carahsoft

Produced by: GovExec

GOVFORWARD®

FedRAMP Headliner Summit:

Streamlining FedRAMP Authorizations with Automation and Data Standards

FEATURED SPEAKER:

Anil Karmel,
Co-Founder, RegScale

Streamlining FedRAMP Authorizations with Automation and Data Standards

Featuring: Anil Karmel, *Co-Founder, RegScale*

Good afternoon, everyone. So, we've had a great day of conversations around FedRAMP and ways to streamline the authorization process. Now we're going to add a concept around how do you leverage automation, what you heard on the prior panel and throughout the day, and data standards to help streamline that process. So, before I kind of step into that, let me kind of take you on a journey of how we got here and why this is a concept that needs to be considered and thought about, perhaps in a different way. So, by way of background, how many have watched the movie Oppenheimer? Couple folks, all right. So, if you watch the movie, Oppenheimer, that is actually where I spent a decade of my life.

So that gives you kind of context, I spent 10 years at Los Alamos National Lab, had the opportunity to build their cloud and collaboration platforms on the classified and unclassified network, and ended up having to write the compliance documentation for all of that. So, I'm an engineer, my boss said, you have to write an SSP. I'm like, what's an SSP? I get handed a binder of NIST 853. I'm like, What's this? Spend 30 days in a room, right and control implementation statements and gathering evidence. And going, this is not fun. So, my fellow co-founder and our CTO, Travis Howard, and he came out of Oak Ridge National Lab, which is also in the movie Oppenheimer. And then we ended up serving as the CTOs of the US nuclear weapons program, the NSA. So now we're on the other side of the table, having to sign off as the Ayios on these compliance artifacts going this is really not scalable. There's got to be a better way to kind of think about how you scale compliance and bridge the divide between security and compliance.

Let's start with why is compliance so hard?

Well, let's think about the world that we live in today. Everyone is trying to transform their organizations, right? But compliance is the paperwork problem that is inherently challenging, and that you have to create. So how do we do our compliance today? It's documented in Word docs, in spreadsheets, stored in file servers, and we built these great processes to keep everything up to date. And then when we have to go gather evidence, we gather data from all of these different monitoring systems. And then when we find an issue, what are we doing, we're sending emails and Outlook, or we're opening up JIRA tickets or ServiceNow tickets to go address issues. And we got to do this across FedRAMP. If you want to get a FedRAMP accreditation, or multiple standards and frameworks, right, so you got to do it for CMMC, the upcoming standard for ISO 27,001. And you got to do it for every app you have.

So, you have different apps in different geographies and different business units. All of this takes a lot of time, it takes a lot of people and a lot of paper to generate, right. The problem with this is, when you think about it, you've got all these different data sources where your data lives today. And you have it takes a long time to free to react to threats, and compliance issues. Because the compliance paperwork is done at a point in time, it's not in real time. So, when you finally find an issue, you're reacting to something that already happened. So, you don't really have any real visibility into your control state. And you're making decisions based on inconsistent data. And this is fundamentally the challenge. So, what I'd like to kind of posit is, is there a better way to think about this problem?

So, the reality is a decade ago, something was created to solve this problem. So, I'm an old school sysadmin, right. So as this old school sysadmin developer would say, I have this great app, I want to go put it into this environment.

So as this old school sysadmin developer would say, I have this great app, I want to go put it into this environment. It's like great, I have to go test all this stuff. And then I have to go validate it, and then go put it in the environment. Well, obviously, that took a lot of time. So, there's this thing called DevOps that was created. So how many people know what DevOps is? All right, so most hands go up here. So, this is the AWS definition of DevOps. So, there's a million different definitions of DevOps. I'm just putting one up here for your consideration.

Applying DevOps Principles for Faster, Smoother Compliance

This discipline was created to take cultural philosophies and practices and tools and transform culture to allow organizations to deliver applications at high velocity, faster than the traditional approach of handing it back and forth. So how can you take the principles of DevOps and apply it to compliance? Well, I'd like to posit a definition for regulatory operations, or reg ops, right. So, this is a transformation of cultural philosophies, practices and tools to increase an organization's ability to ensure compliance of your applications and services against whatever your standards might be at a hive Velocity, right? So, because right now what are we doing point in time compliance? Well, what if we apply those disciplines of DevOps to compliance, right? In this new model. Now that something happened with DevOps is this thing called Agile. So, to really employ DevOps, you have to employ agile, right?

So, there was an agile manifesto that was created. So, in the vein of reg ops, I'd like to posit a compliance manifesto that mirrors an agile manifesto. So, number one, regulations exist to maintain our privacy while keeping us safe and secure, we should honor that the problem is not the regulations, or the compliance standards, or the frameworks. The problem is how we demonstrate compliance against those standards and frameworks, the way in which we're doing it is the problem. maintaining compliance as a business should be affordable, transparent and easy. This is really challenging and takes a lot of time and money. That's why we're all here of how can we streamline this process?

Revolutionizing Compliance Through Automation

We've employed automation in every area of our lives, when it comes to security, we haven't done it in compliance. So, if there are repetitive processes, from a compliance standpoint, we should automate them, they're good for the business, they're good for the regulator, they're good for the people that are doing the work, because now you can do more value-added activities, right? As you're conducting these audits, it shouldn't be, oh, boy, I'm going to have an audit, I'm going to fail these controls. If you're doing this on a continuous basis, you should be doing to sell where your audits are less risky. And they're simpler, right? And the evidence is readily accessible for you to use. And creating these artifacts should be profitable for the producer, and cheaper for the consumer. So that way, you're not having to create these mountains of paper that nobody wants to write, and nobody wants to read, you're doing so in a repeatable way, where it's an outcome of good security, and you're able to reuse this information across different disciplines.

Navigating the Ever-Changing Technological Landscape

Now, the one thing that is a standard in our lives is technology will always change. The tools that we have today are going to be completely different than the tools that we have 10 years from now. So, anything that we implement today must be extensible to take advantage of these future innovations. So, we should be building on compliance standards. And ultimately, whatever we do, if it doesn't improve our privacy, if it doesn't improve our safety or security, we shouldn't do it. So, these are just a couple thoughts to consider in the vein of a compliance manifesto.

So, there's a couple things that you need to consider when you bring the principles of DevOps to compliance. So, number one, API's, we live in a world where API's are how systems talk to each other. So, leverage API's and API

centric platforms to connect your tools and your environment. Use scripts, use DevOps, to connect those API's to your systems, developing repeatable playbooks based on your needs. You see ICD pipelines, right CI/CD pipelines were born as an outcome of DevOps. So, leverage CI/CD pipelines so that as soon as applications are built, the compliance can be attested to in near real time and the compliance artifacts can be created. And then tie IoT devices to all of this. So now when you think about how DevOps was created, right. And DevOps, CI/CD pipelines are created to output applications at high velocity and environments. What if you have reg ops GRC pipelines that output a continuously compliant artifacts in near real time? Same idea, so let's take that to a more tangible notion and leverage standards.

Open Security Controls Assessment Language (OSCAL)

So how many people are familiar with the open security controls assessment language off scale? Okay, most hands are up. So, we're at the FedRAMP headliner Summit. So ultimately, this is around OSCAL. So, this is a collaboration between NIST and FedRAMP. Right to allow a standard Rosetta Stone, if you will, to have a standard way to represent controls and catalogs and systems security plans and assessment plans and results in either XML, JSON or Yamo, or a Word doc or Excel spreadsheet, right? So, and this has full backward traceability back to the control. So, you can take you can start from a system security plan and have an individual unique UU ID and a control and tie that all the way back to a catalog. Right? So, I'm not going to go into full detail here because this could take a whole another 20 minutes. So, but at the at a high level, everything starts with a catalog of controls.

You have a catalog of controls; you select what those controls are. So, from that catalog, you have a baseline. We have the new FedRAMP baselines that were published in Moscow. So then from that baseline is a subset of controls from those catalogs. You take that, that profile and you create a system security plan off that profile. That system security plan has all the controls that are relevant to your particular information system and the control implementation statements for that particular system, then you do a system assessment plan or a sap, right, testing those controls. And then once you've tested those controls, you create a SAR or System Assessment Report validating that, yes, I've done these tests, here's the report. All those artifacts are hundreds and hundreds of pages of Word docs, and Excel spreadsheets, that can actually now be turned into JSON, or XML and turn back into those Word docs or Excel spreadsheets as you need. So, this is kind of this new model of a standard.

Shifting Left: Transforming Compliance into a Connected, Continuous, and Scalable Process

So how does this all come together? How can you actually shift left? So, this is the world we live in today, right? Manual Doc's manual spreadsheets, right? Manual processes to create all our compliance artifacts, right. So, shift left, how many are familiar with the concept of shift left? Okay, so a couple hands. So, shift left is the process of trying to find security issues before they happen.

You have all these different tools that are scanning your environment today finding issues. And when you find issues, these tools automatically create tickets in your ticketing systems like ServiceNow, or JIRA. Or in some cases, you're sending emails back and forth and outlook. But again, we're still doing all our compliance docs and Word docs and Excel spreadsheets and storing them in file servers and across FedRAMP packages and whatnot. So how do you shift left compliance and make compliance like security, fully connected, fully continuous and fully scalable?

The Power of GRC Data Lakes and API-Centric Approaches

The first step on this journey is, you've got to take all those compliance artifacts and all the things that you're doing and get them into a central repository. Think about this as a GRC data lake, we have all these security data lakes

that we've created, but what about for compliance. So, what you need is a GRC, data lake to bring all this information together, bringing in both the human experience for a human to manually go test and assess these controls. And then the tools that are doing the automated assessments into a single repository, so that you can output the documentation that you need, on demand in that Word doc, in that Excel spreadsheet, in that auto scale, JSON or whatever format that your regulator needs for whatever standard or framework leveraging an event driven architecture, right. So, this is that concept of real API's and an API centric approach, having your data available in near real time understanding what your controls are in your real time.

Now you can go query your GRC data lake using Graph QL. And understand, what are my gaps from a control standpoint? What are my actual risks in near real time and then be able to use this information across multiple standards and frameworks. When you think about shifting left both security and compliance, again, that first step is to digitize those compliance artifacts and get them into a system of record. So, this is traditionally where GRC tools end and this is where API centric tools begin, because GRC tools are only as good as you humanly feed them. Most people take data, and they work in Excel spreadsheets and Word docs, and then go push it back into the GRC tool.

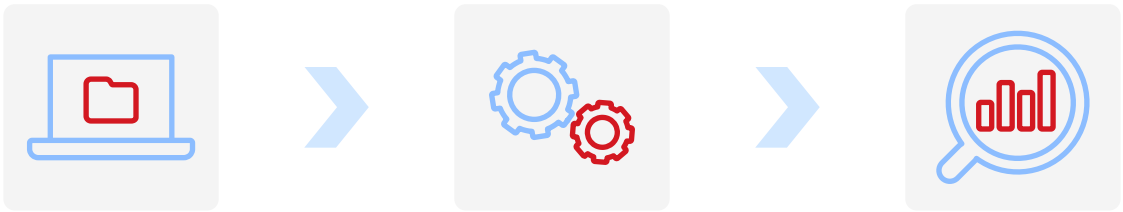
So, let's get the data into the platform. And then integrate with the tools you already have in your stack, right your scanning tools, right your compliance platforms, you may have compliance systems of record that you need to go feed, right. So, integrate with those tools so you can do your work in a platform and then go feed your compliance systems of record, then be able to transform that data in the format that the stakeholders need to see it. So output, your FedRAMP SSP. And all the artifacts in the FedRAMP SSP and SAP and SAR and SRTM templates that organizations need to see on demand. And it's always right as opposed to you having to manage and maintain all those documents outside the system. This enables output in NuSTAR scale JSON, facilitating uniform compliance reporting across diverse standards, frameworks, geographies, and business units. And because of your API centric using business intelligence tools that you already have Power BI Tableau Domo Qlik Sense to dynamically visualize your state of compliance and risk in near real time.

A Six-Step Approach to Optimizing Compliance

Step 1:
Centralize Compliance Data
Gather all compliance artifacts and data into a unified GRC data lake.

Step 2:
Embrace API-Centric Automation
Integrate human assessments and automated tools using real APIs for continuous, real-time access.

Step 3:
Utilize Graph QL for Analysis
Query the GRC data lake with Graph QL to identify control gaps and real-time risks.



Step 4:
Digitize Artifacts
Move from manual to digital records, ensuring accuracy and consistency.

Step 5:
Integrate Tools and Systems
Connect existing tools and compliance systems for streamlined data flow.

Step 6:
Visualize with Business Intelligence
Utilize tools like Power BI and Tableau for dynamic, real-time compliance visualization across standards, frameworks, and geographies.

Transforming Governance, Risk, and Compliance through Standardization and Automation

So, this is kind of a new way to think about How to Do governance risk and compliance. Because the way we do compliance today is hard, right? It's a tedious, manual, time consuming exercise to try and do that across multiple standards and frameworks is exponentially hard. You try to do that across multiple geographies, different lines of business, different products, different tools, this is impossible at scale. So, you've got to leverage standards.

NIST has created standard, the open security controls assessment language to provide this Rosetta Stone to create these artifacts in a standardized manner. And then there are free tools available, we have a completely free community edition that you can download that allows you to start on this journey to create your own Rogowski or see pipelines to output continuously up to date documentation.

Embracing the Compliance Journey with RegScale

So ultimately, the takeaway here is,

> "Automation is the only way we're going to get ahead of this, we're never going to be able to bring enough people and enough paper to demonstrate compliance against all the standards and regulations that are growing because of the rise of AI and new technologies."

You need a way to keep your compliance artifacts continuously up to date, where compliance becomes an outcome of good security.

Reuse the documents and artifacts that you have collected, right across multiple standards and frameworks. So, you're assessing once and reusing it many times, and then rethink how we're doing compliance today. Take the principles of DevOps, apply them to compliance and this discipline you can think of as regulatory operations.

Whether you're a cloud service provider aiming to accelerate your FedRAMP journey, an advisor assisting clients, a 3PL evaluating organizations on their FedRAMP path, or a Federal agency grappling with compliance complexities, this innovative approach is pivotal. This is why this this approach is so important and why RegScale exists. It's why we built the platform because this is ultimately a problem that can only be solved if you've holistically looked at it and created a new approach to do so. With that, I thank you very much for your time.