Why Does the Department of Defense (DoD) Risk Management Framework (RMF) Process Fall Short of Expectations?

Dr. Laurent Boucard, CISSP, KBR, Inc.; Brian Taylor, CISSP, KBR, Inc.; Blaine Dawson, KBR, Inc.; Gerald Beuchelt, CISSP-ISSAP, Sprinklr, Inc.; Charles Kelleher, CISSP, KBR, Inc.

Abstract: This paper discusses the current RMF cybersecurity framework used to assess and authorize sites or systems. The authors used a participant-observation methodology to obtain data points and regressed those findings with informal interviews. The findings suggest that there are many issues associated with RMF, but the biggest issue is that senior leadership appears unaware that RMF is an exercise in compliance vs. a risk reduction effort. Some of the key issues identified demonstrate a lack of empowerment, training, and compensation of CyberSecurity personnel combined with military processes which seeks compliance rather than evaluation of risks.

Introduction

> *Dr. Tim Rudolph (USAF AFLCMC CTO): "The systemic problem with RMF was that it became a checklist exercise, whether controls made sense or not, or if real risk was considered or not. This established a bureaucracy on the system side to produce artifacts for the checklist and a bureaucracy on the certification side which was antagonistic about the checklist items. "No" was the natural answer vs how can we collaborate to improve our cybersecurity posture."*
>
> *John Weiler (Executive Director Information Technology Acquisition Advisory Council – ITAAC): "NIST's RFM is a comprehensive body of work that is challenging most federal agencies due to both the complexity of the framework and the lack of qualified expertise leading to outsourcing of its many functions. This has led to increased conflict of interests with the same companies performing the audits also managing the systems. Worse, a focus on compliance vs measurable outcomes has driven up cost and risk at the same time. I saw this during my tenure in the CMMC1.0 and within FEDRAMP as well."*

The philosophy of the Department of Defense (DoD) Assessment & Authorization (A&A) process is analogous to what private sector companies do to assert compliance. Audits provide board of directors and investors a level of assurance that a company's internal control systems follow generally accepted principles. Audits are mandated in the accounting world audits by the Generally Accepted Accounting Principles, (GAAP) and by the Sarbanes-Oxley (SOX) bill of 2002 for public companies in the financial sector. To address security for the information systems of public companies, the IT general controls (ITGC)[1] provide a framework to secure boundaries. Within the DoD realm, the A&A framework aims to provide confidence that systems (or sites) deploy levels of IT security proportionate to the system Confidentiality, Integrity, and Availability (CIA) requirements. This is called the CIA triad.

Like its predecessor, the DoD Information Assurance Certification and Accreditation Process (DIACAP), the National Institute of Standards and Technology (NIST) - Risk Management Framework (RMF) process leverages DIACAP findings to add a stronger integration with a System Development Life Cycle (SDLC), a renewed focus on Reciprocity, FISMA reporting compliance, a common language within agencies and components, easier system categorization, one standard for all (NIST Special Publication (SP) 800-30 – Guide for conducting Risk Assessments[2]), a continuous

[1] ITGC: https://en.wikipedia.org/wiki/ITGC
[2] NIST SP 800-30: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

monitoring system and a standard control set (NIST SP 800-53[3]). The DIACAP process is shown below in Figure 1 (below) and the RMF process is shown in Figure 2 (below). RMF is defined in the NIST Special Publication (SP) 800-37 Revision 2 and the general framework and references are provided in Appendix 1.

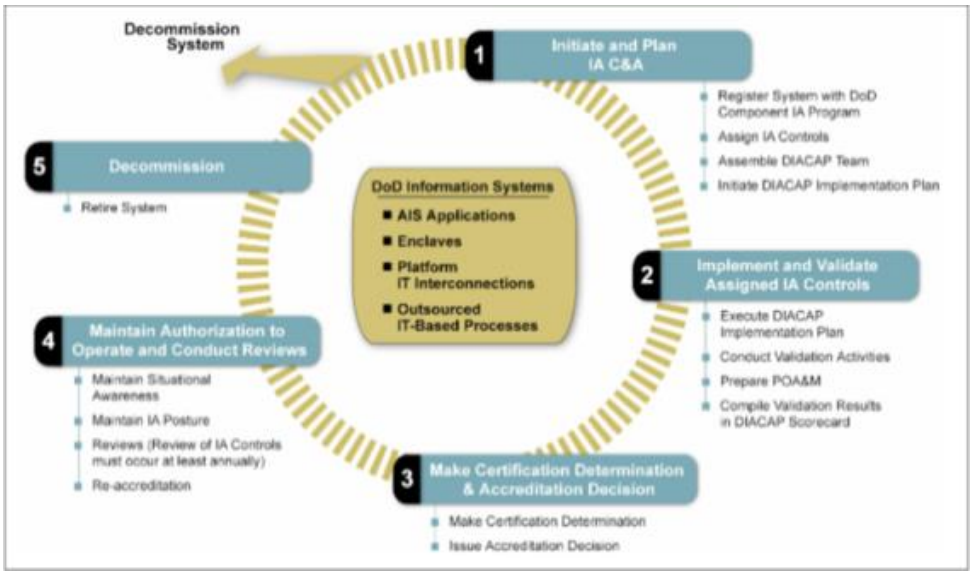

Figure 1: the DIACAP process[4]

Figure 2: the NIST RMF process[5]

[3] NIST SP 800-53: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
[4] DIACAP: http://www.prim.osd.mil/Documents/DIACAP_Slick_Sheet.pdf
[5] RMF: https://csrc.nist.gov/projects/risk-management/about-rmf

RMF[6] works with three main teams: an engineering team produces and maintains an Authorization To Operate (ATO) package. This package contains technical test results (such as individual Security Technical Implementation Guides (STIG)[7] results and automated Assured Compliance Assessment Solution - *ACAS*[8] scans), document inspections (such as network diagram and hardware list) and interviews (with site personnel). This "artifact" demonstrates the compliance status in terms of CIA. This team works under the authority of a site (or system) Information System Security Manager (ISSM) to produce the package. Next, an audit team, comprised of one or more Validator(s), independently asserts the accuracy and completeness of the package. To do that, validators conduct an audit to gather independent test results. Once validators complete their reviews, they forward the package to decision makers. Those individuals are normally comprised of a Security Control Assessor (SCA) and his/her Representative (SCA-R) who will review the package for accuracy and possibly return it to the engineering team if he/she deems the product quality or risk unacceptable. Once the SCA-R is satisfied, the package gets routed to a SCA who will review and forward to the Authorizing Official (AO) for official approval of the package.

The problem:

Armed with many years of experience in the field, the authors observed a discrepancy between the RMF intent and what is done in practice. The authors noted that while RMF aimed to improve security by adding several new controls, RMF became a mandatory compliance checklist rather than a tool aimed at deploying a level of security commensurate with CIA requirements. The next problem is that there appears to be a huge discrepancy between senior leadership and individuals working A&A. While practioners will overwhelmingly assert that RMF is a cumbersome exercise in compliance; senior leadership may see those efforts as effectively reducing risks. While RMF helps to secure baselines, RMF is a complex, expensive and time-consuming process that should be tailored as NIST recommends.

Choice of Research Methodology:

Armed with the above postulate, the authors debated the best methodology to obtain data points to discuss what is not working in RMF. It was quickly decided that discussing what works (such as creating processes, enabling Change Control Boards - CCB, writing policies and training) would be out of scope, since the point of this paper is to discuss what does not work. After discussing techniques to obtain datapoints, it became apparent that gathering official data from DoD sites could be problematic. As a result, the authors determined that the best technique to assess the effectiveness of the RMF framework is to use the Participant Observation methodology. This technique allows for observations made by individuals immersed in the day-to-day activities to record observations. Since the authors come from diverse backgrounds, worked on different projects, and have years of experience in the field, this methodology appears valid in its approach. After discussing past experiences, the authors created the following datapoints for discussion.

Datapoints:

> **Example 1:** An acquisition Program Manager (PM) challenged the need to implement Cybersecurity. He argued that Cybersecurity would unduly delay the program timeline and Cybersecurity requirements were not required from a contractual perspective (Statement of Work - SOW or in the Contract Data Requirement List -CDRL). Once it was clarified that Cybersecurity was a mandatory requirement, the PM tried to fire Cybersecurity individuals that did not put the program needs first and hire individuals who would follow orders. This behavior is also frequently seen in immature, high-growth, or resource constrained projects (including commercial).

[6] Congressional Research Center: https://crsreports.congress.gov/product/pdf/IF/IF10537
[7] STIG https://public.cyber.mil/stigs/
[8] ACAS: https://en.wikipedia.org/wiki/Assured_Compliance_Assessment_Solution

Example 2: A manager of a large DoD research facility observed that DIACAP process took a long time. He collected metrics to demonstrate that a problem existed, and he developed his own approach to doing RMF. With some cursory knowledge about the "Agile Methodology", he implemented an "Agile" process tailored to his needs where ATOs were obtained quickly. He further decided to simplify his baseline by averaging site classification levels (formerly MAC levels) to average costs and simplify work. When challenged, the manager stated that failure to secure a system would not get a person in jail while failure to achieve success would get people fired/demoted. The manager further challenged the Cybersecurity team to verify with law enforcement that failure to implement security was not a criminal offense and this was verified to be accurate. Again, behavior like this is often observed in commercial entities, especially where contracted compliance adherence (e.g., PCI-DSS or SOC2) must be implemented within short timelines.

Example 3: A lead Information Assurance (IA) engineer/architect for a large acquisition program (Acquisition Category - ACAT1) described his approach to developing security as follows: "First we look at the controls selected by the categorization of the program. We buy or build components for each control based on the description. Once these are in place the system is secure." As a result of this checklist approach, there was no evaluation of program-specific threats. Tools were acquired to comply with controls without an overall plan which meant that the system was not cost efficient or well designed. In addition, there was no overarching plan to hire individuals capable of using those tools once the project went live.

Example 4: A site frequently received from its Command new tools without any prior coordination or consideration for Cybersecurity. One example was a communication device which allowed concurrent data communication of networks of different classifications. While doing so is possible, the device required a TEMPEST evaluation. Failure to plan lead to a 24-month delay in the tool implementation. A common comment from leadership was that Engineering oversaw problem solving and that Cybersecurity should secure what was given to them. Questions about "leadership intent" were irrelevant.

Example 5: Prior to an inspection, a site decided to remove most servers/switches/routers from the baseline and apply all possible security settings. While the devices were perfectly secured, none of the devices functioned as intended. The inspection team commended the site for its exceptional security performance, while operations were put on pause during the inspection.

Example 6: A Cybersecurity manager turned in an ATO package to the validators that only assessed Red (critical) and Yellow (urgent) controls. That approach ignored white controls (good to fix) so that the workload would be reduced to evaluating 181 controls out of 518. The manager rational was that RMF being about Risk, timelines being short, personnel being not trained (or available) and resources not being available, the site had to prioritize its work based on the constraints. The SCA-R and SCA declined that approach and warned the site could be disconnected if an ATO was not submitted on time.

Example 7: Sites are often observed that cybersecurity responsibilities were transferred away from the base to the responsible system/site. As a result, sites/systems are now responsible for obtaining ATO's without much notice, personnel, or training. Because RMF requires an Information System Security Manager (ISSM) and a Chief Information Officer, frequently people with limited experience get put in place to fulfill requirements. This often leads to enlisted being put in positions of power where they *should* be able to tell senior officers what is acceptable (and not). Similarly, the person that appoints the ISSM (the CIO) are frequently a junior Officers (O1-O3) with basic manager training but without much training in Cybersecurity. It was further observed that several CIO's resent enlisted powers as ISSM resulting in conflicts and delays.

Example 8: Sites often experience a high turnover of personnel as the result of low wages and contract uncertainties. Short staffing mean that many IT workers must work from high priority items to the next. Few individuals understand the concept of "boundary/site/enclaves", or update the documentation as required in a timely fashion. As a result, at the time of the ATO, it is not uncommon for site personnel not to understand what is in the boundary. At the same time Vulnerability (ACAS), or Mapping (Tannium, NMAP, FPing, AD queries) scans do not always align with the hardware list and/or boundary diagram. Similarly, policy documents may not be current. Those observations were made at multiple locations.

Example 9: A SCA-R became a bottleneck in some ATO processes by focusing on grammar and spelling in packages instead of focusing on technical issues. Another SCA-R was not knowledgeable about Agile and would not endorse any efforts aimed at rapid development. Similarly, some validators have been found not to be competent on technologies that they were tasked with evaluation resulting in issues when the SCA-R reviewed the package.

Discussion

The first note is that A&A is critical to protect unclassified DoD systems. Unclassified is often mistaken to mean that there is nothing of value in such systems. To the contrary, "For Official Use Only" (FOUO) and its replacement the "Controlled Unclassified Information" (CUI) marking indicate items that have a value and should be protected. Cybersecurity aims to protect the data, system, networks, and site(s) from intentional or unintentional actions committed by individuals (including foreign adversaries, criminals, activists, or insider threats) in accordance with the CIA level of the system.

Challenges:

1) At the DoD level:

- The ATO is a snapshot in time:
  - This snapshot may take a few weeks or months to capture, but during this time changes should not occur to ensure the snapshot is representative of the instant "T" where the snapshot was taken. This means that in presence of changes, the package is unlikely to fully represent the baseline, and this will create issues with the next accreditations because of a lack of documentation. In the commercial world, when completing a SOX assessment or within a SOC1/2/3 report, the assessor makes the clear distinction between Type 1 (static assessment of control system) and Type 2 (control effectiveness, sampling over time) tests.

- IA controls contained in RMF are not interpreted and implemented consistently across the Defense Enterprise:
  - No overlapping guidance: There is no detailed written overlapping DoD guidance as to how to interpret and implement controls. As an example, some may interpret that a control cannot be implemented because there is no need for a budget (all procurement conducted by an agency). Others will assert compliance with the RMF checklist is mandatory, therefore the control should be not compliant in the absence of a budget. That position aligns with the position of many validators, SCA-R, SCA, and AOs, but the intent of RMF was to make something highly customizable instead of a checklist.
  - As shown in example 9, it appears that some individuals are placed in positions of authority but are not sufficiently versed in the technologies they are asked to evaluate.
  - Software, for example, can receive an ATO, and yet be required to be evaluated by the NSA or Common Criteria (CC) to be used by another branch/agency. DoD branches apply different standards in terms of source code analysis or runtime assessments. As a result, software security varies based on the agencies/branches. There are cases where software is first "approved" before finally needing an assessment which may take upwards of two years (the underlying problem being that unskilled personnel gave a first thumb up).

- Changing threats:
  - Lack of "Crown Jewel" analysis: RMF has standardized the approach to risk and there is no real customization based on location, environment risks, human threats, and mission to determine what needs to be protected or what is an acceptable level of risk. This Crown Jewel approach had been

championed by the MITRE TARA[9] work, and has recently seen similar interest in the commercial sector through companies such as Gartner in their Risk-Value Analysis (RVA) approach
    - Rapid changes: The rapidly changing environment does not allow for a dynamic control environment based on adversary tactics. Adversaries have been known to commonly exploit perceived security networks, even those that have gone through a full ATO process. Exploits (such as zero-day) known to other State Nations may not be known to the DoD, allowing them to access sites perceived secure network[10].
    - Static framework: Under RMF, risks are effectively evaluated against static frameworks that are based on a generic point-in-time threat landscape.
    - Rigid system: From the moment a risk is identified, the authors observed that it can take 12-18 months for a mitigation to be created, tested, and approved before it can be pushed to a system. DoD is not able to fix most of these risks because issues mostly relate to private companies' equipment/software.

- Contracts: Security requirements are not typically built into the contracts.
    - Legalities: Some Project Management Offices (PMO) or contracting personnel will assert that Contract Data Requirements List (CDRL) and Statement Of Work (SOW) are the only mandatory requirements. While that assertion as some legal basis, individuals holding a DoD security clearance are obligated to protect the information that they are entrusted with as a condition of employment. The underlaying issue is the lack of consequences for failing to implement Security. This was observed in Example 2.
    - Lack of involvement of key personnel: Security Engineers and ISSMs are inadequately involved with the Request For Proposals (RFP) or Request For Quotes (RFQ). Consequently, security and the C&A process are improperly considered in the Initiation phase of the project. Consequently, the SOW may be flawed with incomplete or inadequate requirements which lead to problems throughout the project lifecycle. In practice, unless Cybersecurity is baked in early in the development, the project will struggle to implement cybersecurity.
    - Contracting length: ACAT I program may take five to ten years between the initial RFP and the development of the solution. By the time the tools are developed, they no longer are current in their engineering and/or cybersecurity.
    - Contracts are not typically agile: Because contracts typically define needs at an instant "T", the threat landscape is not adequately part of the contract resulting in a gap between what is built and what is needed. Targets change, but contracts do not easily change! While some programs do implement agile, more efforts should be made to change the acquisition mindset to be Agile.

- Lack of cybersecurity enforceability:
    - Aside of willingly broadcasting secrets to a foreign nation or news agency, punishment for failing to implement security is unlikely to result in a clearance termination, loss employment or incarceration.
    - Without enforcement mechanisms, some Program Managers may be willing to compromise the security of a system to make their projects move forward. This can relate to the work of Dr. Hare, and Matthieu that suggests that some managers may be willing to take more risks than the rest of the workforce.
    - Part of the problem is that under the Committee on National Security System (CNSS) 11, 22, 1253 and 4009, the only individual legally responsible for the security of the system is the AO. It would be urgent to make the PM and ISSM legally responsible.

- Military culture:
    - Military personnel are often allocated based upon program needs with limited regards to experience or qualifications[11]. This results in situation where junior officers can become responsible for large programs they are not always qualified or experienced to lead. Similarly, enlisted staff may end up designated as ISSM to fulfill regulatory constraints (example 7). This may lead to challenging situations where a contractor may tell an enlisted ISSM to sign a document he/she does not comprehend and the enlisted ISSM in turn instructing senior officers.

[9] "Threat Assessment and Remediation Analysis (TARA)", J. Wynn, MITRE, 2014, https://www.mitre.org/publications/technical-papers/threat-assessment-and-remediation-analysis-tara
[10] Cybersecurity: Selected Cyberattacks, 2012-2021https://crsreports.congress.gov/product/pdf/R/R46974
[11] Slashdot, USAF CSO quits: https://tech.slashdot.org/story/21/09/03/2038217/us-air-force-chief-software-officer-quits

- The situation is similar with senior and general officer ranks where some commanders are put in charge of functions that they are not trained to understand. As a parallel, if most general officer are not trained to make medical decisions, they are equally not proficient to make engineering or cybersecurity decisions.
- Military personnel are typically the key decision makers. Lt. Gen. Duke Z. Richardson, the Air Force's senior-most military acquisition officer[12] stated in the Air Force Magazine that "The folks that are working on a lot of these projects are pretty darn astute…". While it is undeniable that many senior military individuals are exceptionally smart, being smart does not make a person trained/qualified in Cybersecurity.
- Military personnel are typically assigned to a project for 2-4 years, while projects may last for years. This means that by the time the person is up to speed, it is time for a Permanent Change of Station.
- Checklist mentality. As was observed by some, some military members want CyberSecurity Checklists. While this approach may work on some systems or sites, Cybersecurity is an evolving field where threats change and the limited fiscal budgeting should lead personnel to focus attention to items with the best Return On Investment (ROI).

- Should all Controls and STIGs be applied blindly?

  - Back in 2012, Bellomo and Woody[13] already asked the question but this important question has not been addressed to this date. Ron Ross from NIST clearly stated during discussions with the authors that RMF should be a guideline. In practice, most individuals in the ATO package chain equate RMF as a mandatory checklist that focuses on compliance vs. risk.

2) Manpower

- Cleared personnel:
  - There is a lack of available cleared individuals. FCW[14] reports that between 2013 and 2021, the pool of DoD cleared individuals as "plummeted by 17%". FCW reports that $10 Billion is lost because contracting companies cannot hire uncleared personnel. This observation is even more striking when some contracts require individuals to be cleared to the Secret level when their work is unclassified.
- Certification:
  - To work in DoD CyberSecurity a CompTIA -Security+ certification is the minimum requirement, but the golden certification is the Certified Information Systems Security Professionals (CISSP). Wikipedia[15] reports that there are 152,632 CISSP individuals in the entire world. In comparison, Cybercrime[16] magazine reports "Nationwide, there are just over 90,000 CISSPs…", "…according to CyberSeek, but more than 106,000 job openings require the CISSP certification, our industry's gold standard. Or consider CISMs (Certified Information Security Managers), with just 17,000 people holding the credentials but nearly 40,000 advertised jobs requesting them."
- Salaries:
  - DoD Cybersecurity salaries are low compared to equivalents. A search conducted on Zip Recruiter[17] on Feb 02, 2022, indicated an average salary for "RMF Boston" personnel of $105,000 with minimum of $58,875 and a maximum of $153,939. In comparison, Randstad[18] reported a $144,012 salary for a Security Engineer ($124,000 to $185,158) annually with a Python Developer would commend a $155,895 salary ($120,246 to $182,143). These figures can be considerably higher in high-cost regions such as Silicon Valley or New York City. Clearly, DoD contracting personnel are underpaid compared to the private sector (example 7, 8). This observation added to notes from education sites such as Coursera[19] appears to show a pattern where Cybersecurity jobs pay less then software development

[12] US Airforce Mag "USAF CSO quits": https://www.airforcemag.com/air-force-software-chief-quit-officials-considering-recommendations/
[13] SEI: *www.**sei**.cmu.edu/reports/12tn024.pdf*
[14] Security Clearance: https://fcw.com/acquisition/2021/06/security-clearance-demands-are-exploding-and-government-must-keep-up/258405/
[15] Wikipedia on CISSP: https://en.wikipedia.org/wiki/Certified_Information_Systems_Security_Professional
[16] Cybersecurity jobs: https://cybersecurityventures.com/jobs/
[17] Zip recruiter: https://www.ziprecruiter.com/Salaries/RMF-Salary-in-Boston,MA
[18] Randstad: https://www.randstadusa.com/salary/cyber-security-engineer-salaries/boston-massachusetts/
[19] Coursera : https://www.coursera.org/articles/it-salaries-roles-location-and-experience

jobs. This situation is in the authors opinion abnormal when Software Development is one of the 8 domains in the CISSP examination. May be because of those low wages, many Cybersecurity folks will quit the DoD security realm in pursuit of better paying jobs.

- Training:
  - While a CISSP requires 40 minimum hours of continuing education per year, the DoD does not typically provide time for its contractor, military, and civilian workforce to pursue educational purposes. In a field that evolves at high speed, this leads to people either not maintaining their certifications or having to make difficult choices in terms of work balance.

  - Reimbursement of training: The IRS[20] has a current $5,250 annual capstone as to how much education can be reimbursed by an employer. With graduate program frequently costing more than $60,000[21], employees face the difficult choice of to invest in their career or use the money for other purposes. Similarly specialized training such as SANS[22] classes frequently cost more than $5,000 for a single class. This leads to a gap between those who will keep investing at their own cost in training vs. those who will chose not to update their skills to match emerging technologies, trends, and threats.
  - Reimbursement of certifications: With employers frequently requesting that employees hold multiple certifications, the cost of being well certified can be high. Sadly, a minority of companies pay the annual maintenance fees and employees face the difficult choice of letting certs expire of paying out of pocket. It was also observed that individuals were approved to take training subject to the above IRS education capstone, but the annual maintenance fee is not covered as "education" therefore after a year, many companies do not reimburse for certification they potentially asked their employees to take.

3) The RMF process "a snapshot in time":

- While a focus is on compliance, unless in major acquisitions (ACAT I), there is no Testing and Evaluation (T&E) to ensure that the package is functioning. As a result, some entities will lock the system to ensure they pass the inspection while the systems are not functional.

4) Agile A&A is very difficult:

- Agile software development process is being used more frequently within DoD. Agile software development has proven to be a very effective methodology in developing software[23] and it is here to stay. Agile works well in software development, but it is unlikely to work well in the A&A process (unless the A&A process is changed from being a snapshot in time to being a dynamic process).
- It is built on the premise that software development can iteratively build tools that fulfill a need. It utilizes a concept called sprints which are normally 1-4 weeks long. During that process a backlog of products (as well as new goals) are constantly re-prioritized. This means that requirements can change and that we can learn to continuously improve delivery and the flow of delivery.
- Can A&A and Agile co-habit? While software development and Agile can cohabit well, in systems or sites, A&A requires the examination of a finished product. Small incremental steps would have to be iteratively aligned and tested across the entire project. This difficulty in implementing Agile was discussed in various research articles such as the one from Carnegie Mellon University Software Engineering Institute (CMU-SEI)[24].
- In a waterfall acquisition model, a complete onsite validation effort of a large project may take upwards of 15 cybersecurity people, 6 weeks, 6 days a week for 14 hours a day and weeks of work post site validation. During those times, the system should be frozen. In an agile acquisition process, the existing RMF process would need to allow for validators to iteratively review and approve sprints (such process would require more validators and cost additional fess).
- In an Operation and Maintenance (O&M) model, there are no iterations, therefore the waterfall model is best when sites are not capable of the Continuous ATO. Levels of efforts like those above.

[20] IRS: https://www.irs.gov/newsroom/tax-benefits-for-education-information-center
[21] US News: https://www.usnews.com/education/best-graduate-schools/paying/articles/is-graduate-school-worth-the-cost
[22] SANS: https://www.sans.org/cyber-security-courses/
[23] Standish Group: https://www.standishgroup.com/
[24] SEI: http://www.sei.cmu.edu/reports/12tn024.pdf

- In software development, agile is possible with small sprints (2-6 weeks), using static code analysis tools (such as Fortify), and when conducting functional testing to assert that the product works.
- AO decisions are based upon a careful analysis of artifacts that demonstrate how a system complies with DoD requirements. To do that, artifacts such as network diagrams, software and hardware lists, list of Ports, Protocols and Services (PPS), Memorandums Of Understanding (MOU), Disaster Recovery plans are created to provide evidence. This documentation process is not easily compatible with Agile process in dynamic systems.
- Agile requires testing: and more specifically automated testing[25]. This is very difficult in A&A because testing must be done on a complete system.
- Agile Incremental testing is inconsistent with DoD Acquisition framework testing milestones of Developmental Testing and Operational Testing of complete systems.
- While automated tools allow for many checks to be automated, in practice, a large part of RMF effort consists of manual checks.

5) Need to produce quicker and cheaper:

- Pressure from senior managers combined with a lack of legal consequences for poor management decisions lead some ISSM's to make poor decisions in terms of the security posture of the system. Each update to the system should trigger a review and potentially a re-accreditation.

6) Over-evaluation of CIA levels and blind application of overlays may create unneeded work:

- While a site may have a CIA level of Medium-High-Medium designation (because of overlays), site leadership may plan to cease operations in the event of a catastrophic event. A medium level of availability defined during the RMF System Categorization process is not compatible with a business decision to cease operations in the event of a disaster. Certainly, a fear of under categorization, going against senior DoD personnel desires or changing the status-quo can lead to a costly and time-consuming over-categorization.

7) Continuous monitoring:

- Rules have only been published recently regarding Continuous-ATO in unclassified systems. While Continuous ATO is possible, they will require an ongoing monitoring of threats that most sites and systems will not be equipped to handle. Continuous monitoring will be requiring the hiring of new staff to document systems, monitor threats, and conduct tasks which may be currently ignored because of a lack of personnel. As a note, FedRAMP has continuous monitoring process defined.

Outlook

As Murdoch[26] mentioned… Certifications fail. What could be done to improve the process?

1) The first suggestion would be to create a universal lexicon that provides clear and unique direction about what each control means, what artifacts are required (what makes the artifact acceptable or not), etc. As an example, questions are often raised as to what constitute a mission essential or mission critical site/system.
2) The second suggestion would be to create metrics for validators, SCA-R, SCAR, AOs with grades like what the US Navy currently does. This would allow for performance metrics.
3) The third advice relates to personnel understanding the Determine Categorization (DETCAT) in RMF Step 1, which can and does result in over classification, for example rating an overall system, as High-High-High when the risk level may be closer to Low-Low-Low. This creates a situation where risks may need to be downgraded to meet the real associated risk. This downgrading creates extra work and takes time, adds personnel labor costs, and has schedule impact in extra time to process the information and present the downgrade information to the SCA and AO.

[25] SEI Agile CyberSecurity: https://resources.sei.cmu.edu/asset_files/whitepaper/2013_019_001_70236.pdf
[26] Murdoch & al, : http://www.cl.cam.ac.uk/~rja14/Papers/ieeesp12warereport.pdf

4) The fourth advice is to require that RMF - Step 3 include a threat analysis step to determine site/system specific risks. This would allow for a customization of controls relevant to the site or system. This is already required for Continuous ATOs.
5) The fifth advice is to Implement Agile Contracting with a focus on delivering small working products that are iteratively improved/developed based on a budget/timeline.
6) Concurrently to suggestion 5, embed validators in the System Development Life Cycle so that solutions are immediately approved. This would be more costly in terms of having a dedicated onsite validator reviewing large projects, but it would dramatically lower risk since solutions would be approved as developed by the Agile team.
7) The sixth advice would be to make security in DoD projects mandatory with possible fines and criminal libaility for actions such as deliberate declassifying of information, failure to implement security or circumventing security.
8) The seventh advice would be to place trained individuals in charge of cybersecurity. While it is possible for someone with no formal IT education to thrive through hands on learning, management of cybersecurity programs should be limited to people that received formal IT and management training to ensure that security is baked in the programs. Those individuals should be empowered at an equivalent senior military level to an O5-O7 position to ensure that cybersecurity managers can direct all command personnel regardless of civilian or military roles. In the absence of trained individuals, it may be necessary to put DoD civilians or contractors in charge.
9) The eighth advice is to dramatically increase Cybersecurity salaries. Cybersecurity staff should receive a higher salary than developers. Many talented individuals learn Cybersecurity with the DoD then quit to work in the private sector with frequent 100% pay bumps. DoD needs to motivate the brightest to work for the DoD.
10) The nineth advice is to mandate a minimum two weeks of annual training for each cybersecurity worker (military, civilian or contractor) to ensure that the DoD has people adequately trained. Ideally allow 4 hours weekly for training so that people's skills stay relevant.
11) The tenth advice is to conduct a review of all manning requirements / skill requirements for contracts supporting RMF activities. Overall, there appears to be a severe shortage of both trained personnel and duty positions listing the requisite skillsets to support RMF activities. With RMF adding new controls such as Supply Chain controls, a deeper focus on Personal Identifiable Information (PII) and health information, there is a need for qualified people in the DoD.
12) The eleventh advice is to further standardize core RMF documents for similarly sized and managed systems allowing DOD Cybersecurity personnel to spend more time effectively managing risk rather than filling out checklists and repetitive tasks.

Conclusion:

While RMF is a step up from DIACAP, it is critical that key decision makers realize that RMF has become a checklist vs. the NIST intended risk reduction tool. To improve security, several recommendations were made, and more research would be warranted to determine what improvements would be beneficial in today's fiscal environment.

Appendix 1:

RMF comes as a response to Executive Order 13800[27] (Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure), OMB Circular A-130[28] (Managing Information as a Strategic Resource), OMB Memorandum M-17-25[29] (Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal

[27] 82 FR 22391: https://www.govinfo.gov/app/details/FR-2017-05-16/2017-10004
[28] Circular 130: https://www.cio.gov/policies-and-priorities/circular-a-130/
[29] White House Circulars: https://www.whitehouse.gov/omb/information-for-agencies/memoranda/

Networks and Critical Infrastructure), and OMB Memorandum M-19-03[30] (Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program). RMF relies on several NIST Special publications to provide guidance. This includes SP 800-39 (Managing Information Security Risk: Organization, Mission, and Information System View[31]), SP 800-16 (Information Technology Security Training Requirements: a Role and Performance-Based Model[32]), SP 800-50 (Building an Information Technology Security Awareness and Training Program[33]), FIPS 200 (Minimum Security Requirements for Federal Information and Information Systems[34]), SP 800-47 (Managing the Security of Information Exchanges[35]), NISTIR 8212 (ISCMA: An Information Security Continuous Monitoring Program Assessment[36]), SP 800-137 (Assessing Information Security Continuous Monitoring (ISCM) Programs: Developing an ISCM Program Assessment[37]), NISTIR 8011 Vol. 1-4 (Automation Support for Security Control Assessments: Software Vulnerability Management[38]), SP 800-128 (Guide for Security-Focused Configuration Management of Information Systems[39]), SP 800-12 (An Introduction to Information Security[40]), NISTIR 8023 (Risk Management for Replication Devices[41]), SP 800-60 (Guide for Mapping Types of Information and Information Systems to Security Categories[42]), SP 800-18 (Guide for Developing Security Plans for Federal Information Systems[43]), FIPS 199 (Standards for Security Categorization of Federal Information and Information Systems[44]), and SP 800-59 (Guideline for Identifying an Information System as a National Security System[45]).

Acknowledgments:

The authors would like to thank Darrel Skubinna CISSP, Chuck Kelleher CISSP, Erich Kron CISSP, Chris Esquire JD, CISSP, Michael Duplantis, Dr. Tim Rudolph, Nicolas Chaillan, Dr. Michael Klipstein, Jim Geurts, John Weiler, Mark Rodrigues, John Barrett, and Dr. Tina Burton for their inputs.

Biographies:

Dr. Boucard is an experienced CyberSecurity Professional who has been supporting US Army, US Navy, US Airforce, and NATO CyberSecurity efforts for the last two decades. The recipient of three Master's degrees, a Doctorate and multiple IT certifications, Dr. Boucard leverages his academic and professional experiences teaching a wide range of topics such as Financial Management, Project Management, IT Security, Database Security, cybersecurity, and Network Security at different Universities. Dr. Boucard can be reached at KBR at laurent.boucard@us.kbr.com

Mr. Taylor is a successful Senior Cyber Security professional with a Master of Science degree in Information Technology and a Certified Information System Security Professional (CISSP). He has broad experience in complex DoD Weapon systems such as aircraft, ground-based Weapon Systems and coalition partner networks, SCADA Systems and Industrial Control Systems, medical device Cybersecurity, and commercial security IT cybersecurity. Mr. Taylor can be reached at KBR at brian.taylor@us.kbr.com

[30] White House Circular M-19-03: https://www.whitehouse.gov/wp-content/uploads/2018/12/M-19-03.pdf
[31] NIST SP 800-39: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf
[32] NIST SP 800-16: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-16.pdf
[33] NIST SP 800-50: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf
[34] FIPS 200 https://csrc.nist.gov/publications/detail/fips/200/final
[35] NIST SP 800-47: https://csrc.nist.gov/publications/detail/sp/800-47/rev-1/final
[36] ISCMA: https://csrc.nist.gov/publications/detail/nistir/8212/final
[37] NIST SP 800-137: https://csrc.nist.gov/publications/detail/sp/800-137a/final
[38] NISTIR 8011 : https://csrc.nist.gov/publications/detail/nistir/8011/vol-4/final
[39] NIST SP 800-128: https://csrc.nist.gov/publications/detail/sp/800-128/final
[40] NIST SP 800-12: https://csrc.nist.gov/publications/detail/sp/800-12/rev-1/final
[41] NIST SP 800-12: https://csrc.nist.gov/publications/detail/sp/800-12/rev-1/final
[42] NIST SP 800-60: https://csrc.nist.gov/publications/detail/sp/800-60/vol-1-rev-1/final
[43] NIST SP 800-18: https://csrc.nist.gov/publications/detail/sp/800-18/rev-1/final
[44] FIPS 199: https://csrc.nist.gov/publications/detail/fips/199/final
[45] NIST SP 800-59: https://csrc.nist.gov/publications/detail/sp/800-59/final

Mr. Blaine Dawson is a long standing Senior Cyber Security professional who has worked in all classification levels of the DoD implementing Cyber Space Security in RMF. He is currently a Cyber Warfare Officer for the Idaho Air National Guard and KBR Senior Cyber Security Engineer supporting the Defense Health Agency. He developed one-of-a-kind testing environments to test RMF configuration changes and worked with Cybercomm to add vulnerability scanning tools to several DoD systems. Mr. Dawson can be reached at blaine.dawson@us.kbr.com

Mr. Beuchelt is the Chief Security Officer (CISO) for Sprinklr and former CISO of Demandware, Inc. He has worked on the architecture, design, implementation, and operation of the information security for highly complex systems within DoD, the Federal Government, and the private sector. Mr. Beuchelt authored various standards in information security and other distributed systems and is a frequent speaker at industry events. He can be reached at 118674c5@opayq.com

Mr. Charles Kelleher is a recognized Subject Matter Expert in the Cybersecurity field with over ten years' experience supporting the Defense Health Agency. His Cybersecurity experience began while serving in the US Army supporting the PACOM J6 followed by multiple roles on DHA IV&V Teams including Lead Validator, deputy for the RMF Counselor Support Team and currently serving as the DHMSM Cybersecurity Team Lead supporting the DODs Electronic Health Record system. His education and training include a Master's degree in Cybersecurity & CISSP. He can be reached at KBR at charles.kelleher@us.kbr.com.

Disclaimer

The views expressed in this paper represents the sole authors opinion based on their work history and interactions with individuals supporting the Department of Defense. This paper does not represent an official position from the Department of Defense, Purdue Global University, KBR, OASIS or Spinklr.