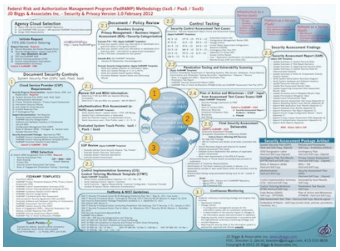
JD Biggs & Associates, Inc.

Your Trusted Partner for Improved Security & Privacy

JD Biggs is an Information Security and Privacy consulting firm located near Washington, DC in suburban Maryland. Current compliance requirements are complex, resource intensive, moderately expensive and challenging. We offer a variety of service offerings to meet your specific FedRAMP needs. Our methodologies are comprehensive and ensure that your company meets compliance standards. These methodologies shall continuously be updated to reflect the changes affecting GSA IT Security Procedures, NIST Publications, FIPS Publications and best practices identified during the assessment process.

FedRAMP Methodology



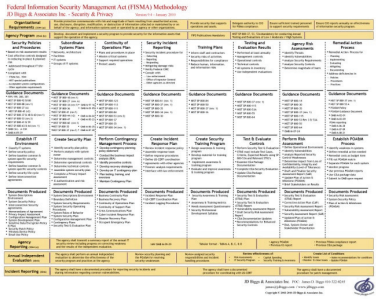
We have developed our Federal Risk and Authorization Management Program (FedRAMP) Methodology in accordance with the Federal Cloud Computing Initiative (FCCI) and the requirements defined by General Services Administration (GSA), the National Institute of Standards and Technology (NIST) and Federal Information Processing Standards (FIPS).

This methodology is our strategy for achieving compliance through assessing risks and providing the Authorizing Official (AO) with accreditation information that is associated with three service models: Infrastructure as a Service (IaaS); Platform as a Service (PaaS); Software as a Service (SaaS).

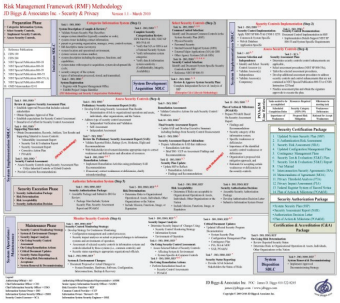
This strategy defines the required activities by the Cloud Service Provider (CSP), system owner as-well-as the 3PAO who is conducting the Independent Verification & Validation (IV&V) on the security controls. The CSP and system owner requirements involve the creation of security program documentation using the GSA templates and guidelines.

FISMA Methodology

Our Federal Information Security Management Act (FISMA) methodology tackles the five (5) major sections of the legislation and eight components of the agency program. The major sections of Title III, E-Government Act requirements imposed by the Office of Management and Budget (OMB) and what are expected to be examined by an auditor (OIG, OMB, GAO, 3rd Party) during an assessment. An Agency or Commercial organization should use this chart to educate stakeholders on FISMA compliance and also identify a specific weakness to the Enterprise Security Program or system.



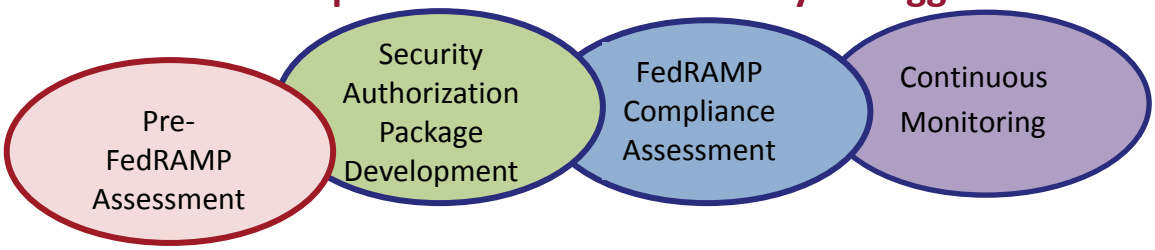
Risk Management Framework (RMF)



The Risk Management Framework (RMF) activities are performed on systems throughout the year. The system owner is required to assess the condition of security controls *annually* and receive a new accreditation decision by the Authorizing Official (AO) when the system has experienced (1) Significant Change as defined by NIST SP 800-37 rev. 1, or (2) New Authorizing Official directs this action.

Federal Risk and Authorization Management Program (FedRAMP)

Compliance Services Offered by JD Biggs



PreFedRAMP Assessment Offering

1. **Architecture Review / Compliance:** The cloud computing service model shall be evaluated for:
   - Accuracy of the system boundary
   - Accuracy of Hardware / Software inventory
   - Cloud Security Alliance "Top Threats" http://www.cloudsecurityalliance.org/topthreats.html
   - Implementation of SC-7 Boundary Protection
   - Implementation of IA-2 User Identification and Authentication Multi-Factor Authentication
   - Implementation of SI-4 Information System Monitoring Tools & Techniques (SI-4)

2. **Security Program Documentation:** FedRAMP has defined system required documents and NIST has defined 17 security policies. This assessment shall encompass the following:
   - System Security Plan (SSP) review and analysis of security categorization, general description / purpose, diagrams, roles, security control implementation descriptions, implementation status and verification of required embedded attachments
   - Formalization of an Information System Security Officer (ISSO)
   - High level review of 17 security policies (Reference NIST SP 800-53 Rev 3) – Mapping to System Security Plan
   - High level review of FCCI Key Security Controls in the SSP:

• RA 5 / 5 (9)	• SA 11 (1)	• PS 3 / 7	
• CM 2 / 6 / 8 (3)	• SI 2	• MP 4 / 5	• IA 2 (1) / 2 (2) / 2 (3) / 7
• IR 4/6	• CP 6/7/8/9	• CA 7 (2)	• SC 2 / 4 / 7 / 8 (1) / 9 (1) / 13

Note 1: *Approved FCCI security program templates (Plans / Policies) shall be provided.*

3. **Vulnerability Scanning:** The Operating Systems (OS), Web, Database (DB) and Virtual Machine (VM) environments will be assessed using software tools to provide a snapshot of vulnerability status. An agreed upon percentage of system components will be Scanned using:
   - Operating Systems (OS) - Nessus
   - Web – Acunetix
   - Database – Nexpose

Pre-FedRAMP Assessment Work Products:

1. **FedRAMP Compliance:** The roadmap document is a strategy for achieving FedRAMP compliance in accordance with current FCCI guidelines, federal mandates, publications issued by the Office of Management and Budget (OMB), NIST publications and FIPS publications. This document is based on the review/analysis and recommendations on current architecture improvements, security program documentation/policies updates, vulnerability scanning results.
2. **Vulnerability Scanning**: The results (raw data scans) from each of the tools for the selected environments shall be provided to key stakeholders for mitigation actions.

Security Authorization Package

Cloud Service Provider (CSP) / Agency System Owner*

- ✓ ISSO Designation Letter
- ✓ Privacy Impact Assessment (PIA)
- ✓ Business Impact Assessment (BIA)
- ✓ Security Categorization (FIPS 199)
- ✓ Control Implementation Summary CIS)
- ✓ Control Tailoring Workbook (CTW)
- ✓ Rules of Behavior (ROB)
- ✓ Configuration Management Plan (CMP)
- ✓ System Security Plan (SSP)
- ✓ IS Contingency Plan (ISCP)
- ✓ IS Contingency Plan Test Results (CPTR)
- ✓ IS Contingency Plan Test Report
- ✓ Continuous Monitoring Plan
- ✓ Incident Response Plan (IRP)
- ✓ Interconnection Security Agreement (ISA)
- ✓ Memorandum of Understanding (MOU)

**JD Biggs can facilitate in the creation of these documents*

Third Party Assessment Organization (3PAO)

- ✓ Security Assessment Plan
- ✓ eAuthentication Risk Assessment
- ✓ Rules of Engagement (ROE)
- ✓ Penetration Test Report
- ✓ Code Review (SAAS)
- ✓ Vulnerability Scans: OS / Web / DB / VM
- ✓ Evidentiary Artifacts (Screen shots, policies, procedures, check lists, scans, etc.
- ✓ Assessment Test Cases (17 control families)
- ✓ Plan of Action and Milestones (POA&M)
- ✓ Security Assessment Report (SAR)
- ✓ Accreditation Decision Letter / Memo

About Us

- Over 30 years of IT experience
- Degreed
- Security Clearances
- Security Professional Certifications (CISSP, CAP, CEH)
- Industry Recognized Subject-Matter-Experts (SME): FISMA, FedRAMP, DIACAP, RMF, HIPAA, NERC, CIP, CSAM, TAF
- GSA Schedule 70
- eMaryland Marketplace
- MD SDAT - D07929995
- DUNS - 180401478 /CAGE- 4V6P7
- MD State CATS II
- Small Business Reserve
- NAICS - 541519, 541512, 541990

Contact Us

President/CEO
James D. Biggs, CISSP
410-322-8245
james@jdbiggs.com

CTO
John D. Biggs, CAP, CISSP
240-393-5798
john@jdbiggs.com

Principal Security Advisor
Brandon Ghrist, CAP, CISSP
410-310-3828
brandon@jdbiggs.com

Contracts Administrator
Suzanne Biggs, CAP
202-596-8245
suzanne@jdbiggs.com