ENTERPRISE MANAGEMENT

INTERVIEW SERIES
INNOVATION IN GOVERNMENT®

Empowering ATO Decision Making: Streamlining Risks with RegScale

A conversation with Travis Howerton, Co-Founder and CEO at RegScale
and Brandt Keller, Software Engineer at Defense Unicorns

TECHNICAL SUMMARY

The quest for efficient risk management and streamlined Authority to Operate (ATO) decision-making processes has become paramount for government agencies. Continuous controls monitoring, automation's influence on ATO procedures, strategies for efficiency improvement, minimizing handoffs and building trust among stakeholders are at the forefront of cybersecurity discussions.

RegScale is a pioneering continuous controls monitoring platform that plays a pivotal role in rethinking and modernizing ATO RMF packages. By leveraging innovative technology and expertise, RegScale aims to streamline ATO decision-making processes and enhance risk management practices that have stalled innovation and added corrosion to the compliance processes today.

Question: With the increasing sophistication of cyber-attacks and threats, how can Government agencies adapt their approval process to stay ahead of emerging risks and vulnerabilities?

Howerton: The cadence mismatch between rapidly evolving cyber threats and slow manual compliance processes needs to be addressed. To modernize, automated approaches leveraging technology advancements are crucial to align compliance with the speed of DevOps, unlocking digital transformation. Moving beyond a controls-based mindset, emphasizing the importance of threat modeling and dynamic defense strategies is essential for enhancing security practices.

Keller: I want to emphasize the importance of shifting compliance evaluation left in the introduction of new technology. Understanding the impact on compliance when transitioning between technologies is crucial. Compliance should play a controlled role in the DevOps process and should be monitored from various angles. Looking ahead, integrating compliance as an additional layer of defense can enhance security practices. Continuous evaluation of compliance can alert to any deviations, prompting investigation into potential risks or malicious activities within the environment.

Question: How do you effectively balance the need to outpace cyber threats while maintaining thoroughness in the ATO approval process, considering the importance of speed and efficiency in today's cybersecurity landscape?

Howerton: I think it is a false choice to say I need speed or thoroughness. As an Authorizing Official (AO), you must balance both to minimize risk to the agency. Providing timely answers is crucial as we serve mission owners and aim to protect critical information. Technology advancements now allow us to achieve both speed and thoroughness, enabling better risk-based decisions and timely support for our mission.

Keller: There is a process piece involved with finding a better way to do something. I want to invest the time in this area as it offers the most value return. Instead of following a strict set of steps, it is about identifying what is critical and important. It is essential to focus efforts efficiently, considering the limited time available. Once you understand what needs to be done, it is crucial to plan how to achieve it effectively. By ensuring thoroughness and setting up for future success, you can establish a reliable process. This confidence allows you to prioritize tasks and address the next challenge effectively.

> ***You just give AOs superpowers by giving them better data, and just getting rid of all the burden. – Keller***

Question: Can you share some common pitfalls or challenges during the ATO approval process, and how that can be mitigated effectively?

Howerton: Documenting dynamic systems on static paper is increasingly failing as systems evolve quickly, especially with cloud data. Instead of static authorizations, can we continuously assess systems based on controls and telemetry? Spending 80% of our time on static paperwork is inefficient. We should focus on providing context and insights from data to improve compliance and security. Compliance should not be seen as equal to security, but as a set of best practices lacking context. The ATO process is paper-intensive, static and costly, hindering real-time decision making for AOs. It is time to modernize and empower AOs with better tools and real-time data for effective decision making.

Keller: I think continuous compliance needs to continue to be the goal. Meeting people where they are is crucial. Bridging the gap between having continuous data and data that is continually updated is essential. Automated governance in DevOps processes has seen a rise in performing compliance checks on commits. This allows for reassessment of data in a timely fashion. Striving for systems and standards that support continuous data is important. Ensuring accessibility and availability of data is key, especially in disconnected environments. Open standards underpinning continuous systems are vital for providing data to AOs in a recognizable format. Avoiding proprietary formats reduces processing time and promotes innovation. Casting early votes for ATO readiness can streamline the process and prevent last-minute rushes for accreditation renewals.

Question: There is a concern about potential drift in the ETL process over time. How can we prevent this drift between what was initially submitted and the current state of the system?

Keller: Focusing on efficiencies in data collection and reporting is crucial for preventing drift. It is important to be active in collecting and reporting data to show the current state. Starting with open standards can help leverage data effectively without the need for a proprietary platform. Automating control by control and ensuring repeatability and reproducibility are essential. Automation can streamline tasks, making them quick and repeatable. It is vital to ensure that changes do not lead to compliance issues and to have checks in place to prevent drift. Implementing checks in the production pipeline can help halt deployments that may lead to non-compliance. Instrumenting different components and projects can provide visibility and facilitate modifications. Understanding the relationships between different elements is crucial for maintaining compliance in platforms like RegScale.

> ***The key is to strategize on applying automation to ensure seamless handoffs, eliminating the need to rely on chance for the completion. By doing so, we can guarantee that these handoffs have occurred, enabling data to reach you swiftly and in a consistently formatted manner – Howerton***

Travis Howerton | Chief Executive Officer, RegScale

Travis Howerton is the Co-Founder and CEO at RegScale. Travis comes from a federal background as the former Chief Technology Officer of the US nuclear weapons program where he led Oak Ridge National Lab's digital transformation program globally.

Brandt Keller | Software Engineer, Defense Unicorns

Brandt Keller is a software engineer at Defense Unicorns, specializing in defense technology solutions. With a strong foundation in architecting systems that require ATOs, Brandt brings a unique perspective to the team.

ADDITIONAL RESOURCES

Tech Spotlight →

AO Perspectives Webinar →

RegScale →

CONTACT US

Regscale@carahsoft.com • (888) 662-2724 • https://www.carahsoft.com/Regscale