PLATINUM
BUSINESS SERVICES, LLC

Assessments & Authorizations (A&A) as a Necessity

Platinum Business Services, LLC

Jody Venkatesan, CISA, CISM, CGEIT, CRISC, CDPSE
President & CEO

Email: jvenkatesan@weareplatinum.net
Phone: 301-651-1297
Fax: 301-483-0104
Website: weareplatinum.net

SBA Certified 8(a) HUBZone, Service-Disabled Veteran Owned Small Business (SDVOSB), Veteran-Owned Small Business (VOSB), Small Business (SB), Small Disadvantaged Business (SDB)
TIN/EIN: 26-3462811
Cage Code: 59N47
DUNS: 828491410
UEI: PCNMDK3FLJB9
CIOSP3 NIH CIOSP3 SDVO
(Contract #HHSN316201800030W)
GSA MAS Professional Services #GS00F344CA
GSA MAS IT #GS-35F-0067Y
GSA 8(a) STARS 3 #47QTCB21D0108

Assessments & Authorizations (A&A) as a Necessity

Assessments and Authorizations (A&A) – A Requirement Under FISMA

In 2002, the Federal Information Security Modernization Act (FISMA) was instituted, providing guidelines and security standards to protect the Government's information and operations. 2014 it was updated to address the rising number of cybersecurity attacks. Over the past decade, these attacks, from both external and internal sources, have continued to increase, making FISMA and other cybersecurity defenses more and more critical.

FISMA presented many agencies with some serious cybersecurity challenges. Before FISMA, security was focused on ensuring that the boundaries of all systems – the network access points – were defended correctly, using the old Certification and Accreditation (C&A) process. FISMA recognized that the risks were based on the internal users' access as they were at risk of external attack. FISMA specifically directed that IT systems be evaluated using the Risk Management Framework (RMF) created by the National Institute for Standards and Technology (NIST).
This change is more than just a procedural change. It is a system-wide cultural change integrating cybersecurity with the entire enterprise rather than as a wrap-around solution.

The Risk Management Framework (NIST Special Publication 800-37) was originally published in 2010. Since then, it has been revised twice, enhancing the standards for designing, implementing, and monitoring an organization's comprehensive approach to managing, monitoring, and protecting against cybersecurity attacks. Accompanying SP 800-37 are NIST SP 800-53 and 800-53A, which define the policies, practices, and controls appropriate to maintaining a relatively secure operation. These standards have been revised 5 times since their initial publication in 2005 and preceded the release of 800-37 to provide a basis for implementing FISMA-compliant controls.

With the expanding use of cloud technologies, NIST also issued SP 800-171 *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* (and other standards known as FedRAMP) to address authorization of cloud providers to deliver systems with effective underlying security controls that would then be shared by all systems being hosted in the Cloud Service Provider's facilities. This authorization does NOT exempt the agencies from conducting SP 800-37 compliant Assessments and Authorizations for their systems.

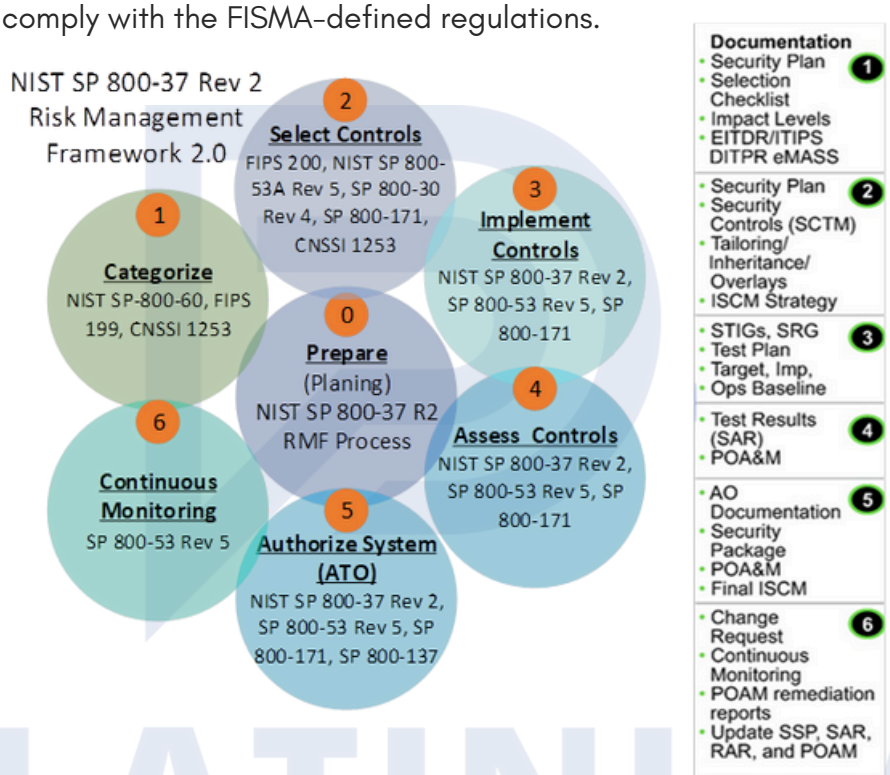
These three documents – the legislation, regulation, and applicable processes and controls – along with the Federal Information Processing Standards (FIPS) 199 for categorizing the security of federal systems provide the standards for conducting Assessments and Authorizations. (A&As).

Conducting the A&A Process

The old C&A process was essentially a system audit conducted every three years. Any action taken between the audit periods was at the agency's discretion. The RMF establishes a lifecycle approach to conducting A&A and monitoring the cybersecurity position continuously.

Assessments & Authorizations (A&A) as a Necessity

Our team takes an enterprise-wide approach to effectively implementing the NIST Risk Management Framework as specified in *NIST Special Publication 800-37 Revision 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy (NIST RMF).* This approach is based on the defined standards and allows our clients to fully comply with the FISMA-defined regulations.



Each phase of the RMF lifecycle has clearly defined standards and related documentation, which can be applied in conjunction with the agency's application development and implementation lifecycle [usually the System Engineering or System Development Lifecycle (SELC/SDLC)].

PREPARE (Organization Level and System Level). We begin by documenting the NIST RMF-defined roles and responsibilities. We develop and/or revise the organization's risk management strategy and risk tolerance. We then conduct enterprise and system-level risk assessments in accordance with NISTIR 8286, *Integrating Cybersecurity and Enterprise Risk Management* (ERM); NISTIR 8286B, *Prioritizing Cybersecurity Risk for Enterprise Risk Management;* and NIST SP 800-30, *Guide for Conducting Risk Assessments.* We develop and/or revise an enterprise continuous monitoring strategy in accordance with NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations.* We collaborate with any Cloud Service Provider (CSP) management to facilitate continued communication about security and privacy requirements between CSP management and our client's senior leadership, program office leaders, mission support leaders, and system owners. We identify all application/system and CSP common controls and develop tailored control baselines per NIST SP 800-53. We then apply enterprise architecture concepts to standardize and optimize security and privacy services. We identify and prioritize mission-critical assets to ensure cost-effective measures are in place to maintain sensitive data's confidentiality, integrity, and availability.

Assessments & Authorizations (A&A) as a Necessity

CATEGORIZE. Platinum's staff collaborates with system owners to ensure the accuracy and completeness of the information system characteristics and technical descriptions. We review information system categorizations based on FIPS 199 and NIST SP 800-60 Volumes 1 and 2. We will validate that the authorization official has reviewed and approved the security categorization for each information system.

SELECT. Platinum staff ensures the system owners have selected the appropriate control baselines and tailored the controls based on NIST SP 800-53 and 800-53A. We determine whether system owners have properly designated system-specific, hybrid (shared with CSP or other agency systems), or standard controls. We validate that controls have been allocated to specific system components. We review and provide feedback on system-level continuous monitoring strategies. We confirm that the authorizing official has reviewed and approved the security and privacy plans.

IMPLEMENT. Our assessors review previous security assessment reports to determine whether controls specified in security and privacy plans are implemented and effective. We also review security and privacy plans to ensure accuracy in selecting appropriate controls based on the FIPS analysis of the system sensitivity.

ASSESS. The assessors develop and review assessment plans to ensure alignment with NIST SP 800-53A. We will assess controls, review assessment reports, note satisfied and other-than-satisfied controls, and determine whether Plans of Action and Milestones (POA&Ms) exist to address each control other than the satisfied control. It is up to the client to determine if the risks presented by unsatisfied controls are acceptable to the agency. An acceptable risk is " evaluated in accordance with accepted practices and for which an informed decision to accept the frequency and consequence that comprise that risk has been made and documented." Platinum typically uses the standards defined by NIST SP 800-39 *Managing Information Security Risk*.

AUTHORIZE. Once the assessment of controls is complete and the documentation has been deemed complete, we will assemble the Authorization to Operate (ATO) package. Platinum assessors work with our client's stakeholders and managers to assemble the complete ATO package, which addresses management, operational, and technical security standards and includes, at a minimum:

- FIPS Categorization Report
- Security Plan, including a selection of security controls with tailoring notes, inheritance from the CSP, and overlays from shared use elements.
- Operational test plan
- Security Assessment Report
- POA&Ms
- Information Security Continuous Monitoring Plan (ISCM).

Assessments & Authorizations (A&A) as a Necessity

We also ensure compliance with agency-specific policies and procedures. The submission is presented to the individual designated as the Authorizing Official (AO) for review, and if it is complete and accurate, the AO will issue the ATO.

Continuous Monitoring. There are two aspects to continuous monitoring, both of which are critical. The first is conducting annual reviews of approximately one-third of the applicable controls under RMF so that all controls have been checked at the end of three years. The full RMF assessment is then conducted again to maintain the ATO. The other is conducting partial or complete assessments if necessary as changes are made to the system, whether through patching or updating. The objective is to ensure that the best possible control is maintained over the system as dynamic changes are made - and that the documentation is kept complete and up to date.

Platinum brings a wealth of experience in managing A&A and the resulting ATO documentation to assist any organization, large or small, in meeting the rigorous requirements of FISMA and protecting mission-sensitive systems and data from cybersecurity threats.