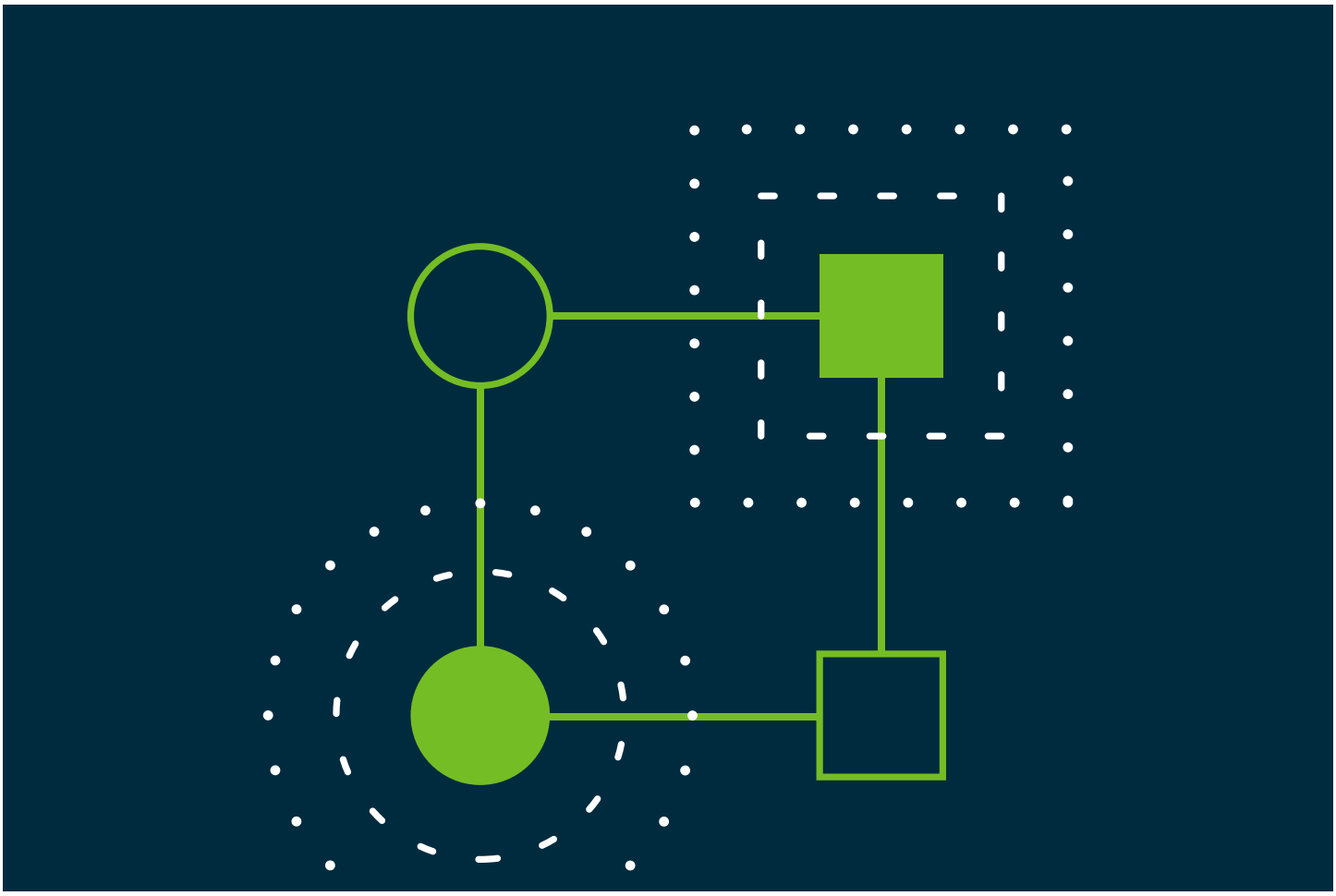
Collibra

Whitepaper

Collibra and FedRAMP



Overview

In order for the US Federal Government to operate in the cloud with a Cloud Service Provider (CSP), the CSP has to obtain the Federal Risk and Authorization Management Program (FedRAMP). FedRAMP is a standard that was created in order to ensure there is a standard approach to measuring and monitoring security in the Cloud for Federal Agencies. In order to achieve FedRAMP, a CSP has to undergo an audit from a 3rd party assessment organization. An organization can obtain a FedRAMP level of Low, Moderate, and High. The levels each have different amounts of controls for compliance, with High having the most stringent controls.

Why is FedRAMP important?

FedRamp is a way for the US government agencies to ensure Cloud Providers are adhering to a set of security standards that will keep their data safe. Achieving this certification is necessary for a cloud provider that wants to do business with most US Federal Government agencies.

FedRAMP Security

FedRAMP is like many other compliance frameworks, including NIST CSF, and is organized into 17 different families of controls (i.e. Access Control, Auditing, Incident Handling). Each family of controls have a control name and description that the FedRAMP auditor can use to ensure compliance. A couple of examples are:

- Does the information system disable inactive accounts after 90 days?
- Does the organization provide basic security awareness training to end users?

The number of questions vary depending on FedRAMP level. Low has 124, Moderate has 261, and High has 343. A qualified accessor (3PAO in government terms) for FedRAMP will help a company achieve compliance.

Collibra and FedRAMP

Collibra undertook FedRAMP certification in order to allow government agencies to be able to benefit from using the Collibra Platform. Our FedRamp compliance level is Moderate and we received our Authority to Operate (ATO) from a Federal Agency. Collibra will continue to keep its FedRAMP certification current and recertify every year as required. We maintain resources on the Collibra Security team dedicated to ensuring our FedRAMP Compliance. In addition to annual recertification, the Collibra FedRAMP environment undergoes frequent vulnerability scanning by a FedRAMP-certified vulnerability scanner to ensure Collibra is up to date on patches.

Operational Security

Operational practices

As a part of doing business, Collibra complies with various regulations and policies. One of the ways we comply by maintaining a comprehensive, written information security program that contains technical and organizational safeguards designed to prevent unauthorized access to customers' data.

Vulnerability management

We scan our code for vulnerabilities using industry standard tools on a regular basis. For FedRAMP this is completed every month at a minimum. Any vulnerabilities found are remediated and prioritized based on the criticality level of the issue.

Incident management

We have a formal security incident response plan in place that involves all aspects of Collibra's team including CloudOps, Development, Support, Legal, Finance, and Executives. The plan ensures that we can react quickly to incidents and prioritize fixes or compensating controls.

Application Security

Our applications undergo constant application security testing. This process includes source code analysis, open source analysis, website scanning, and routine 3rd party penetration testing. The testing happens in all stages of the development lifecycle from ideation through production release.

Cloud Security

Cloud architecture

Our cloud architecture is designed to segregate and restrict data access to ensure security of the customer data. The architecture of the cloud environment used by Collibra provides logical data separation and role-based access privileges, all controlled on a customer-specific level.

Identity and access management

We control and restrict access to our software to ensure appropriate identity, entitlement, and access management. We support industry identity federation standards such as SAML which allows integration with customers' single sign-on (SSO) solutions.

Encryption

Collibra implements encryption for data at rest using the Advanced Encryption Standard (AES) algorithm with a key size of 256 bits. Encryption in transit is secured using Transport Layer Security (TLS) >1.2.

Collibra – built securely for the future

Collibra's cloud-based platform is built for both today's digital transformation and the data challenges of tomorrow. This includes both private and public organizations that can utilize out world class data intelligence capabilities. Our commitment to FedRAMP shows this and we will continue to support the security requirements of our public-sector partners. Security is at the core of everything we do, and federal agencies will be able to use Collibra in the cloud with confidence.

For additional questions, contact us at:

United States
+1 646 893 3042

United Kingdom
+44 203 695 6965

All other locations
+32 2 894 79 60

By email
info@collibra.com