Zertø

Quick Guide to FedRAMP

Cloud Migration

To support efforts to modernize the delivery of services to citizens, federal agencies are migrating many of their systems from legacy networks to cloud-based environments. Cloud computing delivers multiple benefits, including:

- Reduced IT acquisition and operating costs
- Faster services provision
- Improved scalability
- Accelerated adoption of new technologies

The adoption of cloud services allows government entities to realize efficiencies th y cannot achieve with legacy IT systems. But cloud services adoption must take place in a safe, uniform way to avoid creating security risks, which is why federal agencies must follow the standardized, repeatable guidelines of the Federal Risk and Authorization Management Program (FedRAMP) framework.

What is FedRAMP?

FedRAMP standardizes security assessments, authorization, and ongoing monitoring of cloud solutions and services for government agencies. With FedRAMP, agencies adopting cloud services receive clear guidance on how to comply with the data protection guidelines of the Federal Information Security Management Act (FISMA).

Do It Once

The driving philosophy behind FedRAMP is “do once, use many times.” The framework provides a repeatable model for the implementation of cloud services. As such, it saves costs, time, and staff y accelerating security assessments and the procurement of systems and services. It allows federal agencies to properly implement security controls without duplicating effort or driving up risk management costs. In short, incorporating the FedRAMP framework with internal security authorization processes ensures that agencies meet federal requirements for cloud services.

Cloud Service Providers

FedRAMP-compliant Cloud Service Providers (CSP) use the same security baseline for their systems, which means government entities can expect the following standardization when they leverage authorizations:

- Security requirements for identifying qualified third-party security assessors
- A repository of authorization packages for secure clouds that all agencies can leverage
- An ongoing assessment and authorization approach for government clouds
- Contract language to help agencies integrate FedRAMP requirements and best practices into acquisitions

Interagency Collaboration

The development of FedRAMP guidelines was a joint effort of the National Institute of Standards and Technology (NIST), General Services Administration (GSA), Department of Defense (DOD), and Department of Homeland Security (DHS), with collaboration from other agencies, working groups, and industry experts. In November 2017, the government released version 2.4 of the FedRAMP Security Assessment Framework, which replaced the FedRAMP Concept of Operations.

Why FedRAMP?

FedRAMP ensures the implementation of security controls on cloud systems that process, store, and/or transmit government data. Cloud systems used by government agencies must be secured in accordance with the government’s specific, stringent requirements (focused on risk management) rather than simply meeting compliance requirements. When agencies adhere to standardized processes, procedures, and controls, they are more effective in identifying, assessing, and mitigating risks.

Zerto IT Resilience Platform

FedRAMP categorizes the level of security for each system in use by agencies as low, moderate, or high impact. Agencies must determine the impact level for each system before implementing security controls. The Zerto IT Resilience platform helps agencies meet a significant number of security requirements, including contingency planning and incident response:

Efficient Contingency Plan

Legacy disaster recovery and backup tools can quickly become cumbersome with unwieldy runbooks and too many time-consuming recovery steps. Zerto simplifies contingency planning orchestration, automation, and near synchronous replication, providing best-in-class Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs)—all managed through a single platform.

Quick Incident Response

Effective incident response is essential to risk management. Zerto delivers the ability to meet stringent data protection guidelines and recover from an incident in minutes with near-zero data loss.

For more information, download the IT Resilience Overview for Government

DOWNLOAD SOLUTION OVERVIEW

Simple Recovery

DR tests and failovers are orchestrated and automated, requiring only four simple steps and significantly reducing the DR runbook.

Automated DR Test Reports

Zerto documents the pass/fail of each step of the recovery process, making 3PAO and other assessments hassle-free. Reports are delivered in concise PDFs for auditing and management purposes. They can be generated for any failover test, customized with company logos, and scripted to run anytime.

DR Target Options

Zerto is storage-agnostic and provides mixed hypervisor support. Any site can be replicated to any other site, whether it is a private, public, hybrid, or multi-cloud environment; service provider site; or branch office.

Best-in-class RPOs and RTOs

VM-level replication delivers best-of-breed replication with the tightest available RTOs and RPOs to ensure a quick recovery. And it’s possible to rewind if a migration or other modification doesn’t deliver as expected.

Long-term Retention

Most backup solutions rely on snapshots for recovery, a complex and limiting process when timely recoveries are needed. Zerto uses continuous data protection, so the always-updated, replicated VM data in the recovery site can be used to create offsite copies on a daily, weekly, monthly, or yearly schedule.

Zerto’s IT Resilience Platform helps agencies comply with these controls

	SORT ID	Family	ID	Control Name
145	CP-01	CONTINGENCY PLANNING	CP-1	CONTINGENCY PLANNING POLICY AND PROCEDURES
146	CP-02	CONTINGENCY PLANNING	CP-2	CONTINGENCY PLAN
147	CP-02 (01)	CONTINGENCY PLANNING	CP-2 (1)	CONTINGENCY PLAN | COORDINATE WITH RELATED PLANS
148	CP-02 (02)	CONTINGENCY PLANNING	CP-2 (2)	CONTINGENCY PLAN | CAPACITY PLANNING
149	CP-02 (03)	CONTINGENCY PLANNING	CP-2 (3)	CONTINGENCY PLAN | RESUME ESSENTIAL MISSIONS / BUSINESS FUNCTIONS
150	CP-02 (04)	CONTINGENCY PLANNING	CP-2 (4)	CONTINGENCY PLAN | RESUME ALL MISSIONS / BUSINESS FUNCTIONS
151	CP-02 (05)	CONTINGENCY PLANNING	CP-2 (5)	CONTINGENCY PLAN | CONTINUE ESSENTIAL MISSIONS / BUSINESS FUNCTIONS
152	CP-02 (08)	CONTINGENCY PLANNING	CP-2 (8)	CONTINGENCY PLAN | IDENTIFY CRITICAL ASSETS
154	CP-03 (01)	CONTINGENCY PLANNING	CP-3 (1)	CONTINGENCY TRAINING | SIMULATED EVENTS
155	CP-04	CONTINGENCY PLANNING	CP-4	CONTINGENCY PLAN TESTING
156	CP-04 (01)	CONTINGENCY PLANNING	CP-4 (1)	CONTINGENCY PLAN TESTING | COORDINATE WITH RELATED PLANS
157	CP-04 (02)	CONTINGENCY PLANNING	CP-4 (2)	CONTINGENCY PLAN TESTING | ALTERNATE PROCESSING SITE
158	CP-06	CONTINGENCY PLANNING	CP-6	ALTERNATE STORAGE SITE
159	CP-06 (01)	CONTINGENCY PLANNING	CP-6 (1)	ALTERNATE STORAGE SITE | SEPARATION FROM PRIMARY SITE
160	CP-06 (02)	CONTINGENCY PLANNING	CP-6 (2)	ALTERNATE STORAGE SITE | RECOVERY TIME / POINT OBJECTIVES
161	CP-06 (03)	CONTINGENCY PLANNING	CP-6 (3)	ALTERNATE STORAGE SITE | ACCESSIBILITY
162	CP-07	CONTINGENCY PLANNING	CP-7	ALTERNATE PROCESSING SITE
163	CP-07 (01)	CONTINGENCY PLANNING	CP-7 (1)	ALTERNATE PROCESSING SITE | SEPARATION FROM PRIMARY SITE
164	CP-07 (02)	CONTINGENCY PLANNING	CP-7 (2)	ALTERNATE PROCESSING SITE | ACCESSIBILITY
165	CP-07 (03)	CONTINGENCY PLANNING	CP-7 (3)	ALTERNATE PROCESSING SITE | PRIORITY OF SERVICE
166	CP-07 (04)	CONTINGENCY PLANNING	CP-7 (4)	ALTERNATE PROCESSING SITE | PREPARATION FOR USE
167	CP-08	CONTINGENCY PLANNING	CP-8	TELECOMMUNICATIONS SERVICES
172	CP-09	CONTINGENCY PLANNING	CP-9	INFORMATION SYSTEM BACKUP
173	CP-09 (01)	CONTINGENCY PLANNING	CP-9 (1)	INFORMATION SYSTEM BACKUP | TESTING FOR RELIABILITY / INTEGRITY
174	CP-09 (02)	CONTINGENCY PLANNING	CP-9 (2)	INFORMATION SYSTEM BACKUP | TEST RESTORATION USING SAMPLING
175	CP-09 (03)	CONTINGENCY PLANNING	CP-9 (3)	INFORMATION SYSTEM BACKUP | SEPARATE STORAGE FOR CRITICAL INFORMATION
176	CP-09 (05)	CONTINGENCY PLANNING	CP-9 (5)	INFORMATION SYSTEM BACKUP | TRANSFER TO ALTERNATE STORAGE SITE
177	CP-10	CONTINGENCY PLANNING	CP-10	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION
178	CP-10 (02)	CONTINGENCY PLANNING	CP-10 (2)	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | TRANSACTION RECOVERY
179	CP-10 (04)	CONTINGENCY PLANNING	CP-10 (4)	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | RESTORE WITHIN TIME PERIOD
213	IR-02 (01)	INCIDENT RESPONSE	IR-2 (1)	INCIDENT RESPONSE TRAINING | SIMULATED EVENTS
215	IR-03	INCIDENT RESPONSE	IR-3	INCIDENT RESPONSE TESTING
216	IR-03 (02)	INCIDENT RESPONSE	IR-3 (2)	INCIDENT RESPONSE TESTING | COORDINATION WITH RELATED PLANS
220	IR-04 (03)	INCIDENT RESPONSE	IR-4 (3)	INCIDENT HANDLING | CONTINUITY OF OPERATIONS
226	IR-06	INCIDENT RESPONSE	IR-6	INCIDENT REPORTING
227	IR-06 (01)	INCIDENT RESPONSE	IR-6 (1)	INCIDENT REPORTING | AUTOMATED REPORTING
231	IR-08	INCIDENT RESPONSE	IR-8	INCIDENT RESPONSE PLAN

About Zerto

Zerto helps customers accelerate IT transformation by eliminating the risk and complexity of modernization and cloud adoption. By replacing multiple legacy solutions with a single IT Resilience Platform, Zerto is changing the way disaster recovery, data protection and cloud are managed. With enterprise scale, Zerto’s software platform delivers continuous availability for an always-on customer experience while simplifying workload mobility to protect, recover and move applications freely across hybrid and multi-clouds. **www.zerto.com**