanced, or punitive damages, (b) increased costs, diminution in value, or lost business, production, revenues, or profits, (c) loss of goodwill or reputation, (d) use, inability to use, loss, interruption, delay, or recovery of any data or breach of data or system security, or (e) cost of replacement goods or services, in each case regardless of whether AWS was advised of the possibility of such losses or damages or such losses or damages were otherwise foreseeable.


NOTICES

By opening or using this Customer Compliance Guide (CCG) document, you agree to the Terms of Use set forth below. If you do not wish to adhere to the Terms of Use, do not open or use this CCG document.

This CCG is intended to serve as an informative resource for customers leveraging the shared responsibility model in navigating their security compliance needs. The CCG is derived from AWS Service User Guides and is designed to provide a consolidated view of AWS security practices based on the configurable options applicable to a service, related compliance topics and control requirements. Customers may use this CCG to facilitate an understanding AWS’s current product offerings and practices as of the date of issue of this CCG.

The CCG is not designed to address all aspects of a given compliance framework or all possible configurable options for a service. Customers are responsible for determining compliance requirements and validating control implementation in accordance with their organization’s policies, requirements and objectives. The security practices described in this CCG may not represent the best course of action for every organization.

Instructions for Opening AWS Customer Compliance Guides

1. **First, download this document**
2. **Open with Adobe Acrobat (preferred) or your alternate PDF viewer**
3. **Next, double click the paper clip icon to open the AWS Customer Compliance Guides** 

Note: Some products referenced in this CCG may not yet be in scope for a particular compliance program or in a certain region. Refer to the [AWS Services in Scope page](#) for a list of services in scope by compliance program.

We encourage you to share feedback on your experience using CCGs and your recommendations for improvements in our [CCG Survey](#). You can also email us at ccgrequests@amazon.com. To learn more about the background of CCGs and how best to use them, see the YouTube video [Simplify the Shared Responsibility Model](#).

CCGs are built by the [AWS Global Security and Compliance Acceleration \(GSCA\) Program](#). We help customers meet their security and compliance authorization goals by connecting them with AWS Partners and offering one-on-one sessions with AWS Security Strategists and Solution Architects. If you need assistance with achieving compliance certifications, [please fill out this form to engage us](#).

About Customer Compliance Guides

Customer Compliance Guides help customers address three primary challenges:

1. Explaining how configuration responsibility might vary depending on the service and summarizing security best practice guidance through the lens of compliance
2. Assisting customers in determining the scope of their security or compliance assessments based on the services they use to run their workloads
3. Providing customers with guidance to craft security compliance documentation that might be required to meet various compliance frameworks

CCGs map key details from [public AWS user guides](#) to industry-leading control framework requirements. The scope of CCGs is concentrated to address technical security controls implemented within AWS accounts. This makes the guides lightweight and focused on the unique security considerations for individual AWS services.

Customer Compliance Guides work backwards from security configuration recommendations for each service and map the guidance and compliance considerations to the following frameworks:

- NIST 800-53 Rev5
- NIST Cybersecurity Framework (CSF)
- NIST 800-171
- System and Organization Controls (SOC) II
- Center for Internet Security (CIS) Critical Controls v8.0
- ISO 27001
- IRAP (Australian ISM)
- Canadian Centre for Cyber Security (CCCS)
- Cloud Security Alliance (CSA) CCM v-4
- NERC Critical Infrastructure Protection (CIP)
- HIPAA
- Payment Card Industry Data Security Standard (PCI-DSS) v4.0
- Department of Defense Cybersecurity Maturity Model Certification (CMMC)
- New York Dept. of Financial Service Cybersecurity Regulation (NYDFS)
- Federal Financial Institutions Examination Council Cybersecurity Assessment Tool (FFIEC)
- Cloud Computing Compliance Criteria Catalogue – C5:2020
- MPA Content Security Best Practices v-5.2