Code42 and FedRAMP compliance

Who is this article for?
Find your product plan in the Code42 console on the Account menu (https://support.code42.com/Administrator/Cloud/Code42_console_reference/01_Code42_console_overview#Account_menu).

√ Incydr Professional and Enterprise
√ Incydr Basic and Advanced
√ CrashPlan Cloud
√ CrashPlan for Small Business (https://support.code42.com/Small_Business) (https://support.code42.com/Small_Business)
√ Other product plans

Overview

This article gives an overview of the FedRAMP program and describes the Code42 federal environment and its compliance with federal requirements.

Considerations


• Code42 maintains several cloud environments, only one of which complies with FedRAMP requirements due to the configuration and hosting of its infrastructure.

The Code42 federal environment

The Code42 federal environment implements the same set of robust security measures and practices as all Code42 environments, but differs slightly in functionality due to its architecture. For the Code42 federal environment:

• The Code42 federal environment is categorized in the moderate impact level according to FIPS 199 (https://csrc.nist.gov/publications/detail/fips/199/final) requirements.

• The Code42 console, CrashPlan, and all data is encrypted according to FIPS 140-2 (https://csrc.nist.gov/publications/detail/fips/140-2/final) requirements, instead of via other strong encryption methods that may not be FIPS compliant. In all Code42 environments, data is encrypted both at rest and in transit.

• To ensure the use of FIPS encryption in the Code42 app, app installations must be deployed with a deployment policy (https://support.code42.com/Administrator/Cloud/Planning_and_installing/Manage_app_installations_in_your_Code42_environment/Deploy_Code42_apps). Users cannot download the installation
package from the Code42 console or an email message.

- External keystores (such as a Vault server) cannot be used to separately store encryption keys.
- Zip file restores (https://support.code42.com/Administrator/Cloud/Monitoring_and_managing/Restore_files_from_the_Code42_console#Zip_file_restore) from the Code42 console are not available. Administrators can still restore any files to any device using the device or "push" restore (https://support.code42.com/Administrator/Cloud/Monitoring_and_managing/Restore_files_from_the_Code42_console#Device_restore) feature.
- Cloud and email service data sources (https://support.code42.com/Administrator/Cloud/Configuring/Introduction_to_adding_data_connections) for Forensic File Search are not available.
- Code42 backs up data in the Code42 federal environment in the order that files were discovered and added to the to-do list, instead of backing up the most recent files first followed by older files.

Request the Code42 security package

Government agencies can request access to the Code42 security package using the request form available on the FedRAMP Marketplace (https://marketplace.fedramp.gov/#/products?sort=productName). To access the form, select Code42 from the marketplace list and then click the Package Access Request Form link.

You can also contact your Customer Success Manager (CSM) for more information on Code42's FedRAMP compliance. If you do not know your CSM, please contact our Customer Champions for support (https://support.code42.com/Terms_and_conditions/Code42_customer_support_resources/Get_support_for_CrashPlan_for_Small_Business_or_Code42_CrashPlan).

FedRAMP program overview

The Federal Risk and Authorization Management Program (https://www.fedramp.gov/) (FedRAMP) from the United States Government provides a standard method for the security assessment, authorization, and continual monitoring of cloud products and services. Government agencies (and companies who partner with them) are required to choose FedRAMP authorized providers when using cloud products and services to ensure the security of their data.

The Federal Information Security Management Act (https://csrc.nist.gov/projects/risk-management/detailed-overview) (FISMA) enacted in 2002 defines the IT security requirements that U.S. federal agencies are required to meet. The FedRAMP program clarifies how FISMA's requirements apply to cloud services.

Non-government, public sector companies may use FedRAMP authorized cloud services if they frequently partner with government agencies, want to leverage known approvals and standard practices, or value the robust assessment and continuous monitoring of security risks offered by FedRAMP.
FedRAMP compliance

The FedRAMP framework emerged from a need to modernize government agencies' aging IT infrastructure and systems that were cumbersome, individually managed, and inconsistent in the application of security practices. By standardizing the method by which providers can assess, manage, monitor, and report security risks, FedRAMP helps accelerate the adoption of cloud services and products across government agencies. This adoption helps make agencies more nimble and agile by:

- Leveraging existing security assessments to save agency time and resources: "do once, use many"
- Ensuring a standard approach to security risk assessments and mitigation
- Increasing confidence in the security of cloud services and products
- Increasing automation and data access

Governance

Development, maintenance, and operation of FedRAMP is governed by several U.S. entities (https://www.fedramp.gov/governance):

- The Office of Management and Budget (OMB) issued the FedRAMP policy memo that defines the key requirements and capabilities of the program.
- The Joint Advisory Board (JAB) is responsible for primary governance and decision-making. This board is comprised of chief information officers from:
  - The Department of Homeland Security (DHS)
  - The General Services Administration (GSA)
  - The Department of Defense (DOD)
- The CIO Council distributes FedRAMP information for cross-agency coordination.
- The FedRAMP Program Management Office (PMO) is responsible for the development of the program and management of day-to-day operations.
- The National Institute for Standards and Technology (NIST) advises on FISMA compliance and develops the standards used to assess that compliance.

Applicable regulations and standards

Requirements for U.S. government agency's IT systems and security are defined in the following:

The National Institute for Standards and Technology (https://www.nist.gov) (NIST) develops the standards by which organizations can demonstrate compliance to those regulations. Some of the NIST standards that form the backbone of FedRAMP authorization include:


NIST also develops and maintains Federal Information Processing Standards (FIPS) (https://www.nist.gov/standardsgov/compliance-faqs-federal-information-processing-standards-fips) that define how data and information systems should be categorized, encrypted, signed, verified, or authenticated in accordance with FISMA. These standards are also valuable resources to help public sector companies establish strong information security programs.

**Impact levels**

Under FedRAMP, cloud service providers are categorized into one of three impact levels (https://www.fedramp.gov/understanding-baselines-and-impact-levels/), based on the impact an outage would have on the federal agencies using the CSP's services:

- **Low**: Loss of confidentiality, integrity, or availability results in limited impact to an agency's reputation, finances, or safety. Low impact systems typically store minimal personal identifiable information (PII) beyond that needed to authenticate users (such as usernames, passwords, and email addresses).
- **Moderate**: Loss of confidentiality, integrity, or availability results in serious impacts to an agency's operations, assets, or individuals. These impacts include significant operational disruption, financial loss, or non-physical harm to individuals. The Code42 federal environment falls into this moderate impact level.
- **High**: Loss of confidentiality, integrity, or availability results in catastrophic impacts to an agency, potentially including financial loss or closure, halting of operations, or loss of intellectual property or individual lives. CSPs at this level usually handle high-risk systems, such as defense, intelligence, healthcare, finance, or emergency or law enforcement systems.

**Authorization process**

Achieving FedRAMP authorization (https://www.fedramp.gov/cloud-service-providers/) is a complex process. A high-level overview follows:

1. The cloud service provider (CSP) connects with the FedRAMP Joint Advisory Board (JAB) and determines the type of authorization to pursue.
   
   *Two types of authorization are available: Provisional Authority to Operate (P-ATO) or Agency Authority to Operate (ATO). CSPs identify which type of authorization to pursue based on their processes, impact level, deployment model, and market demand.*

2. The CSP partners with a third party assessment organization (3PAO) as needed and completes a readiness assessment report detailing its cloud service offering or product.
   
   *If the JAB approves the provider's readiness assessment report, the CSP is then designated "FedRAMP Ready" and is*
advertised in the FedRAMP Marketplace.

3. With the 3PAO, the CSP uses FedRAMP-provided templates to create and submit the following documentation:
   ◦ System Security Plan (SSP)
   ◦ Security Assessment Plan (SAP)
   ◦ Security Assessment Report (SAR)
   ◦ Plan of Actions and Milestones (POA&M)

4. All documentation is reviewed and any questions or comments are submitted to the CSP for assessment. After all questions are addressed and remediation activities are completed, the CSP receives FedRAMP authorization.

5. After receiving authorization, the CSP provides documents generated during continuous monitoring activities to the agencies using their service. The CSP also works with the 3PAO to complete an annual security assessment that is submitted to the FedRAMP repository to validate continued compliance.

External resources

• FedRAMP.gov (https://www.fedramp.gov/)

• NIST resources
  ◦ Computer Security Resource Center (https://csrc.nist.gov/)

Related topics

• Detect and respond to insider risks (https://support.code42.com/Administrator/Cloud/Monitoring_and_managing/Detect_and_respond_to_insider_risks)
• Detect and respond to insider risks (https://support.code42.com/Administrator/Cloud/Monitoring_and_managing/Detect_and_respond_to_insider_risks)
• Restore files (https://support.code42.com/CrashPlan/6/Restoring)
• Replace your device (https://support.code42.com/CrashPlan/6/Configuring/Replace_your_device)