Defense Unicorns

Accelerating ATOs: A Declarative & Open-Source Approach

Prepared By

Defense Unicorns In Collaboration With Volunteer Interviewees (Both Within The Dod And Without) Who Have Experienced The Ato Process First Hand

Content

Executive Summary

Objective: To validate, through interviewing and cataloging first hand accounts of ATO participants, the hypothesis that through the adoption of Open-Source, Declarative Packages (OSDPs) that are already mapped in accordance to NIST 800.53, it's possible to accelerate and streamline the Authorization To Operate (ATO) process of the Department of Defense (DoD) as defined by Risk Management Framework (RMF). OSDPs are software tools or frameworks that provide a set of predefined configurations and settings for building secure applications.

Background: The RMF process, essential for safeguarding DoD information systems, suffers from significant delays and inconsistencies across departments due to varied implementation, extensive documentation, and resource constraints. Established initially as a collaborative effort among DoD entities and National Institute of Standards & Technology (NIST), the framework requires modernization to keep pace with evolving cybersecurity threats and technological advancements.

Advantages of OSDPs:

- With the introduction of OSCAL, declarative software packages have a common, machine readable language that allow for automating a significant portion of the ATO documentation.
- Enhanced Security and Transparency: Open source allows for greater scrutiny by subject matter experts, promoting ongoing rigorous security standards.
- Improved Collaboration Around Best Practices: OSDPs allow a lower entry point for industry involvement, fostering greater collaboration between industry and DoD, expediting vulnerability resolutions and sharing innovative solutions. This would also encourage the adoption of industry proven security protocol improvements.

Research Insights: Interviews with over 50 DoD ATO participants process identified consistent challenges.

- Extended waiting times for RMF certification due, in large part, to significant documentation requirements.
- Lack of additional clarity and guidance beyond the RMF documentation.
- Insufficient resources and training for effectively carrying out certification.
- Inconsistent application of RMF requirements across organizations.

Benefits of Innovation with OSDPs

- Reduced Cost and Time: Pre-mapped controls in OSDPs decrease the time and resources needed for documentation.

- Enhanced Risk Mitigation: OSDPs address a significant portion of risks, focusing on actual security rather than mere compliance.
- Democratized Knowledge: Publicly available OSDPs enable easier networking and collaboration on common challenges.

Conclusion: The integration of OSDPs into the RMF process presents a transformative opportunity for the DoD to enhance its cybersecurity measures as the documentation and testing of controls becomes a programatic process. By leveraging the strengths of open-source technology and the collaborative community it fosters, the DoD can achieve a more agile, transparent, and effective RMF process, resulting in quicker ATO achievements and a stronger defense posture.

Recommendation: Defense Unicorns recommends the creation and adoption of common OSDPs (fully mapped to NIST 800.53) to accelerate the RMF process. Embracing this approach will lead to significant improvements in security, efficiency, and cost-effectiveness, ensuring that our defense systems are both rapidly deployable and robustly secure.

Introduction

Accelerating the DoD RMF to get updated software and capabilities to the front line of our nation's defense force faster is not a new topic. There have been multiple efforts to improve, clarify, and expedite the DoD RMF process (and several efforts are underway in the present day).
At Defense Unicorns, we believe the use of an Open Source Declarative Package (OSDP) that maps to NIST 800.53 can significantly accelerate the DoD ATO process by allowing greater collaboration and scrutiny between DoD and industry, saving time and money in the manual mapping process and (over time) providing a standardized baseline of expectations for assessing and mitigating cyber-risk.

This has never been more attainable thanks to the creation of Open Security Controls Assessment Language (OSCAL) by NIST. OSCAL's focus on security automation, planning, and assessment aligns well with the structured nature of declarative packages, enhancing the efficiency and accuracy of risk evaluations within the ATO process. By utilizing OSCAL alongside declarative packages, government agencies can automate the assessment of security controls, ensure compliance with standards like NIST SP 800-53, and facilitate continuous monitoring of IT systems post-authorization.

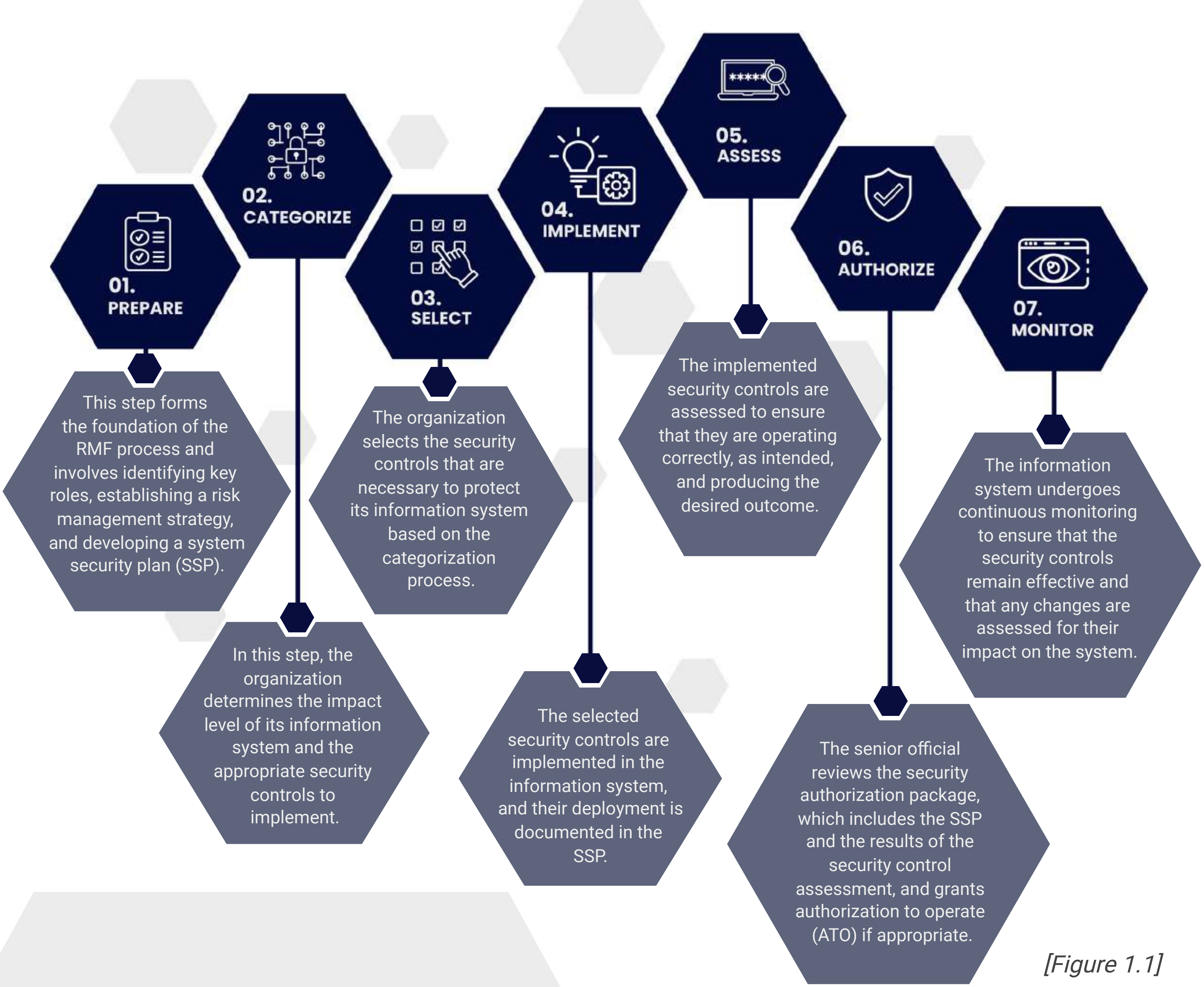
The ATO process today

Before discussing how an OSDP can accelerate the DoD ATO process, it's important to understand the current process and the challenges involved. The RMF was developed as a collaboration between the DoD, the Committee on National Security Systems (CNSS), and the National Institute of Standards and Technology (NIST) to provide a standardized process for managing and mitigating risks related to information systems (1). Prior to the RMF being officially adopted in 2014, cyber security risk evaluation was governed by the Department of Defense Information Assurance Certification and Accreditation Process (DIACAP).

The RMF is a guide that each department within the DoD follows to identify, assess, and mitigate risks associated with information systems; however, how each department implements the RMF can vary, leading to inconsistencies when comparing the process across the DoD. *[See figure 1.1]*

"OSDP": Open-source Declarative Package

Introduction [continued]



01. PREPARE

This step forms the foundation of the RMF process and involves identifying key roles, establishing a risk management strategy, and developing a system security plan (SSP).

02. CATEGORIZE

In this step, the organization determines the impact level of its information system and the appropriate security controls to implement.

03. SELECT

The organization selects the security controls that are necessary to protect its information system based on the categorization process.

04. IMPLEMENT

The selected security controls are implemented in the information system, and their deployment is documented in the SSP.

05. ASSESS

The implemented security controls are assessed to ensure that they are operating correctly, as intended, and producing the desired outcome.

06. AUTHORIZE

The senior official reviews the security authorization package, which includes the SSP and the results of the security control assessment, and grants authorization to operate (ATO) if appropriate.

07. MONITOR

The information system undergoes continuous monitoring to ensure that the security controls remain effective and that any changes are assessed for their impact on the system.

[Figure 1.1]

Why choose an OSDP?

OSDPs are software tools or frameworks that provide a set of predefined configurations and settings for building secure applications. These packages have several advantages when it comes to accelerating the DoD ATO process.

Open-Source Allows Greater Scrutiny By Subject Matter Experts

Firstly, the open exposure of these software packages allows researchers to delve into the source code to understand how each portion of the software operates and potentially improve upon it. This level of transparency and accessibility allows for thorough evaluation and scrutiny, ensuring that the software meets the highest standards of security.

Open-Source Has A Greater Opportunity To Align With Industry Best Practices

Secondly, OSDPs are designed to align with industry standards and best practices. This means that organizations using these packages can leverage established security frameworks and guidelines, such as NIST 800-53, without reinventing the wheel.

Open-Source Allows Greater Collaboration Between Industry And Dod

Thirdly, open-source declarative packages promote collaboration and knowledge sharing within the development community. This collaboration allows for faster identification and resolution of vulnerabilities or weaknesses, as well as the sharing of best practices and innovative solutions to security challenges.

Oscal Has Paved The Way For Declarative Packages To Succeed

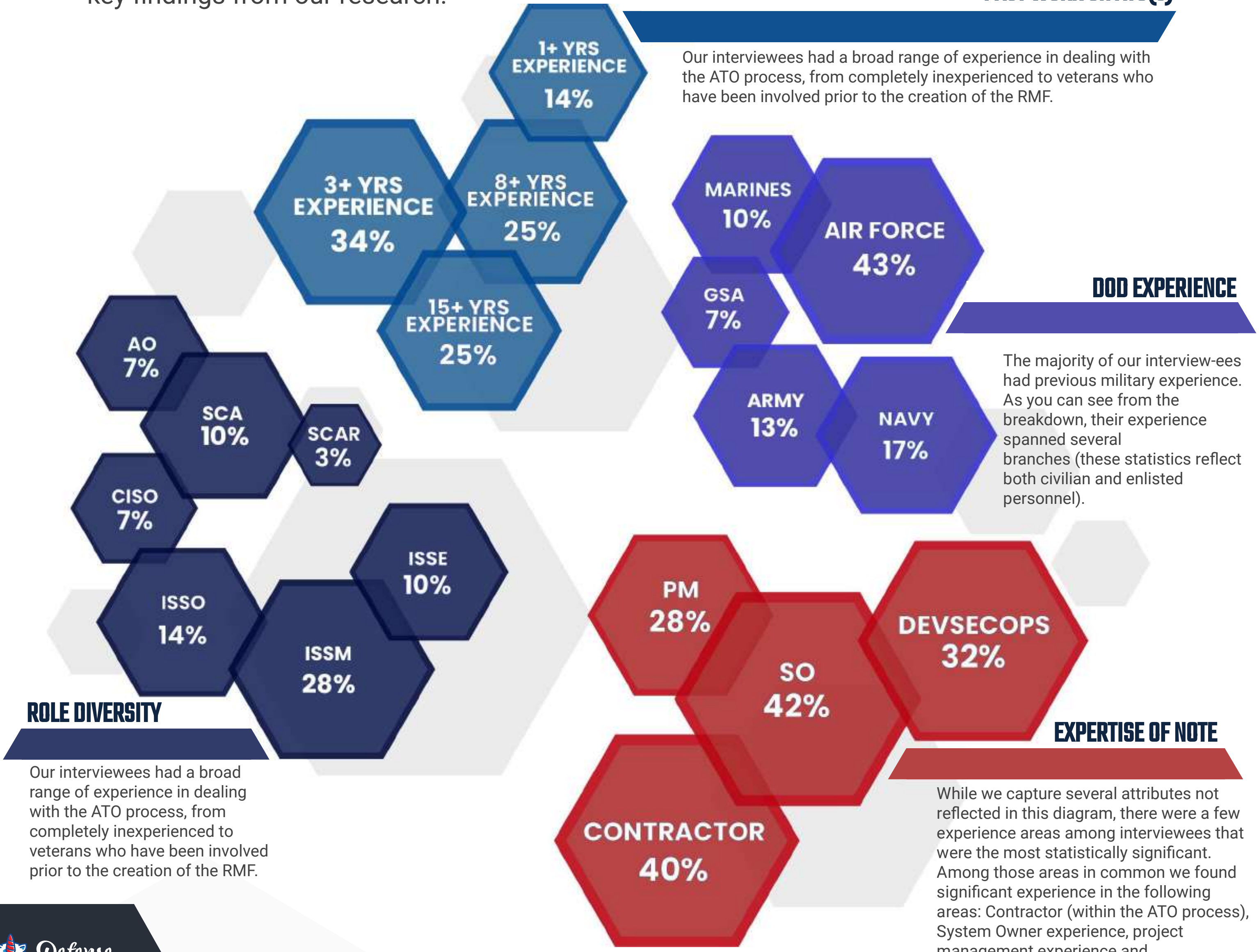
The recent creation of OSCAL (Open Security Controls Assessment Language) by NIST (2) marks a significant milestone for security automation. The relationship between OSCAL and declarative packages in terms of automating assessments is significant in the context of streamlining security evaluations and compliance processes within government agencies like the DoD. OSCAL, as a standardized language for expressing security controls, complements declarative packages by providing a structured framework for describing security controls and assessment information.

Interviews Show Open-Source Could Accelerate Ato Process

Through conducting research interviews with individuals involved in the DoD ATO process, several commonly experienced blockers were identified. Several of these blockers are problems that could be addressed by using an OSDP that, out of the box, is mapped back to NIST 800.53. In this section, we will share some of the key findings from our research.

WHO WE INTERVIEWED

We conducted in-depth interviews with a diverse sample of over 50 individuals currently or formerly involved in the ATO process. These interviews covered representatives from Army, Navy, Air Force, and Marine Corps across multiple acquisition programs. The interviewees included software developers, system administrators, information security officers, program managers, authorizing officials (AO)s and chief information security officers (CISO)s.



PAST WORK ON ATO(S)

Our interviewees had a broad range of experience in dealing with the ATO process, from completely inexperienced to veterans who have been involved prior to the creation of the RMF.

DOD EXPERIENCE

The majority of our interview-ees had previous military experience. As you can see from the breakdown, their experience spanned several branches (these statistics reflect both civilian and enlisted personnel).

ROLE DIVERSITY

Our interviewees had a broad range of experience in dealing with the ATO process, from completely inexperienced to veterans who have been involved prior to the creation of the RMF.

EXPERTISE OF NOTE

While we capture several attributes not reflected in this diagram, there were a few experience areas among interviewees that were the most statistically significant. Among those areas in common we found significant experience in the following areas: Contractor (within the ATO process), System Owner experience, project management experience and DevSecOps experience.

Perceptions vs. Facts

It is important to note that the following information is based on interview findings from our subjects. While some of the data collected were objective facts, the majority of it was based on their personal experience and perceptions. Perceptions may not be facts, but they are the interpretation of facts and therefore can be extremely helpful in illuminating opportunities for improvement.

The following collection represents common themes shared by our interviewees and does not necessarily represent the views of Defense Unicorns or its employees. The main challenges identified by interviewees revolve around documentation, knowledge-sharing barriers, and some issues with the availability and usage of required resources for RMF certification(3).

Commonly Shared Challenges

During the research interviews, several commonly shared challenges were identified that slowed down the DoD ATO process.

Extended Wait Times

Many individuals reported experiencing significant delays in the RMF certification process. These delays were often attributed to factors such as lack of available personnel, lack of clarification, and lack of communication between System Owner (SO) representatives and ATO stakeholders.

Insufficient Resources

Most interviewees identified that they faced challenges due to limited resources, including personnel and budget, which impacted their ability to effectively carry out the RMF certification process.

Inadequate Training

Most interviewees stated that there was a lack of comprehensive training and education on the RMF certification process, leading to difficulties in fully understanding and implementing the necessary requirements. This reporting came from both the System Owner side and the AO/security control assessor (SCA) side; however, this reporting was not consistent across all DoD branches.

Inconsistent Application

Interviewees mentioned that the application of RMF certification requirements varied across different organizations and branches of the DoD, leading to confusion and inconsistencies in the certification process.

Lack Of Clarity And Guidance

Interviewees expressed frustration with the lack of clear and consistent guidance provided during the RMF certification process.

Interview Results... [continued]

These insights were shared not only by applicants of the RMF process (the SOs) but also by the representatives of the RMF process (AOs, SCAs, information systems security managers, etc.).

This commonality of complaints from both sides indicates a critical need for improvements in the RMF certification process to address these shared challenges and to cater to the needs of all stakeholders involved.

Unveiling Patterns: A Deep Dive Into Collective Interview Insights

Our research interviews uncovered several patterns and insights regarding the challenges faced by organizations seeking DoD ATO. When taking into account the segmentation differences of our groups we were able to identify commonalities among these differences:

"Size Matters"

ATO success among System Owners (SOs) is far more likely the larger the resources they possess. One of our SCA participants shared that on average it took their team of three full-time personnel a minimum of 60 days to prepare a new SO so that they can start the ATO process. That is a minimum of 1,440 man-hours just for the initial set. How many hours (and dollars) would it take a small business to create an ATO package from scratch? This cost can be significant for smaller companies, especially if they don't realize the task's effort until they are already in the process of seeking certification.

"Perception Is Policy"

The RMF was not intended to be an exhausted collection of policies or a primer on cyber security. It is a general framework intended to give guidance to the various offices/branches on the requirements of the ATO. However, this lack of clarification was cited by most respondents as being unhelpful when it comes to more complicated or nuanced systems.

"Risk Mitigation Vs. Checking The Box"

Many of our interviewees spoke of the importance of keeping risk mitigation as the central focus of the RMF process instead of exclusively focusing on meeting the certification check marks, which may lose sight of the ultimate goal of ensuring cybersecurity (4). Many respondents shared that the NIST 800.53 controls are not always easily applied to complex software systems and may require interpretation and customization to address the unique risks of each system adequately. Further, most respondents recounted the tension of establishing cyber security risk mitigation over the typically bureaucratic approach of merely "checking the box" in compliance with regulatory obligations, emphasizing a need for agile and adaptable risk management solutions suitable to the evolving cybersecurity landscape.

"Lack Of Incentives For Accelerated Certification"

- Respondents reported a lack of sufficient incentives to expedite the lengthy and often onerous certification process, suggesting that policies that encourage faster, more efficient certification could greatly improve RMF effectiveness. If an ATO is slow in its progress, the mission timeline may suffer or the SO may incur unnecessary delays and costs. However, there is no real downside for the maintainers of the ATO process (specifically AOs or SCAs). ATO completion is not a performance metric for these positions. However, there is significant personal perceived risk to AOs or SCAs should the SO incur a data breach - resulting in political pressure, career insecurity, etc. There is greater personal incentive to deny an ATO than there is to successfully award an ATO.

"Varying Subjective Interpretations"

- Varying experiences highlighted how assessments were significantly affected by the personality, education and experience of the assessor and/or the AO. This results in a lack of standardization from branch to branch (and even among AO offices within the same DoD branch). The more complex the software/environment, the more challenging the experience, suggesting the necessity for a unified approach that caters to different operational and environmental contexts(7). The only commonality among branches was the controls themselves (NIST 800.53); how to meet those controls or even how to word the evidence of mitigation could vary greatly.

"If You Know You Know"

- The presence of personal connections and relationships within the certification process was identified as a significant factor in successfully completing the RMF process. Those who had previous military experience were far more apt to make use of resources beyond official documentation and channels, such as personal networks and relationships, to navigate the RMF certification process successfully. Those who lacked previous experience or personal contacts within their respective AO office recounted being unable to find resources or receive the necessary support to navigate the RMF certification process effectively. Examples:
  - “I was told to go find a two-star general”
  - “There are resources out there, you just have to know where to look.”
  - “No single point of sharing of information that would allow me to know what other services are out there that already have an ATO.”
  - “Hiring someone who has worked with that particular AO office is your best bet for success."

"Complex Tech Prone To Misled Cyber Safety Efforts"

Most interviewees cited the difficulty of assessing risk for highly technical processes and systems in a language that non-technical stakeholders can understand. This led to delays in decision-making and a lack of understanding and support from higher-level officials who may not have the technical knowledge. Examples were shared of key milestone meetings that proved ineffective because there was no Subject Matter Expert present to explain agenda items. Several respondents experienced having to change ATO control package wording per SCA instruction that later (when the ATO was up for reevaluation) the same SCA gave feedback that the wording was now unacceptable.

Synthesis reveals that many identified patterns align well with the strengths of open-source solutions.

Osdp Innovation: A Significant Aid To Rmf Challenges?

"Size Matters"

Having a significant percentage of controls met and mapped out of the box significantly lowers the cost for the documentation portion of the RMF process. Furthermore, using an open-source, declarative package that aligns with NIST 800.53 allows for better auditability and traceability of security controls.

"Lack Of Incentives For Accelerated Certification"

While the use of an OSDP doesn't directly affect this, a secondary benefit of greater adoption of an OSDP would streamline the ATO process overall and potentially create more incentives for accelerated certification.

"Risk Mitigation Vs. Checking The Box"

Having a significant percentage of controls met and mapped out of the box significantly lowers the cost for the documentation portion of the RMF process. Furthermore, using an open-source, declarative package that aligns with NIST 800.53 allows for better auditability and traceability of security controls.

"If You Know You Know"

The OSDP would be hosted in a publicly available repository, making it easier for SOs to network and collaborate on commonly shared challenges.

"Varying Subjective Interpretations"

The nature of the open-source community would promote greater collaboration between SO and DoD stakeholders, reducing misunderstandings and allowing for clearer communication of technical processes and risks.

"Complex Tech And Cyber Safety Challenges"

Having pre-established, vetted documentation language solved for risk mitigation lowers cyber risk vulnerability and puts less risk on individual assessors/SOs.

"Perception Is Policy"

An OSDP can reinforce DoD priorities for risk by having these prioritized controls and requirements built into the package, ensuring that all stakeholders are aligned on what is necessary for accreditation.

Conclusion

By using an OSDP mapped to NIST 800.53, organizations can accelerate the time it takes to create, certify and deliver secure systems through the ATO process. The common platform provides pre-configured controls and documentation templates, reducing the time and effort required for assessment and authorization. This enables organizations to obtain ATO more efficiently, allowing them to deploy their systems and applications faster and more securely.

The quest for a more efficient DoD RMF is a crucial endeavor that can significantly benefit from the creation and adoption of OSDPs. Defense Unicorns has illuminated the path forward with compelling evidence that such packages can, indeed, revolutionize the ATO process within the DoD. The current RMF process can gain from the transparency, standardization, and collaborative nature of OSDPs. Our research underscores the critical advantages of embracing open-source solutions: enhanced scrutiny by experts, alignment with best practices, and collaborative dynamics that collectively drive innovation and improve cyber-risk assessment and mitigation.

The OSDPs' alignment with NIST 800.53 controls not only propels the ATO process forward but also ensures that compliance is not just a box-checking exercise but a meaningful stride toward robust cybersecurity. The challenges identified through our interviews—from the need for clarity and guidance to the barriers in knowledge sharing and resource allocation—paint a clear picture of the current landscape's complexities. The OSDP approach directly addresses these concerns, offering a beacon of hope for small and large organizations alike, democratizing access to secure software development, and expediting the authorization process.

Defense Unicorns believes that the future of cybersecurity in the DoD environment hinges on our collective ability to adapt and innovate. The implementation of OSDPs represents more than a technological advancement; it is a paradigm shift towards a more unified, efficient, and secure framework that respects the agility required by our defense forces. By reducing the subjectivity of interpretations and leveraging the collective intelligence of the open-source community, we can transform perceptions into policy, ensuring that our cybersecurity measures are as formidable as the forces they are designed to protect.

The acceleration of the ATO process is not merely a logistical improvement but a strategic imperative. As we move forward, the adoption of OSDPs stands out as a clear and promising avenue to enhance the DoD's defensive and operational capabilities. By embracing the open-source movement, we align ourselves with a future that values collaboration, innovation, and security at every turn, ensuring that the front lines are supported by systems that are as secure as they are swiftly approved. Let us not shy away from this opportunity to reform, streamline, and empower the RMF process with the vigor and vision it demands.

Citation Sources

1. Quirolgico, S., Voas, J., Karygiannis, T., Michael, C., & Scarfone, K. (2019, April 1). Vetting the security of mobile applications. https://scite.ai/reports/10.6028/nist.sp.800-163r1
2. NIST has developed the Open Security Controls Assessment Language (OSCAL 1.0.0), 2021, https://www.nist.gov/news-events/news/2021/06/nist-has-developed-open-security-controls-assessment-language-oscal-100
3. Bush, J P., Westervelt, E T., Clark, B., Schwenk, D M., Briggs, S., Shepard, D P., Long, M C., Patel, T P., Johnson, M., & Lynch, E D. (2022, August 16). Installation utility monitoring
4. Borky, J M., & Bradley, T H. (2018, September 9). Protecting Information with Cybersecurity. https://scite.ai/reports/10.1007/978-3-319-95669-5_10and control system technical guide. https://scite.ai/reports/10.21079/11681/45081

Appendix A

Key Roles Involved in RMF process

- System Owner: The system owner is typically the individual or organization responsible for the development, operation, and maintenance of the system or application seeking an ATO. They are responsible for ensuring that the system complies with security policies and standards and for providing necessary documentation and resources.

- Authorizing Official (AO): The authorizing official is a senior-level individual with the authority to grant or deny an ATO. This role is crucial in the ATO process as the AO evaluates the risks associated with the system and makes the final determination on whether it can be authorized for use within the DoD. he AO has often received this designation in addition to their official duties. There are few 'full-time' AOs. **DAO*

- *Information System Security Engineer (ISSE): The ISSE is responsible for conducting information system security engineering activities. These activities include capturing and refining information security requirements and ensuring their integration into information technology component products and information systems through purposeful security design or configuration.*

- Information System Security Manager (ISSM): The ISSM is responsible for managing the security of the system or application throughout its lifecycle. They are key in preparing and maintaining security documentation, overseeing security controls, and coordinating security assessments.

- Information System Security Officer (ISSO): The ISSO assists the ISSM in implementing and managing security controls. They work closely with system administrators and users to ensure compliance with security policies and procedures.

- Security Control Assessor (SCA): The SCA conducts security assessments evaluation, in particular working through the list of controls as defined by NIST 800.53. They evaluate whether the system meets security requirements and provide their assessment to the AO (though the AO does not hold a supervisory role). **SVA, SCARs*

- Security Engineers and Analysts: These professionals assist in the technical aspects of security assessments, including vulnerability scanning, penetration testing, and analysis of security controls. They provide expertise in identifying and mitigating security risks.

Appendix A [Continued]

Key Roles Involved in RMF process

- Program Managers and Developers: Those responsible for designing, developing, and maintaining the system or application must ensure that security is integrated into every phase of the development lifecycle. They collaborate with security personnel to implement necessary security features and controls.
- Information Assurance Manager (IAM): The IAM oversees the organization's overall information assurance program. They help ensure that security policies and practices align with DoD guidelines.
- Compliance and Legal Teams: Legal experts and compliance officers ensure that the ATO process complies with all applicable laws, regulations, and DoD policies. They may also help address legal and contractual requirements related to security.
- Continuous Monitoring Teams: These teams are responsible for ongoing security monitoring, including reviewing security logs, responding to incidents, and ensuring that security controls are maintained and updated as needed.
- External Assessors: In some cases, external third-party assessors may conduct security assessments to provide an independent evaluation of the system's security posture.
- DoD Component Leaders: Leadership within various DoD components (e.g., Army, Navy, Air Force) may have oversight and involvement in the ATO process, especially for systems specific to their branch.
- Defense Information Systems Agency (DISA): DISA plays a key role in providing guidance, tools, and support for the ATO process across the DoD. They offer security resources and maintain the Risk Management Framework (RMF) standards used in the ATO process.
- National Institute for Standards and Technology (NIST): A federal agency within the United States Department of Commerce. NIST is responsible for developing and promoting measurement standards, technology standards, and best practices to enhance innovation and competitiveness in various industries, including science, engineering, and technology. NIST is the author of the source documents that guide each phase of the ATO process, in particular the NIST 800.53 which defines the security controls that a system owner must satisfy to be awarded an ATO.