Decoding FedRAMP

> "Think about FedRAMP early and build it into product and processes from the start."
>
> - Ignacio Martinez, Smartsheet.

Security impact levels explained

FedRAMP (Federal Risk and Authorization Management Program) defines three security impact levels—Low, Moderate, and High—based on the sensitivity of data and the potential impact of a security breach. Each level dictates the number of required security controls and the rigor of compliance, ensuring federal data is protected according to its risk profile.

High

Moderate

Low

Low

For systems handling public or non-sensitive data where a breach would have minimal impact on operations, finances, or reputation.

Typical Data:
Generic login info, no sensitive personal or mission-critical

Use Case:
Public-facing websites, SaaS apps with no sensitive PII

Impact Risk:
Generic login info, no sensitive personal or mission-critical data

Moderate

For systems containing sensitive but unclassified data, including PII, where a breach could disrupt agency operations or cause significant financial loss.

Typical Data:
Sensitive but unclassified info, PII, agency operational data

Use Case:
Most federal cloud services (about 80% of FedRAMP-authorized CSPs fall here)

Impact Risk:
Serious adverse effects, such as significant operational disruption or financial loss, but not life-threatening

High

For systems handling the government's most sensitive, unclassified data, where a breach could threaten national security, public safety, or cause catastrophic financial loss.

Typical Data:
Law enforcement records, health data, financial systems, mission-critical operations

Use Case:
Law enforcement, emergency services, healthcare, financial systems, national security

Impact Risk:
Severe or catastrophic effects, including potential loss of life, mission failure, or irreparable institutional damage

How 1Kosmos supports FedRAMP compliance

- **FedRAMP High Authorization:**
  Meets 421 NIST 800-53 security controls, providing the most stringent civilian security standard.
- **FIPS 140-3 Encryption:**
  All data is protected in transit and at rest with federal-grade cryptography.
- **Continuous Monitoring & Fast Remediation:**
  Delivers real-time threat detection, automated logging, and rapid vulnerability fixes per FedRAMP requirements.
- **U.S. GovCloud Hosting:**
  Managed by U.S. citizens with strict background checks, supporting data sovereignty and compliance.

1KOSMOS

Is proud to be FedRAMP High Certified

1kosmos.com