Enabling Agile Authorization for Mixed Reality Training Applications and Devices

Brandi Pickett	Jason Ingalls
Ingalls Information Security	**Ingalls Information Security**
Woodworth, LA	**Woodworth, LA**
Brandi.pickett@iinfosec.com	**jringalls@iinfosec.com**

ABSTRACT

Accelerating technical training, equipping, and empowering Airmen for the battlespace is a strategic goal for the Air Force. Commands, Wings, and Users want to leverage training applications coupled with mixed reality devices as it saves training time, makes it more accessible, and saves costs. However, training applications and devices are delayed for operational use due to navigating the inscrutable Authorization to Operate (ATO) process.

The DoD adopted the Risk Management Framework (RMF) to empower services to assess, manage, and validate cybersecurity risks. The RMF process is directed to be used for DoD Assessment and Authorization (A&A) processes. However, these processes are exhaustive, resource-intensive, requiring a sophisticated skillset, and often not considered until the application is ready to deploy, significantly delaying the timely delivery of today's technology to the warfighter. RMF implementation can take a year or longer for an application to get an ATO. This creates significant problems with industry costs and effective risk management.

The military member responsible for performing the A&A activities must accomplish the mysterious ATO process without the training and experience needed to succeed while tackling the many misconceptions and esoteric rules.

DoD must shift from a cybersecurity “snapshot in time” and paper drill compliance culture to a culture where automation is tightly coupled with real-time continuous risk monitoring.

Thought leaders have expressed ways in which to combat the A&A challenges. Analyzing these processes is necessary to identify the best approaches for agile authorization.

Innovative solutions that enable real-time risk management must reduce lead time for compliance by assessing applications with an agile, DevSecOps approach and marginalize the labor and financial costs for obtaining an ATO.

ABOUT THE AUTHORS

Brandi Pickett is the Director of Consulting at Ingalls Information Security. She leads a team of experts providing cybersecurity assurance processes for Virtual Reality and Augmented Reality applications and training simulators developed by the USAF. With over a decade's experience, she is proficient in Risk Management Framework (RMF), Assessment & Authorization, and Vulnerability Management. Ms. Pickett is a Certified Information System Security Progressional (CISSP), Certified in Governance, Risk and Compliance (CGRC), and Cybersecurity Maturity Model Certification Registered Practitioner (CMMC RP). Ms. Pickett entered the cybersecurity field while working at the Arkansas Department of Human Services as a HIPAA Privacy and Security Auditor. This job led to continued work in the federal space supporting a DoD contract in the HQ Air Education & Training Command (AETC) Communications Directorate. There she served as a valuable team member offering support to over fifty HQ staff at one of the largest joint bases in DoD (Joint Base San Antonio - Randolph Air Force Base). She was responsible for ensuring compliance with FISMA and DoD/AF policies. Ms. Pickett was a vital representative on a SAF-CIO level forum facilitating management, oversight, and execution of the AF Cybersecurity Program. She holds a Master of Science in Operations Management from the University of Arkansas.

Jason Ingalls is an engineer-turned-entrepreneur who founded Ingalls Information Security in 2010. Before that, he was an Information Assurance Engineer and Incident Responder for General Dynamics for nine years. As an established Incident Response veteran having helped lead through some of the most significant data breaches in history, beginning with his 2007 work on the Hannaford Brothers Grocers and TJ Maxx breaches and continuing through servicing multi-national nonprofits, financial and healthcare institutions, Mr. Ingalls and his team's work to successfully remediate many high-profile breaches have earned industry-wide respect.

Mr. Ingalls' career has been spent delivering human-centered, technology-enabled solutions to reduce information technology risk. He leads a team of the best and brightest professionals who deliver information security services that scale. He focuses on establishing trusted partnerships with Ingalls' clients, elevating their unique needs and goals into a long-term strategy for enhanced cybersecurity posture through a proven process. As a life-long resident of Louisiana, he is passionate about establishing his home state as a cybersecurity center of excellence and bringing 5,000 industry jobs to uplift the state's people and economy within the next 20 years.

Mr. Ingalls was recently awarded a United States patent for the virtual reality software, Viewpoint, a network security monitoring and correlation system that provides a three-dimensional (3D) visualization of network traffic overlaid with security alerts and other relevant discrete data. This innovation gives security professionals the ability to see and interact with data spatially, eliminating the need to scroll through massive spreadsheets of technical data and providing a standard data model that all stakeholders can see and understand, enabling faster and more robust insights, data correlation and informed, risk-based decision making in real-time. This quantum leap forward in cybersecurity data visualization provides capabilities that have never existed.

Enabling Agile Authorization for Mixed Reality Training Applications and Devices

Brandi Pickett	Jason Ingalls
Ingalls Information Security	Ingalls Information Security
Woodworth, LA	Woodworth, LA
Brandi.pickett@iinfosec.com	jringalls@iinfosec.com

INTRODUCTION

Delays hinder the Air Force's strategic goal of accelerating training for airmen in the Authorization to Operate (ATO) process for training applications and mixed reality devices. The transition to RMF was completed in 2018 and brought a dynamic approach to focusing on risk management and ongoing continuous monitoring. The RMF process is a Seven-Step Process.

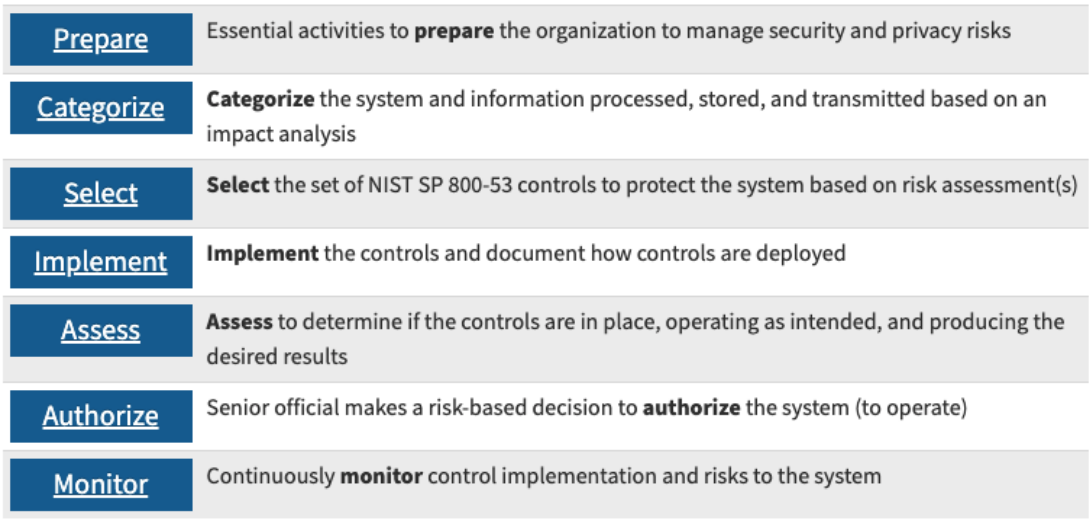

Figure 1: NIST RMF Seven (7) Steps

According to NIST, the RMF is a comprehensive, flexible, risk-based approach. The RMF provides a process integrating security, privacy, and cyber supply chain risk management activities into the system development life cycle. The risk-based approach to control selection and specification considers effectiveness, efficiency, and constraints due to applicable laws, directives, Executive Orders, policies, standards, or regulations. Managing organizational risk is paramount to adequate information security and privacy programs; the RMF approach can be applied to new and legacy systems, any type of system or technology (e.g., IoT, control systems), and within any organization regardless of size or sector.

According to DOD Information Assurance principles, performing RMF Steps will render an Authorization Decision such as an Authorization to Operate (ATO) for an application. An ATO must be obtained before the application can be used in an operational environment. Application owners must complete the required ATO documentation and security controls. Authorizing Officials (AO) review the ATO documentation and upon their provision of an ATO, accept any risk of the application.

Challenges with the current ATO process

Many challenges contribute to the delays in the ATO process. These include factors such as complex bureaucracy, lengthy documentation requirements, and lack of streamlined communication channels that impede the timely approval of applications. According to The Rand Corporation Research Report, Improving the Cybersecurity of the USAF Military Systems throughout their Life Cycles, "the stakeholders for cybersecurity in the AF are confronted with a welter of laws and policies that are voluminous, complicated, and changing faster than the life cycle of a military system."

The challenges around the RMF, as a path to secure applications consists of the following:

- The length of time it takes to complete the mandatory forms to start the ATO process
- The length of time it takes for a user to complete the security control implementation details
- The length of time it takes for the AO and Security Control Assessor (SCA) staff to inform the AO and SCA of their assessment of the packages (including staffing PowerPoint slides or other administrative documents for an AO Decision Briefing)
- The length of time to schedule the ATO Decision discussion with those that have the power to issue the ATO
- The number of controls to test and evaluate, and the level of effort required to do so

The DoD adopted the RMF to empower the services to assess, manage, and validate cybersecurity risks. However, current RMF implementation can take up to 8 months or longer for an application to get an ATO, a significant amount of time invested in assessment compared to an application's development timeframe. This creates problems with effective risk management.

The ATO process has been seen as a persistent hurdle for cloud adoption and IT modernization. As Carten Cordell describes in a FEDSCOOP commentary, the regulatory framework that vendors must navigate to offer new services to the federal government creates substantial issues, where "both timelines and industry costs for obtaining ATOs, which have been estimated to average as long as four-to-six months and cost between $300,000 and $700,000 is a major hurdle to overcome. ATOs across government have traditionally taken 6-18 months (about 1 and a half years), with a lot of slow back-and-forth between system owners and the assessors."

As Mary Lazzeri stated in her work, ATO ASAP: Let's finally fix the security compliance problem, "the muddled, bureaucratic process to obtain an ATO and launch an IT system inside the government is widely maligned — but beyond that, it has become a pervasive threat to system security. The longer the government takes to launch a new-and-improved system, the longer an old and potentially insecure system remains in operation."

Understanding Agile Authorization

Agile authorization is an iterative and collaborative approach to the ATO process. This section explores agile authorization's fundamental principles and characteristics, emphasizing its ability to foster efficiency, flexibility, and adaptability. It also highlights the importance of continuous communication and early stakeholder involvement.

"Agile is a set of four values and twelve principles used to guide decision-making throughout the project life cycle, also known as the Agile Manifesto," says Ms. Nyte in the Why of Agile Article. Organizations can align agile practices to improve their cybersecurity posture. Here are some agile principles that can be leveraged in cybersecurity:

Iterative and Incremental Approach: Agile authorization embraces an iterative and incremental approach to authorization, allowing for continuous feedback, learning, and improvement. Rather than waiting for a complete and final authorization package, the process is broken down into smaller, manageable increments, allowing for faster evaluation and deployment.

Early and Continuous Stakeholder Involvement: Agile authorization involves stakeholders, such as trainers, subject matter experts, security personnel, and administrators, from the early stages of the authorization process. By engaging stakeholders throughout the development lifecycle, their insights and feedback can be incorporated, ensuring alignment with their needs and reducing the likelihood of late-stage revisions and delays.

Transparent and Frequent Communication: Clear and frequent communication is a fundamental principle of agile authorization. Regular communication channels are established to foster collaboration, share progress updates, address concerns, and gather feedback. This transparency ensures that all stakeholders are informed about the authorization process, enabling better coordination and quicker decision-making.

Lean Documentation: Agile authorization promotes lean documentation, focusing on essential information and avoiding unnecessary bureaucracy. Instead of extensive and time-consuming documentation, the emphasis is on providing concise and relevant documentation that supports the authorization process without sacrificing compliance or security requirements. This lean approach reduces administrative burden and speeds up the approval process.

Continuous Risk Assessment and Mitigation: Agile authorization encourages continuous risk assessment and mitigation throughout the development and deployment of training applications. Risk assessment is not a one-time activity but an ongoing process that adapts to changes in the application and its environment. Addressing risks proactively and continuously can minimize potential roadblocks and delays, ensuring a smoother and faster authorization process.

Collaboration and Cross-Functional Teams: Agile authorization promotes collaboration and cross-functional teams that include representatives from various disciplines, including training, security, compliance, and administration. This collaborative approach enables a holistic and comprehensive evaluation of training applications, fosters shared understanding, and facilitates faster decision-making.

Continuous Improvement and Adaptability: Agile authorization embraces a culture of continuous improvement and adaptability. Lessons learned from each authorization process are used to enhance future processes, resulting in increased efficiency and effectiveness over time. The approach allows flexibility and adaptability to changing requirements, ensuring that the authorization process remains responsive and aligned with evolving needs.

By adhering to these key principles, the Air Force can successfully implement agile authorization, leading to faster approval of training applications, increased stakeholder collaboration, and improved responsiveness to changing requirements.

Adopting Agile Principles in Cybersecurity for Authorization

An agile authorization framework provides a structured approach for implementing agile principles and practices within the authorization process. While no standardized framework exists, organizations can adapt and customize existing agile frameworks, such as Scrum or Kanban, initially created for the software development work, to fit their specific authorization needs. Mr. Konrad of World Wide Technology states "Adopting an agile workflow for cybersecurity can lead to a more efficient environment through process consistency, enhanced project visibility, and team collaboration." Here is a general outline of an Agile Authorization Framework:

Define Roles and Responsibilities: Identify the key stakeholders involved in the authorization process, including trainers, subject matter experts, security personnel, administrators, and other relevant parties. Clearly define their roles, responsibilities, and authority within the framework.

Establish Cross-Functional Teams: Form cross-functional teams comprising representatives from different disciplines involved in the authorization process. These teams should include individuals from training, security, compliance, administration, and other necessary areas. The teams collaborate to ensure a holistic evaluation and decision-making process.

Adopt Agile Methodologies: Select and adopt agile methodologies that align with the organization's needs and culture. Popular frameworks such as Scrum or Kanban can be leveraged to manage the authorization process. Agile methodologies provide a set of practices, such as sprints, backlogs, and daily stand-ups, which can be adapted to the specific requirements of the authorization process.

Implement Iterative Development Cycles: Break down the authorization process into iterative sprint cycles. Each sprint focuses on a specific subset of the authorization requirements, enabling faster evaluation, feedback, and progress tracking. At the end of each cycle, the teams review and adapt the approach based on lessons learned and stakeholder feedback.

Enable Continuous Stakeholder Engagement: Foster regular and transparent communication with stakeholders throughout the authorization process. Conduct frequent meetings, demonstrations, and feedback sessions to gather inputs, address concerns, and inform stakeholders of progress. Engage stakeholders at every stage to ensure alignment and reduce the likelihood of late-stage revisions.

Streamline Documentation: Embrace lean documentation principles to streamline the authorization process. Focus on capturing essential information while minimizing bureaucratic and unnecessary paperwork. Identify the critical documentation requirements and ensure they are aligned with compliance and security standards.

Leverage Technology Solutions: Utilize technology tools and solutions to automate and streamline the authorization process. Workflow management systems, document collaboration platforms, and automated testing tools can expedite communication, review, and approval cycles. Integrate technology solutions that enhance transparency, efficiency, and traceability.

Embrace Continuous Improvement: Cultivate a culture of continuous improvement within the agile authorization framework. Encourage teams to reflect on their practices, identify areas for enhancement, and implement changes in subsequent iterations. Promote learning, knowledge sharing, and applying lessons learned from previous authorization cycles.

Benefits of Agile Authorizations in the Modeling and Simulation Domains

This section outlines the potential benefits of implementing agile authorization in the Air Force's training application and mixed reality approval process. It discusses how agile authorization can lead to reduced time-to-market, improved responsiveness to changing requirements, enhanced stakeholder collaboration, and increased transparency.

Here are some key benefits of agile authorization, according to Ms. Hunter of BuiltIn:

Reduced Time-to-Market: Agile authorization enables faster approval and deployment of training applications, leading to reduced time-to-market. By breaking down the authorization process into smaller, iterative cycles, organizations can expedite decision-making, streamline documentation, and address concerns promptly, resulting in accelerated training for airmen.

Improved Responsiveness to Changing Requirements: Agile authorization allows for greater flexibility and adaptability in addressing changing requirements. Through continuous stakeholder involvement and regular feedback loops, training applications can be adjusted and refined iteratively, ensuring alignment with evolving needs. This responsiveness helps avoid delays caused by late-stage revisions and ensures that the approved applications remain relevant.

Enhanced Collaboration and Stakeholder Engagement: Agile authorization emphasizes cross-functional collaboration and early stakeholder involvement. By actively engaging stakeholders throughout the authorization process, communication channels are established, and a shared understanding is developed. This collaborative approach fosters better coordination, knowledge sharing, and collective decision-making, leading to more effective and efficient approval processes.

Increased Transparency and Visibility: Agile authorization promotes transparency by establishing clear communication channels and providing regular progress updates to stakeholders. This transparency enables better visibility into the authorization process, ensuring that all stakeholders are aware of the status, potential bottlenecks, and risks. Improved visibility reduces ambiguity and facilitates informed decision-making, ultimately expediting the approval of training applications.

Streamlined Documentation and Administrative Burden: Agile authorization adopts a lean documentation approach, focusing on essential information while minimizing administrative burden. By avoiding excessive paperwork and bureaucracy, organizations can streamline the documentation process, reducing the time and effort required for authorization. This streamlining enables quicker processing and ensures compliance and security requirements are met without unnecessary delays.

Continuous Improvement and Risk Mitigation: Agile authorization promotes a culture of continuous improvement and risk mitigation. Through iterative cycles, organizations can continuously assess and address risks, allowing for proactive risk management throughout the authorization process. This approach minimizes the likelihood of surprises and enables timely risk mitigation strategies, ensuring a smoother and faster approval process.

Agile Documentation in support of RMF Prepare Step

NIST RMF provides ample guidance and even breaks down the process of evaluation into steps that are necessary to perform to complete the entire process. However, the jargon used, and the subject itself (cybersecurity risk management) put the topic out of the reach of many ATO process stakeholders. For example, the NIST RMF Prepare step is relatively straightforward, but users still have difficulty knowing how to start the RMF process and which tools to use to help them do it.

There are striking similarities between the ATO process and other documentation efforts that must be certified by Federal authorities, and a great example is the personal tax return. Filers must collect information, enter copious amounts of data into forms, sometimes multiple times, and then print, collate, and submit a packet of documents as part of their filing. The process requires arcane knowledge of esoteric tax laws, and an understanding of accounting. However, several commercial companies have created successful applications (e.g. "Turbo Tax") that provide tax filers with a simple user interface and a manageable and intuitive workflow. TurboTax converted a dreadful user experience into a delightful one utilizing clever UX design (Noel, J).

Addressing the inefficient and error-prone nature of ATO package manual data entry by automating and deduplicating wherever possible minimizes user workload for ATO creation. The complex processes of deciphering AF ATO mandatory forms, such as the Information Technology Categorization and Selection Checklist (ITCSC), Privacy Impact Assessment (PIA), and Personally Identifiable Information Categorization Impact Level (PCIL) can be created automatically through conditional logic.

The user's answers can also populate fields in multiple forms. A Digital Asset leverages this to minimize memory load on both the user and the database by mapping provided answers to multiple forms and allowing for these form maps to be updated as forms change. ATO experts must maintain the maps.

Another critical area of improvement that an automated solution like Digital Asset can provide is to keep the user focused on one task at a time via a serial process guide or wizard. The current RMF process, even though it begins with Step 1, can be very confusing to non Subject Matter Experts (SME), since each AO may approach the process differently. With so many forms to complete and steps to take, the process is easily overwhelming and often results in inaction. To combat the potential "analysis paralysis" of where to start and go next with RMF and the subsequent delayed ATO journey, expert systems like Digital Asset should have a prescriptive flow that focuses the user's attention on one level at a time.

Another key element in assisting with ATO documentation is the elimination of archaic DoD-centric language whenever possible, and the use of plain English and a coherent series of questions which makes the user feel confident and successful every step of the way. Presenting questions about the Information System under scrutiny in a way that helps any stakeholder understand what is implied or required to answer the question allows for more users to complete forms and the ATO process.

Infusing Automation with the ATO Process

As referenced previously, the ATO journey can be long and arduous. However, by infusing some ATO-informed decision recommendations while leveraging automation gives the user some pre-decisional commentary, it's possible to notify and divert the user from making costly design mistakes that are incompatible with an ATO and drive them to build secure applications, when they can understand how design choices can affect ATO likelihood.

For example, during the initial assessment and analysis of how a system will achieve an ATO, questions posed around cloud hosting environments can help inform users which options are appropriate. Critical application hosting considerations such as whether the application lives in a commercial cloud versus an approved government cloud should be determined before an application reaches a feature-complete status. Expert systems with guidance on topics such as this can advise to the user that an approved government cloud supports an expedited path for an ATO versus a delayed path for the commercial cloud. These pre-decisional recommendations inform the user of design decisions and best practices while aligning with DoD Software Modernization and Fast Track Authorization initiatives.

A modular approach to the ATO process that is gated by the use of an expert system that provides categories that are revealed as users complete checkpoints, allows for an ordered effort that can be scheduled during the development phase of an

application. This is especially important when users are non-SMEs who can't appreciate the latitude that the RMF provides to evaluate the system. Within each module, users should only be prompted with questions that are relevant to the RMF Action Path. This prevents "analysis paralysis" during the RMF process and focuses the user's attention on one level at a time.

ATO pre-decisional recommendations are another, additional benefit of using automation and digital assets during the Prepare Step. ATO forms are complicated for laypeople to complete; however, when users have a tool that offers suggestions and recommendations as the user inputs their responses, they can correctly answer each question or identify what resources may be available to assist them.

To change a complex, paper-driven, compliance-based process toward operationally informed risk management, with quicker decision analysis, continuous monitoring, and continuous authorization, process automation is critical. Processes like ATO package development are particularly well suited for automating redundant steps like form completion and evidence collection and archiving.

As referenced in the DoD Faces Risk White Paper, Kevin Dulany, chief of the Risk Management Framework Division in the Office of the Secretary of Defense stated "If we leverage automation, I can get a more complete risk picture and I can do it more often. I can get more of an up-to-date picture, and I can be more efficient in finding my major problems and allocating my resources."

Case Studies and Success Stories

To further illustrate the effectiveness of agile authorization, this section presents case studies and success stories from 18F, a GSA collaborative group that has adopted similar approaches. It showcases tangible examples of how agile authorization has accelerated the approval process for training applications in various domains.

Rapid Iterative Development: Agile authorization allows for iterative development cycles, enabling continuous feedback and improvement. This approach can be applied to training applications, allowing them to be developed, tested, and refined in shorter cycles, leading to faster deployment and more efficient training programs.

Agile Documentation: Traditional authorization processes often require extensive and time-consuming documentation. Agile authorization promotes a leaner and more targeted documentation approach, focusing on essential information. This streamlining of documentation enables faster processing and reduces administrative burden without compromising compliance.

Cross-Functional Collaboration: Agile authorization encourages stakeholder collaboration, including trainers, subject matter experts, security personnel, and administrators. By involving all relevant parties from the early stages of the authorization process, potential bottlenecks and delays can be identified and addressed promptly, ensuring a smoother and faster approval process.

Continuous Stakeholder Engagement: Agile authorization emphasizes regular and transparent communication with stakeholders. This can involve frequent meetings, demonstrations, and feedback sessions. By involving stakeholders throughout the development and authorization process, the training applications can align more closely with their needs, reducing the likelihood of late-stage revisions and subsequent delays.

Agile Risk Assessment: Agile authorization allows for dynamic risk assessment throughout the development and deployment of training applications. Instead of conducting a single comprehensive risk assessment at the beginning, the risk assessment can be continuously updated as the application evolves. This iterative approach enables more effective risk mitigation strategies and expedites the approval process by addressing concerns in real-time.

Automation and Technology Solutions: Agile authorization can leverage automation and technology solutions to streamline the approval process. For instance, utilizing workflow management tools, automated testing, and continuous integration can significantly reduce manual effort and increase the speed of reviewing and authorizing training applications.

Compliance and Security Integration: Agile authorization can integrate compliance and security considerations directly into the development process. By incorporating compliance requirements and security controls from the outset, potential roadblocks and delays arising from separate compliance assessments can be minimized, allowing quicker approval and deployment.

Scalability and Flexibility: Agile authorization enables scalability and flexibility, making it easier to handle a large volume of training applications. By adopting agile practices, the Air Force can efficiently manage and prioritize the authorization process based on training needs and resource availability, ensuring faster turnaround times for approving applications.

These use cases demonstrate how agile authorization can expedite the approval of training applications in the Air Force, resulting in accelerated training for airmen and more efficient use of resources.

Conclusion

In conclusion, the delays faced by the Air Force in the ATO process for training applications demand a proactive and efficient solution. Agile authorization emerges as a promising approach to address these challenges and accelerate the approval of training applications. By embracing agile principles and practices, the Air Force can navigate the complexities of the authorization process with agility and effectiveness.

The benefits of agile authorization are significant. It offers reduced time-to-market, allowing airmen to access crucial training resources more rapidly. The iterative nature of agile authorization enables enhanced responsiveness to changing requirements, ensuring that training applications remain relevant and practical. The increased collaboration and stakeholder engagement fostered by agile authorization promotes streamlined communication, alignment, and collective decision-making.

Transparency and visibility are vital advantages of agile authorization, enabling all stakeholders to have a clear understanding of the authorization process's status and potential bottlenecks. By adopting lean documentation principles, bureaucratic layers are minimized, streamlining the approval process and freeing up valuable resources.

Moreover, the continuous improvement and risk mitigation aspects of agile authorization facilitate proactive identification and mitigation of risks, leading to a more robust and secure training environment for airmen.

The time has come for the Air Force to embrace agile authorization fully. By implementing agile authorization principles, streamlining processes, and leveraging technology solutions, the Air Force can expedite the approval of training applications, reduce administrative burden, and empower airmen with timely access to critical resources.

In this era of rapid technological advancements and evolving training needs, embracing agile authorization is not only a strategic goal but a necessity. The Air Force must seize the opportunity to revolutionize its ATO process and pave the way for accelerated training for airmen.

Let us forge ahead with determination, embracing the agile authorization approach, empowering airmen, and ensuring our readiness to meet the challenges of the future. By adopting agile authorization, the Air Force will position itself at the forefront of innovation and effectiveness in training application approval processes. Together, let us embark on this transformative journey and unlock the full potential of our airmen.

TERMS & DEFINITIONS

Assessment and Authorization (A&A)	An assessment of information system policies, technical / non-technical security components, documentation, supplemental safeguards, policies, and vulnerabilities. Reviewed by the Authorizing Official (AO), resulting in either an Authorization to Operate (ATO), ATO with conditions, or denial of authorization to operate.
Authorizing Official (AO)	An official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals.
Authorization to Operate (ATO)	The official management decision given by a senior organizational official to authorize the operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets,

	individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.
Development, Security, & Operations (DevSecOps)	An approach to culture, automation, and platform design that integrates security as a shared responsibility throughout the entire IT lifecycle.
IT Categorization and Selection Checklist (ITCSC)	Per AF Policy, the Program Manager/RMF Team must fill out this form during the Prepare Step to identify and prepare for the management of cybersecurity and privacy risks. The impact of confidentiality, integrity, and availability is categorized into one of three designations (low, moderate, or high) to address the impact of a potential loss of data. By signing this form, it documents the PM and AO concurrence on Categorize and Select elements.
Privacy Impact Assessment (PIA)	Also known as DD Form 2930, the PIA identifies impact and categorization of a system that has PII and Personal Health Information (PHI).
Personally Identifiable Information (PII) Confidentiality Impact Level (PCIL) Categorization Worksheet	The AF worksheet used as a follow on step to the Categorization Step. It is intended to help the user select the PII Confidentiality Impact Level and corresponding Privacy Overlay. According to the AF, the PCIL is different from, and does not equate to, the impact values for the security objectives of confidentiality, integrity, and availability for the system overall, which are used to determine the security control baselines.
Risk Management Framework (RMF)	A structured approach used to oversee and manage risk for an information system.
System Development Life Cycle (SDLC)	A conceptual model used in project management that describes the stages involved in an information system development project, from an initial feasibility study through maintenance of the completed application.

REFERENCES

18F Digital Service Delivery “Agile” Use Cases.
https://18f.gsa.gov/tags/agile/

Committee on National Security Systems (CNSS) Glossary. (2015).
https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf

Cordell, C. (2018, May 13). 18F slices ATO 18 times from 6 months to 30 days. FedScoop.
https://www.fedscoop.com/18f-slices-ato-times-6-months-30-days/

Hunter, T. (2023, January 20. The 11 Most Important Benefits to Agile, According to Experts. BuiltIn.
https://builtin.com/agile/benefits-of-agile

Konrad, C. (2018, April 25). Adopting Agile Principles in Cybersecurity. World Wide Technology.
https://www.wwt.com/article/adopting-agile-principles-cybersecurity

Lazzeri, M. (2021, February 4). ATO ASAP: Let’s finally fix the security compliance problem.
https://fcw.com/it-modernization/2021/02/ato-asap-lets-finally-fix-the-security-compliance-problem/258357/

NIST Risk Management Framework. (2022). Computer Security Resource Center.
https://csrc.nist.gov/Projects/risk-management/about-rmf

Noel, J. (n.d.) How TurboTax turns a dreadful user experience into a delightful one. Appcues.
https://www.appcues.com/blog/how-turbotax-makes-a-dreadful-user-experience-a-delightful-one

Nyte, R. (2018, November 20). The Why of Agile. World Wide Technology. https://www.wwt.com/article/the-why-of-agile

Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. (2018, December 2). Computer Security Resource Center. https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final

Snyder, D., Powers, J., Bodine-Baron, E., Fox, B., Kendrick, L., & Powell, M. (2015). Improving the Cybersecurity of U.S. Air Force Military Systems Throughout Their Life Cycles. https://www.rand.org/content/dam/rand/pubs/research_reports/RR1000/RR1007/RAND_RR1007.pdf

United States Air Force. (2022, June 10). Department of the Air Force Guidance Memorandum (DAFGM) to Air Force Instruction (AFI) 17-101, RISK MANAGEMENT FRAMEWORK (RMF) FOR DEPARTMENT OF THE AIR FORCE INFORMATION TECHNOLOGY (IT). Washington, DC: United States Air Force.

United States House of Representatives. (2022). H.R. 7900—FY23 NATIONAL DEFENSE AUTHORIZATION BILL. Washington, DC.