cATO Manifesto

Rise8

© 2023

Table of Contents

© 2023

Manifesto for a Continuous Delivery Risk Management Framework (CD-RMF)©

AKA THE C-ATO MANIFESTO

Manifesto for a Continuous Delivery Risk Management Framework (CD-RMF)© 2023 by Rise8, Inc. is licensed under CC BY-ND 4.0. This license requires that reusers give credit to the creator. It allows reusers to copy and distribute the material in any medium or format in unadapted form only, even for commercial purposes.

Introduction

We believe that achieving continuous delivery as part of DevOps in the federal government, subject to FISMA, requires a truly continuous application of the NIST Risk Management Framework (RMF). While this can be done within the letter of NIST 800-37r2, we intend to advocate for a new authorization type or a new subset of ongoing authorization. This would require a particular implementation of the RMF for Continuous Delivery as part of Agile Software Development & Operations.

The US Air Force pioneered such an implementation which resulted in a Continuous Authority to Operate (cATO). Since then, there has been little consensus on what a cATO is, much less how to implement the RMF to achieve one. In fact, many cATOs have completely diverged from RMF and cannot be considered FISMA compliant. **For that reason, we are proposing the term "cATO" no longer be used.** Even if the poor practices could be cleaned up, the name itself is problematic and cannot be found as an authorization type/decision within NIST 800-37. It was always intended to be a very opinionated subset of ongoing authorization with prescribed practices. We hope to codify this under a new authorization type/decision.

This manifesto and the playbook aim to align the community around achieving the "early and continuous delivery of valuable software" in federal government as promised by the *Manifesto for Agile Software Development*. Given that, we have intentionally stayed true to the format and content of the Manifesto, highlighting how compliant DevOps naturally fits in.

This artifact draws heavily from the Manifesto for Agile Software Development, which can be found at: https://agilemanifesto.org/

2024-03-23 23:56:48

© 2023

The 8 Values

> “We are uncovering better ways of [managing security and privacy risk] by doing it and helping others do it. Through this work, we have come to value:”

1. **Proactive Prevention over Reactive Remediation**
   - While we recognize the importance of addressing vulnerabilities and breaches, we prioritize building systems that prevent these issues from arising in the first place.
2. **Automated Assurance over Manual Checks**
   - While manual checks have their place, we believe in harnessing the power of automation to ensure RMF standards are consistently and efficiently met.
3. **Continuous Collaboration over Siloed Departments**
   - Rather than isolating teams with differing incentives, we value the synergy of development, operations, and risk management teams working together to achieve common goals.
4. **Adaptive Frameworks over Rigid Rulesets**
   - While certain standards are non-negotiable, we believe in a flexible approach, as encouraged by the RMF, that can adapt to new challenges, technologies, and learnings without compromising security or privacy.
5. **Real-time Feedback over Periodic Audits**
   - While periodic reviews are necessary, we prioritize systems that provide instant feedback on security and privacy risk, enabling immediate actions and adjustments.
6. **Team Education over Enforcement Only**
   - Instead of just imposing rules, we value educating teams on the importance of RMF, fostering a culture of shared responsibility and awareness.
7. **Transparency in Processes over Obscurity**
   - We believe in clear visibility into our RMF processes, technologies, and their outputs, ensuring that all stakeholders understand, trust, and can validate our approach at any time.
8. **Tailored Implementations over One-size-fits-all**
   - While generic solutions can provide a foundation, we prioritize implementations that meet the unique mission objectives for each organization.

> "That is, while there is value in the items on the right, we value the items on the left more."[^1]

This artifact draws heavily from the Manifesto for Agile Software Development, which can be found at: https://agilemanifesto.org/

2024-03-23 23:56:48

© 2023

The 12 Principles behind the Manifesto

We still believe that the *Agile Manifesto for Software Development's principles* have withstood the test of time and are completely relevant to, and perhaps always included, security and privacy. We therefore offer them here with slight refactoring to emphasize what has always been true:

1. "Our highest priority," even as security professionals, "is to satisfy the customer through early and continuous delivery of valuable software."
2. "Welcome changing" software, at any stage of the system's lifecycle. Agile risk management "processes harness change for the customer's competitive advantage."
3. "Deliver working software frequently," even as often as multiple times per hour, "with a preference to the shorter timescale," without increasing security and privacy risk.
4. Security & Privacy professionals, "business people, and developers must work together daily throughout the project."
5. "Build projects around motivated individuals. Give them the environment and support they need, and trust them to get the [risk management] job done," and implement the right controls in the right way.
6. "The most efficient and effective method of conveying information to and within a development team is face-to-face conversation" or via APIs. Any GRC should be written in code with automated workflows to the greatest extent practical, not in static documents.
7. Mission outcomes in prod are still "the primary measure of progress," and risk professionals should view themselves as protagonists.
8. "Agile [risk management] processes promote sustainable development" and operations. "The sponsors, [the cross-functional team], and users should be able to maintain a constant pace indefinitely."
9. "Continuous attention to technical excellence and good design," which includes information security and privacy, "enhances agility."
10. "Simplicity--the art of maximizing the amount of work not done--is essential."
11. "The best [privacy/security] architectures, requirements, and designs emerge from self-organizing teams."
12. "At regular intervals, the [cross-functional] team reflects on how to become more effective, then tunes and adjusts its behavior accordingly."

This artifact draws heavily from the Manifesto for Agile Software Development, which can be found at: https://agilemanifesto.org/

2024-03-23 23:56:48

© 2023

History: The Evolution of Continuous Authority to Operate

It is important to understand that this has already been done.

On April 18, 2018, in an Air Force memorandum titled “Implementation of Ongoing Authorization for Agile Software Development”, Authorizing Official Lauren Knausenberger, then Air Force Director of Cyberspace Innovation, approved the first so-called “Continuous Authority to Operate” (coined by Bryon Kroger) implemented by Kessel Run.

Kessel Run had stood on the shoulders of giants, such as 18F’s accelerated ATOs on cloud.gov and NGA’s ‘ATO-in-a-day’ for their GEOINT Services Platform, but they were the first to implement the Risk Management Framework in a way that fully aligned with the Agile and DevOps SDLC without tradeoffs between speed and compliance/risk, and included the full-stack implementation and assessment of the associated controls. Kessel Run, at the time, could produce a full, up-to-date authorization package for every release in real time.

The first applications to achieve this were Raven and Marauder, both deployed to an on-premise cloud stack running Pivotal Cloud Foundry (like our friends at NGA) on the SIPR network. The Kessel Run team, led by Bryon Kroger and Andrew Altizer (ISSM), implemented this combination of people, process, and technology for an ongoing authorization that was tailor made for DevOps with deployment frequencies measured in hours. Bryon coined the term “cATO” to describe that **specific implementation of an ongoing authorization within RMF to enable true continuous delivery.** Some of the technology and process underpinnings were adapted from NGA and 18F, while some were changed or added.

Unfortunately, the cATO would take on a life of its own and headed in a different direction, away from an RMF-based controls implementation, assessment, and authorization to something based on political favor and a particular reference design that required the use of certain technologies, at odds with the RMF’s technology neutral stance. Senior leaders also began to espouse “certifying the people and the process”, instead of systems themselves and, unfortunately, placed their trust in the wrong people who weren’t even practicing the RMF-deficient method they were preaching.

During that time, Bryon Kroger left the Air Force and founded Rise8, where we have continued advancing RMF for continuous delivery, improving both process and automation. It has been difficult, however, to get the community to adopt this rigorous approach given that many organizations were able to get all the benefits of being able to continuously deploy their software without doing the work. It’s a close cousin of Shadow IT: Shadow ATO.

Thankfully things started to change when the DOD CIO published a cATO memorandum that most insiders would describe as an attempt to clean up the mess of existing cATOs.

While this was great to see and a cleanup is much needed, we believe it misses the mark on how to apply NIST RMF to continuous delivery. The office has not consulted the actual practitioners who have implemented a truly RMF-based authorization for continuous delivery and, as of this writing, are writing additional guidance without doing so.

That is why Rise8 authored the manifesto and are making our playbook for CD-RMF public. Additionally we are forming a group of like-minded experts to lead an open source community that continues advancing CD-RMF.

2024-03-23 23:56:48

© 2023