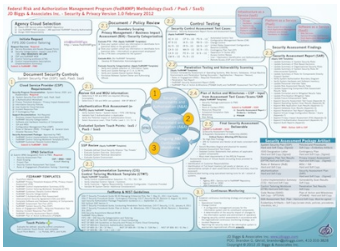
JD Biggs & Associates, Inc.

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 are an approved Third Party Assessor Organization (3PAO)*** *through the General Service Administration (GSA) Federal Risk Management Program (FedRAMP). 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



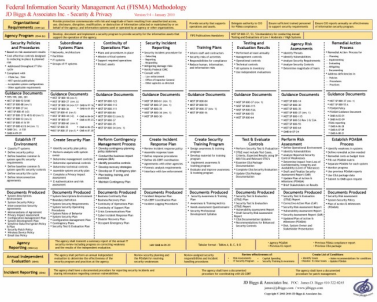
We have developed our Federal Risk and Authorization Management Program (FedRAMP) Methodology in accordance with the Federal Cloud Computing Initiative (FCCI) and the requirements defined by General Services Administration (GSA), the National Institute of Standards and Technology (NIST) and Federal Information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

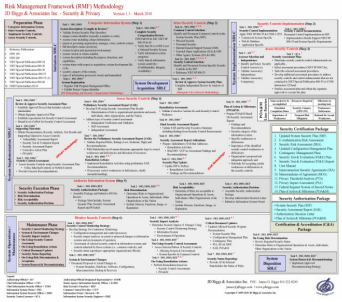
This strategy defines the required activities by the Cloud Service Provider (CSP), system owner as-well-as the 3PAO who is conducting the Independent Verification & Validation (IV&V) on the security controls. The CSP and system owner requirements involve the creation of security program documentation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

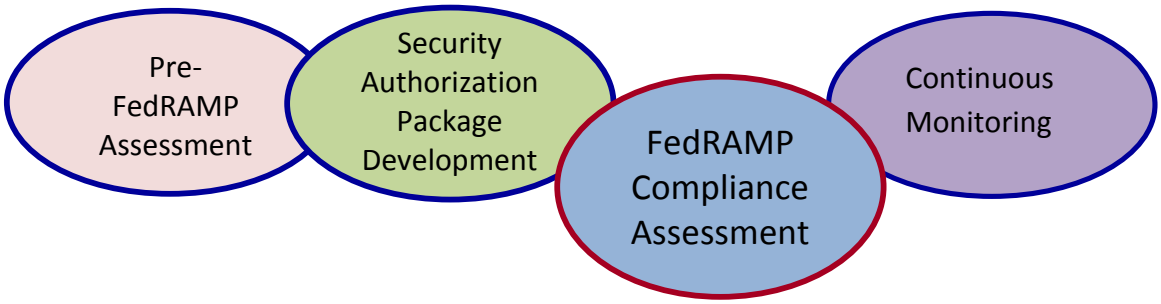


Risk Management Framework (RMF)



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



FedRAMP Compliance Assessment Offering

1. **Security Assessment Plan:** Develop the assessment plan for the service model or federal agency system accreditation boundary.
2. **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)
3. **Facilitate Security Program Documentation Updates IAW:**
   - IaaS Security Authorization Package Preparation Guidance v1.3, April 18, 2012
   - GSA IT Security Procedural Guide - Contingency Planning, CIO-IT Security 06-29, Revision 2, August 16, 2010
   - GSA IT Security Procedural Guide 06-30 Managing Enterprise Risk, Rev 7, May 31, 2011 User Guide.
   - Federal Standards - OMB Memorandums, NIST and FIPS Publications, ISO / IEC 17020:2012
4. **Penetration Testing & Vulnerability Scanning:** The Operating Systems (OS), Web, Database (DB) and Virtual Machine (VM) environments, for the cloud computing service model, must be assessed using FCCI approved software tools. An agreed upon percentage of system components will be scanned.
   - In accordance with FAS Vulnerability Scanning SOP Revision 3, April 19, 2011
   - In accordance with GSA IT Security Procedural Guide, Conducting Penetration Test Exercises, CIO IT Security, 11-51, January 4, 2011
     - Operating Systems (OS) - Nessus
     - Web – Acunetix
     - Database – Nexpose
5. **Security Control Testing:** Our security control tester shall conduct Interview, examine artifacts and conduct testing in accordance with NIST SP 800-53A Revision 1 and using the FCCI 17 templates.
6. **Plan of Action & Milestone (POA&M):** The results from the vulnerability scans and/or penetration test, along with the assessment test case workbook, shall be used to create/update the POA&M. (Apply FCCI Template)
7. **Security Assessment Report (SAR):** The SAR is assembled using the FCCI template and must reflect the risks identified from: (Apply FCCI Template)

- 17 Assessment Test Cases
- Penetration Test Report
- Vulnerability Scans
- Existing / Updated POA&M

Security Authorization Package

Cloud Service Provider (CSP) / Agency System Owner*

- ✓ ISSO Designation Letter
- ✓ Privacy Impact Assessment (PIA)
- ✓ PIA Questionnaire
- ✓ Business Impact Assessment (BIA)
- ✓ Security Categorization (FIPS 199)
- ✓ Control Implementation Summary CIS)
- ✓ Control Tailoring Workbook (CTW)
- ✓ Rules of Behavior (ROB)
- ✓ Configuration Management Plan (CMP)
- ✓ Customer Responsibility Matrix (CRM)
- ✓ Detailed System Inventory
- ✓ 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)
- ✓ Separation of Duties Matrix
- ✓ Security Training Records
- ✓ Third Party Audit Report

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

Third Party Assessment Organization (3PAO)

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

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
- Approved 3PAO through GSA
- 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