The digital environment increases agency exposure to adversarial risk. Cybercrime can disrupt business, disclose PII, and impact national security. Protecting the security and privacy of digital assets and cultivating the ability to monitor, identify, contain, and address risks are critical to mitigating cybercrime.

Deploying a Uniform Risk Management Approach to Cloud

To provide cloud services to agencies, vendors must meet the Federal Risk and Authorization Management Program (FedRAMP).

FedRAMP is a uniform risk management approach and assessment process of a standard set of approved, minimum security assessments, controls, and continuous monitoring.

FedRAMP security controls are based on NIST and FISMA baselines and address the unique elements of cloud computing.

FedRAMP categorizes federal systems as:
- Low Impact, those meeting 125 security controls
- Moderate Impact, those meeting 325 security controls
- High Impact, meeting 421 security controls.

DoD Cloud Computing Security Requirements

DoD uses Impact Levels, based on the type of data to be processed, to assess a cloud provider’s offering, and issues similar authorizations as FedRAMP.

FedRAMP Moderate Impact = DoD Impact Level 2

FedRAMP Moderate Impact + 44 additional controls = DoD Impact Level 4

FedRAMP High Impact + 9-10 additional controls = DoD Impact Level 5

FedRAMP High Impact + 9-10 additional controls = DoD Impact Level 6

Security in the Cloud Is a Shared Responsibility

- For both FedRAMP and DoD Impact Levels, cloud security is a shared responsibility between the mission owner and cloud vendor.
- Certified vendors must maintain a security authorization of continuous monitoring and ongoing controls meeting FedRAMP and/or DoD requirements.
- Vendors must provide monthly operating system, database, and web application vulnerability scanning reports to detect security changes.
- Agencies must ensure clear/meaningful roles and responsibilities for security, scan for application vulnerabilities, review monthly continuous monitoring reports, and annually assess cloud service providers’ security practices and documentation.

As Vendors Increase Their FedRAMP and DoD Security Authorizations, Agencies Must Migrate

When vendors discontinue lower levels of security for higher level controls, agencies must move to better protect digital assets.

At higher security levels, agency responsibilities will reflect the more stringent security controls.

To find out more about how FedRAMP is paving the way for cloud adoption and saving the government money, click here.