Harnessing Compliance as Code: The Future of Audit Readiness

A conversation with Travis Howerton, Chief Information Officer, RegScale and Christine Horwege, Consulting Expert, CyberFathom

TECHNICAL SUMMARY

As systems become more dynamic and ephemeral, static paper-based approaches are causing organizations to lag in compliance. It is crucial for organizations to begin utilizing automation technologies, like auto-scale language or automated language and scripting, to avoid the inability to operate due to outdated processes. Integrating AI/ML and automation into compliance processes can improve efficiency, accuracy, and adaptability, making compliance as code the path for the future of audit readiness.

Question: How would compliance as code challenge the traditional paper-based compliance process?

Howerton: When people think compliance, they think controls and they think government mandates and regulation. But a lot of that is just a collection of best security practices. It gives you a baseline of how well you are doing against the standards and best practices in the industry. The problem is, how much it costs, and it goes back to the paper problem. Too much paper is generated and decays too fast now at the speed things are moving. All the cost is going into the thing that has none of the value. The audit compliances code can flip it on its head, where all the cost is going into the thing that is valuable, and it is more cost effective and time efficient.

Question: What is compliance and how do we shift people's thinking in a more positive direction?

Horwege: Security and compliance are not the same. Just because I am compliant does not mean I am secure. Start with security. The key there is to think about control objectives, it is not about the singular controls that you are doing, it is about, 'What is the objective you are trying to achieve?' Once you have identified the risk, then you determine what you need to secure for, what you are trying to achieve and your objective there. Compliance is just those few extra steps that meet additional line items' key requirements.

Howerton: I tend to move away from the concept of the term "control," I use "response." How are you responding to this? If you think about all our shared services, control structures or policies, we do the checks and balances to ensure things are working. It is that productive force of, "How do I manage what I am doing, keep everything standardized and also make sure I grow the business and innovate?" I think a lot of times innovation gets pushed to the side over ensuring that you are complying. You need to make sure you are staying even on both sides.

Question: What are the benefits of compliance as code?

Howerton: I get risk reduction, always audit ready and cost reduction. We can bring new technologies on faster. There are tons of benefits to rethinking it. Machines should attest to their own state, they should post their own audit evidence of 'I am in this secure state.' You should be able to grab it anytime you need it. And so, timeliness gets more accurate. What makes it also important is that it is in a digital format that is readable. Compliance and audits require precision, and you get precision by having better structured data.

Horwege: I think compliance is about preventing and detecting. But when it comes to compliance, we can easily look at entity to entity activity, and use that to then drive baselines and understand how to reduce those costs. This is where we have the opportunity with all this digital information and the way we can capture. You can store a lot of this in a document management system and then be able to access it and do it very easily. That gives you the near real-time approach that organizations need just to operate.

Harnessing Compliance as Code: The Future of Audit Readiness

Question: What is the role of compliance as code in bridging the divide between security, risk and compliance?

Howerton: By putting controls in one place, you can get a good baseline that incorporates your security environment, threat environment and operational environment. So that is what we mean by bridging. And then, once it is there, what you want to do is manage those controls efficiently through their lifecycle with automation and AI. Being able to collect evidence with automation can save a lot of money. Then asses it with an AI-based auditor to fix the issues found. All along the way, you are going to make risk-based decisions around what you can afford to do, what the technology you count on is able to do and then you are going to make governance decisions.

Question: How do you start on the path to achieve compliance as code?

Howerton: Start with standards because this is an emerging space. Try to adopt a standard and get your developers on board early so that everything as code is not just a security mandate, it is an operational mandate. Bring your developers onboard with you to get to where you ultimately want to be.

Howerge: My answer was requirements; you need to know what you have to do. What are the rules? I think at that point, also going back to having the open discussion with your developers and your different IT functions to say, "what are the constraints?" You really have to look at what you are incentivizing, what your strategy and your objectives are for your organization. Then, align everything and make sure everybody is on the same page and understands the value and the why.

> ***Compliance and audits require precision, and you get precision by having better structured data. – Howerton***

Travis Howerton | Chief Information 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.

Christine Horwege | Consulting Expert, CyberFathom

Christine Horwege is a Consulting Expert at CyberFathom where she works with companies consulting on how to think about risk and compliance as well as governance. Christine started off in compliance when she worked as an engineer officer for a combat engineer group in the Army.

ADDITIONAL RESOURCES

Tech Spotlight →

Blog: CISO Focus Group →

Blog: OSCAL-Native Tools →

RegScale | carahsoft.