**CFCSA Exam Objectives**

**Updated 06/06/2025**

The **Certified Federal Cloud Solutions Architect (CFCSA)** certification is essential for experienced cloud professionals aiming to thrive in the U.S. federal sector, as it uniquely validates your ability to design secure, compliant, and efficient cloud solutions specifically tailored to the rigorous demands of federal mandates like FedRAMP, NIST, and FISMA.

By demonstrating specialized expertise in federal cloud policy, security architecture, procurement, and operational best practices, the CFCSA elevates your credibility, unlocks advanced career opportunities within government agencies and contractors, and positions you as a critical asset in navigating the complex landscape of federal cloud adoption.

The CFCSA certification covers the following key domains, each with a specific weight reflecting its importance:

1. **Federal Cloud Policy & Compliance (20%)**
   * NIST Special Publications (SP) series: SP 800-53 (Security and Privacy Controls for Federal Information Systems and Organizations), SP 800-37 (Risk Management Framework), SP 800-171 (Protecting CUI in Nonfederal Systems).
   * Federal Risk and Authorization Management Program (FedRAMP): JAB, Agency ATO process, impact levels (Low, Moderate, High).
   * Defense Information Systems Agency (DISA) STIGs (Security Technical Implementation Guides).
   * FISMA (Federal Information Security Modernization Act).
   * CMMC (Cybersecurity Maturity Model Certification) - awareness and basic understanding of its impact.
   * Cloud First, Cloud Smart initiatives.
   * OMB M-XX-XX memoranda relevant to cloud adoption.
2. **Federal Cloud Security Architecture (25%)**
   * Secure multi-tenancy in federal environments.
   * Data sovereignty and residency requirements for federal data.
   * Identity and Access Management (IAM) for federal users (e.g., PIV/CAC integration, MFA requirements).
   * Encryption standards (FIPS 140-2 validated modules).
   * Network security controls (VPC/VNet design, firewalls, IDS/IPS, WAFs specific to federal use cases).
   * Logging, monitoring, and auditing for federal compliance.
   * Incident response and reporting in a federal cloud context.
   * Zero Trust Architecture principles for federal deployments.
3. **Cloud Solution Design for Federal Use Cases (20%)**
   * High availability, disaster recovery, and business continuity for federal systems.
   * Scalability and elasticity considerations for government workloads.
   * Cost optimization strategies within federal budgeting constraints.
   * Hybrid and multi-cloud strategies for federal agencies.
   * Application modernization and migration strategies for legacy federal systems.
   * Data management, storage, and archival solutions compliant with federal records management.
   * DevSecOps principles and automation in a federal secure pipeline.
4. **Federal Cloud Procurement & Contracting (15%)**
   * Understanding of federal acquisition regulations (FAR) as they apply to cloud services.
   * Contract vehicles commonly used for cloud (e.g., GSA schedules, GWACs).
   * SLA negotiation and management for federal cloud contracts.
   * Vendor lock-in mitigation strategies.
   * Open standards and interoperability in federal cloud environments.
5. **Operational Best Practices in Federal Cloud (20%)**
   * Continuous Monitoring (ConMon) for FedRAMP authorized systems.
   * Change management and configuration management in highly regulated environments.
   * Vulnerability management and patching strategies for federal cloud systems.
   * Performance management and optimization for government applications.
   * Auditing and reporting for compliance purposes.
   * Supply chain risk management in a federal cloud context.