DEFINING RISK MANAGEMENT FRAMEWORK COMPLIANCE FOR CONTRACTORS
“It is not the strongest or the most intelligent who will survive but those who can best manage change.” - Charles Darwin

As cyber threats and attacks continue to increase in scale and impact across organizations of all sizes, cyber security must be considered as a key component to both information security and risk management programs. As alluded to in Darwin’s quote above, those who do not adapt their IT environment and risk frameworks to account for the changing threat landscape may compromise organizational and customer information. Leakage or exposure of information, specifically that of a classified nature, may cause irreparable harm to not only the organization in question, but also to national security.

The U.S. Federal Government has taken notice.

As of January 1, 2018, the Defense Security Service (DSS) now requires that all cleared contractors processing classified information under their watch must fully transition to the new Risk Management Framework (RMF). This new framework establishes a more uniform and consistent approach to managing risk associated with assessing and authorizing information systems. At a high level, the intent of this new framework is as follows:

- Manage risk more effectively and efficiently
- Build trust across the U.S. Federal government
- Establish a common foundation for information security
- Streamline DSS processes

What Does RMF Replace?

The RMF replaces the DSS’s Certification and Accreditation (C&A) process and the Department of Defense’s (DoD’s) Information Assurance and Accreditation Process (DIACAP).

C&A is a federally mandated standard process which requires national security information systems to meet documented security requirements and maintain the accredited security posture throughout their system life cycle. C&A is mandated upon all systems of the U.S. Federal Government and is the required step in order to stand up an information system. The C&A process establishes security configurations, controls, policies, and procedures. It also verifies their correct implementation.

The National Institute of Standards and Technology (NIST) has developed a four-phase C&A process used by the U.S. Federal Government to certify compliance with mandated federal controls. The four phases are as follows:

Initiation & Planning → Certification → Accreditation → Continuous Monitoring

Each phase has a list of C&A activities that must be completed before beginning the next phase.
Why Transition To RMF?

RMF was established by NIST, in partnership with the DoD, the Office of the Director of National Intelligence (ODNI), and the Committee on National Security Systems (CNSS). The purpose of the RMF transition is to develop a common information security framework for the U.S. Federal Government and its contractors in making risk-based decisions.

When discussing the risks associated with an organization’s information systems, considerations must be given but not limited to:

- System security
- Confidentiality
- Data integrity
- Availability
- System compliance with regulatory standards
- Business continuity
- Disaster recovery efforts

Implementation of the DSS RMF will ensure organizations take these risks and considerations in mind when determining appropriate risk mitigation strategies.

This framework is meant to change the way that government contractors assess their information systems, moving away from an archaic C&A process that largely promoted a “check-the-box” mentality. The prior process limited key stakeholders from having significant input in the initial assessment and later management of the risks associated with information systems.

Additionally, this framework is meant to build reciprocity with other federal agencies. By requiring federal agencies and government contractors to adhere to the same risk management standards, trust amongst government stakeholders regarding how information systems are managed will be built via a more transparent, comprehensive, flexible, and strategic process.
RMF Six-Step Process

The RMF has been broken down into six key steps by the DSS and NIST in order to ease this transition.

1. CATEGORIZE Information Systems (IS)
   - Information System Security Manager conducts risk assessment to determine system categorization (confidentiality, integrity, and availability)

2. SELECT Security Controls
   - Information System Security Manager selects security controls and applies tailoring and supplemental controls as needed based on risk assessment. Information System Security Professional reviews system security plan and provides concurrence.

3. IMPLEMENT Security Controls
   - Information System Security Manager implements security controls selected for the information system.

4. ASSESS Security Controls
   - Information System Security Manager conducts self-assessment and updates the system security plan to reflect the actual state of the information system. Information Security Systems Professional reviews submitted system security plan and assesses the information system.

5. AUTHORIZE Information System
   - Authorizing Official determines risk. If acceptable, Authorizing Official formally authorizes system to operate.

6. MONITOR Security Controls
   - Information System Security Manager continuously tracks and reports information system changes to the Information System Security Professional, updating the continuous monitoring plan/strategy.

The figure above outlines the six-step RMP process. Additional information on RMF can be obtained from NIST SP 800-37 “Guide for Applying the Risk Management Framework to Federal Information Systems.”
Categorize the Information System

Each government contractor must categorize an information system based on the following criteria:

- Confidentiality – Confidentiality is categorized based on the impact due to the loss of confidentiality of the information within the information system and provided by the company.
- Integrity – Integrity is categorized based on the impact to the company and DSS if (1) the information system was not operating properly and (2) the information provided by that information system could not be relied upon as accurate.
- Availability – Availability is categorized based on the impact to the company and DSS if the information system or the data that it provides is not available when it is needed.

Companies must assign a value of low, moderate, or high to each category (excluding confidentiality which can only be classified as moderate or high).

For more information on this step, refer to NIST SP 800-30 “Risk Management Guide for Information Technology Systems” for additional guidance.

Select Security Controls

Security controls must be selected from NIST Special Publication 800-53 Revision 4 framework, which maintains a corresponding set of controls to implement based on information system categorization. These controls may be substituted or supplemented by additional controls, as long as risks are mitigated as required by the RMF. Additional control resources based on the information system are provided by the National Industrial Security Operating Manual (NISPOM) and Committee on National Security Systems (CNSS).

Appropriate personnel from each organization must select and agree on a security control set for each information system as well as a plan to continuously monitor the controls they select. The control set for each information system must effectively identify risks and meet applicable security requirements. These controls will be documented in the System Security Plan (SSP).

For more information on this step, refer to NIST SP 800-53 R4 “Security and Privacy Controls for Federal Information Systems and Organization” for additional guidance.

Implement Security Controls

Appropriate personnel for each information system must implement the agreed upon control set, and they may conduct an initial assessment to identify potential weaknesses and deficiencies. Personnel must be qualified to implement the changes, provide measures to note that the control is operating effectively, as well as document the implementation within the SSP.
A Security Assessment Plan and assessment must be completed for each information system’s control set. Any issues, recommendations, or findings must be documented for submission to the DSS. Any remediation actions conducted based on the findings of the assessment should also be documented in the Plan of Action and Milestones (PoAM) document for submission to the DSS.

A Security Assessment Report (SAR) must be generated as a result of the review of security controls, and the SSP should be updated with control status/effectiveness as needed.

Appropriate company personnel must create, review, and submit a security authorization package to the Designated Authorizing Official (DAO) at the DSS. The DAO assesses the security authorization package and issues an authorization decision for the information system—either Authorization to Operate (ATO) or Denied Authorization to Operate (DATO)—which includes any terms and conditions of operation as well as an Authorization Termination Date (ATD) if required.

Each information system must be continuously monitored, tested, and have identified issues remediated in order to keep its authorization status with the DSS/DoD. The continuous monitoring plan/strategy must be formally documented and will be periodically reviewed by those who approved the plan/strategy. The PoAM and SSP should be updated as needed in order to document the latest operating status of the information system.

As noted within the “DSS – Assessment and Authorization Process Manual”:

“Cleared contractors processing classified information under the cognizance of DSS will follow the guidance contained within this manual to complete the RMF process and obtain IS authorization.”

Maintaining compliance and executing the RMF process requires organizations to execute and complete the processes and documents discussed within the six steps previously outlined.
In order to show information system compliance, organizations must produce the following seven key documents to the DSS:

1. Requirements Document
2. Risk Assessment Report (RAR)
3. System Security Plan (SSP)
4. Security Assessment Report (SAR)
5. Information System Security Manager (ISSM) Certification Statement
6. Plan of Action & Milestones (PoAM)
7. Authorization Decision Letter for Signature

These seven documents are required for each information system processing classified information. Those familiar with the C&A process will notice some similarities between the processes. However new terminology is now in place, in addition to new requirements and responsibilities for stakeholders in RMF execution. As compared to the C&A process, the RMF process will require the inclusion of additional artifacts when government contractors submit a security authorization package to DSS.

For organizations that are unable or unwilling to produce the seven key documents noted above, the ramifications to their bottom line will likely be negative, and they may not fully realize the downstream impacts non-compliance may have on their business.

So What If I Don’t Act?

Although the deadline for these requirements was January 1, 2018, these documents do not need to be available to the DSS until your company’s next security vulnerability assessment.

However, by not adhering to the RMF, organizations stand to be non-compliant with DSS standards. This may result in loss of business from government clients until compliance is achieved, resulting in lost opportunities, decrease in goodwill, and reputational impacts.

Also, implementing the RMF will streamline DSS processes to support the authorization of any new information system processing classified information as part of the National Industrial Security Program (NISP), decreasing time to begin working on new engagements.

Don’t let inaction or hesitation on meeting government requirements impede continued business for your organization. Taking initial steps to implement the RMF will not only put you in the right direction for compliance, but it will also strengthen your organization’s internal information security and risk management programs.

Now is the time to start promoting synergy across all DSS stakeholders and begin the transition to the RMF. Selecting a firm with rooted knowledge in the organizational change requirements to assist is often the best first step organizational leaders can make.
How Aronson Can Help

While the RMF steps outlined above may be considered vague as to what is acceptable, Aronson has dealt with this transition before. Our team has the necessary expertise to ease the burden of the transition to the RMF and help your organization navigate:

- What is acceptable to the DSS
- What documents are required to be in compliance
- How to expertly compose these documents
- The NIST frameworks that drives the change in compliance requirements

We have the ability to effectively assist you with this transition, while allowing you and your organization's personnel to focus on what's important: your core business.

By attempting to make this transition on your own, you may risk inconsistency and inefficiency across departments which ultimately drives increasing costs and greater risks to your company as a whole. Our consistent approach will minimize the disruption to your business and reduce the risks associated with making changes to your information systems and internal controls if necessary. **Let our experienced team provide guidance on how to achieve RMF compliance.**

**INTERESTED IN LEARNING MORE?**

**FOR MORE INFORMATION, CONTACT PAYAL VADHANI, LEAD PARTNER OF ARONSON’S CYBERSECURITY, RISK & COMPLIANCE PRACTICE, AT PVADHANI@ARONSONLLC.COM OR 301.231.6259.**

**About Aronson LLC**

Aronson LLC provides a comprehensive platform of assurance, tax, and consulting solutions to today’s most active industry sectors and successful individuals. For more than 55 years, we have purposefully expanded our service offerings and deepened our industry specialties to better serve the needs of our clients, people, and community. From startup to exit, we help our clients maximize opportunity, minimize risk, and unlock their full potential. For more information about Aronson LLC, please visit www.aronsonllc.com or call 301.231.6200.