



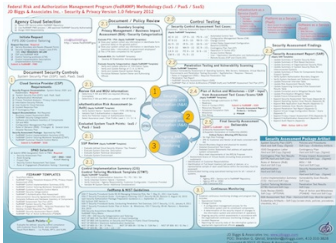
JD Biggs & Associates, Inc.



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

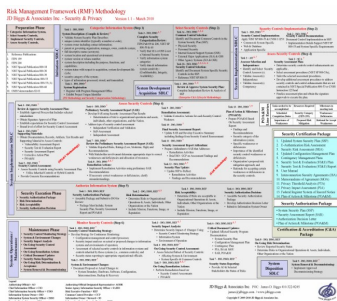


We have developed our Federal Risk and Authorization Management Program (FedRAMP) Methodology in accordance with the Federal Cloud Computing Initiative (FCCI) and the requirements defined by General Services Administration (GSA), the National Institute of Standards and Technology (NIST) and Federal Information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

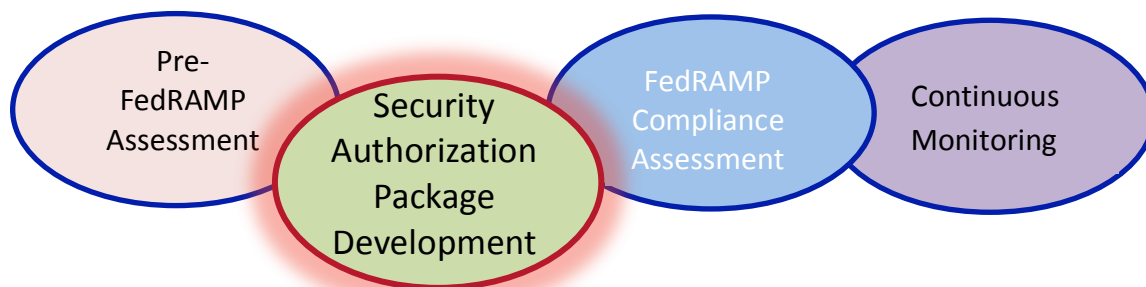
Our Federal Information Security Management Act (FISMA) methodology tackles the five (5) major sections of the legislation and eight components of the agency program. The major sections of Title III, E-Government Act requirements imposed by the Office of Management and Budget (OMB) and what are expected 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



Security Authorization Package Development Service Offering

In this service offering, we will develop the Security Authorization Package, which will ultimately be presented to the Joint Authorization Board (JAB) for an accreditation decision. This offering can be a stand-alone activity or follow our Pre-FedRAMP Assessment offering.

The authorization package is the final product of implementing the 6 steps of the Risk Management Framework (RMF). This package is comprised of documents compiled by the Cloud Service Provider and/or Federal Agency System Owner with our guidance and input. Throughout the process, our security and privacy professionals evaluate these documents and apply FedRAMP templates to ensure compliance at every level.

Security Authorization Packages

JD Biggs & Associates Inc. will develop the Security Authorization Package based on results of the security control assessment, contingency plan test results, vulnerability assessment and penetration test results. This package will provide the JAB with crucial information necessary to make a risk-based decision on whether to grant a provisional Authority to Operate (ATO). The authorization package contains the following standard core documents:

System Security Plan (SSP) - The SSP provides an overview of the security requirements and describes the security controls Fully Satisfied, Partially Satisfied, Not Satisfied and Not Applicable for meeting those requirements. The plan provides sufficient information to understand the intended or actual implementation of each security control and enhancement employed within or inherited by the CSP. The SSP provides the baseline or foundation, which the security control assessment is conducted.

Security Assessment Report (SAR) - The SAR, prepared by JD Biggs & Associates Inc., provides the results of assessing the implementation of the security controls as defined in the SSP to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the specified security requirements. This assessment is conducted in accordance with NIST SP 800-53A (latest revision) and FedRAMP defined parameters. The SAR also contains a list of required corrective actions for each weaknesses or deficiencies identified in the security controls.

Plan of Action & Milestone (POA&M) - The POA&M describes the specific measures planned to correct weaknesses or deficiencies noted in the security controls, vulnerability and Penetration testing.

Note 1: After completion of the Security Authorization Package, JD Biggs & Associates Inc. completes the process by assisting with delivery of the final security authorization package to the authorizing official.



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
- ✓ 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

