AWS GovCloud (US)

Compliance Cloud Solutions

Stratus Environment:
Secure Design Description

Purpose

Compliance Cloud was built to help companies (and the consultants that support them), achieve their complaince goals by leveraging security, workflow, and automation. A key component of this mission is doing our part to assure the data contained within Compliance Cloud is protected with controls that meet or exceed the compliance frameworks we are helping companies evaluate against.

The goal of this document is to provide a high level overview of the controls which are in place to protect the data contained within Compliance Cloud. For operational security purposes, we will not publicly disclosure the technical details of these controls, so if you have further questions or need more details, please contact security@getcompliancecloud.com.

Hosting

Compliance Cloud is hosted within Amazon Web Services (AWS) GovCloud.

From Amazon: *AWS GovCloud (US) gives government customers and their partners the flexibility to architect secure cloud solutions that comply with the FedRAMP High baseline; the DOJ's Criminal Justice Information Systems (CJIS) Security Policy; U.S. International Traffic in Arms Regulations (ITAR); Export Administration Regulations (EAR); Department of Defense (DoD) Cloud Computing Security Requirements Guide (SRG) for Impact Levels 2, 4 and 5; FIPS 140-2; IRS-1075; and other compliance regimes.*

This infrastructure are operated by employees who are U.S. citizens on U.S. soil. For more details on AWS GovCloud, please see https://aws.amazon.com/govcloud-us/.

Security

Compliance Cloud is a true cloud native application. The entire application is hosted leveraging serverless technologies which eliminates the need to manage any operating system configuration, security patching, or access management consideration to an underlying server. We follow the principle of least privilege when provisioning IAM users and roles. All data is encrypted in transit and at rest, and we have visibility into all activity in the environment using the built-in logging capabilities that AWS provides and recommends for it's services.

Finally, we continuously monitor our environment, run security scans across the AWS account using industry standard tools, and engage third-party penetration tests to evaluate the web application itself.