The Cybersecurity Readiness Podcast Series

Episode Title	Compliance in the Cloud: Challenges and Best Practices
Podcast Series	The Cybersecurity Readiness Podcast Series https://www.cybersecurityreadinesspodcast.com/
Host and Producer	Dave Chatterjee, Ph.D. https://dchatte.com
Guest	Dale Hoak, Director of Information Security at RegScale
Summary Pitch	Accelerating into the cloud without caution often brings complexities that can cause more harm than good. Gartner has noted that cloud configuration errors cause 95% of cybersecurity breaches. With the rapid pace of cloud adoption, less time is spent ensuring systems are built and operated effectively with proper cyber hygiene. In this episode, Dale Hoak, Director of Information Security at RegScale, joins me in discussing cloud compliance-related challenges and best practices. Here are some terrific Dale Hoak one-liners: "Compliance is essentially where fun went to die." “Compliance is the enemy of innovation.” "Nobody steals your work. So, we need to use automation to do the work." "Compliance is a key driver of trust in our world." **Action Items and Discussion Highlights** • Invest in automation to gather and maintain compliance evidence. • Implement "compliance as code" to bake compliance into the software development lifecycle. • Automate change management processes to speed up compliance reviews.

	• Establish a single pane of glass to prioritize and manage compliance issues. • Conduct regular manual reviews to validate automated compliance processes and findings. • Ensure prompt action on compliance alerts and issues to avoid consequences.
Time Stamps	00:02 -- Introduction 03:12 -- Dale Hoak's professional highlights 05:34 -- Given your experience in the Navy and then with the NYPD and now you're in the corporate world, what are the similarities or differences in how security practices happen? 08:46 -- Commitment-Preparedness-Discipline Framework and Creating a High-Performance Information Security Culture 11:12 -- Building a culture of compliance 13:26 -- Why do organizations tend to be lax with compliance requirements and take the superficial check-the-box approach? 16:19 -- Key problems with the ATO (authority-to-operate) compliance process 19:15 -- Practical recommendations 23:05 -- If we go the automation route, what kinds of checks and balances should be in place where there is periodical and prompt human intervention to ensure you can pick up on errors or glitches? 26:17 -- Prompt processing of threat intelligence 27:06 -- Narrating an incident of non-securely migrating to the cloud 29:33 -- American Cancer Society's migration to the cloud. 31:51 -- Closing Thoughts

Memorable Dale Hoak Quotes/Statements	"Compliance is essentially where fun went to die, and it became very complex. It was very subjective, and it was the enemy of innovation." "Today, as the cloud expands, particularly with AI, we're seeing that innovation is outpacing compliance." "Regulatory compliance is becoming more challenging, but also more central in a cloud-first world." "We've got to put compliance up there in front, and we've got to bake it in instead of bolt it on." "Folks just tend to recycle and use compliance as the checklist." "Compliance becomes highly interpretive and subjective, depending on your auditor -- if you bring in an experienced auditor versus a less experienced auditor." "To be honest, compliance can be subjective, and compliance does not equal security. Just because you meet the guidelines and pass an audit does not make you secure." "If you give a company an opportunity to save money by slacking on security, they're going to." "Small companies just don't have the funds it takes to build a reliable security platform in a timely manner." "Often regulatory compliance guidelines are outdated. They can't keep up with the speed of innovation out there." "So, how do we make compliance faster? How do we make it more affordable? How do we optimize the resources? CISOs are really challenged with these questions today."

	"So, when I speak of automation, I speak of doing the data gathering automatically, using tools to set a scoring criteria against the priorities, and then you make a determination of review." "Nobody steals your work. We don't have unlimited resources where you can roll out bodies, right, and write an unlimited number of checks. So, we need to use automation to do the work." "Let the humans do what they were meant to do, which was think through the problem intelligently and conduct the risk assessments. Where you can automate pieces of the risk assessment do that, but ultimately, you need a person to evaluate and either exempt or accept or whatever you need to do for that risk. That's where the humans need to come in. Let's use automation to clear out the noise, and let's focus on the music in the middle." "So they (company migrating their data and systems to the cloud) tried to bolt on security at the end, and as a result of not having that security in place, first, they got fined for data exposures that could have been prevented during the move." "Compliance isn't a one-time task. That's been my goal, which is to make it a living, breathing process in today's cloud environment. It's an ongoing, evolving process that must be continuously monitored and enforced." "Compliance is a key driver of trust in our world."