Scott Cacal

3.8.2025

CSD 380

Module 12.2

Compliance

This week's final assignment for the course is a great way to wrap up DevOps (the areas of product release and feedback) and product compliance. When one thinks of compliance it’s easy to associate compliance with outright bureaucracy with full intent to limit organizations. But much like my take on platform engineering, with some level of “order” you can leverage that to help speed up product development. In this week’s text are two case studies that validate the importance of cohesion and DevOps pretty well and to further complicate things, address the challenge with the nature of change.

Providing Compliance in Regulated Environments

The problem with auditing for compliance sake is, the way it is performed in some areas such as operations may work but it may not work in terms of coverage for software development. Bill Shinn, principal security architect for Amazon Web Services (AWS) addresses some of the points as to why that can occur and why you should adapt to then improve development. Some dated methods of evaluating asset management can evolve verification screenshots of irrelevant information (for example; servers that disappear due to auto-scaling). The proposal for this is a combination of transparency and really getting ahead of the game, before things can go wrong; Telemetry, a way of transmitting data for analysis and monitoring. To further improve that is frequent discussion, between regulatory officers and DevOps and security teams to, as the textbook puts it so elegantly, “prevent, detect, and correct problems”.

Relying on Production Telemetry for ATM Systems

This case study talks about large failures that can happen when the level of auditing may be missing the mark due to the market it is being performed. For example, when it comes to banking and ATM systems, there should be a bit more involvement other than code reviews for fraud detection. For Mary Smith, guide of DevOps initiatives for large US financials service organizations uses a previous incident of an internal threat placing backdoors in code to obtain cash from ATMs by setting them into a maintenance mode. The issue here is this could not have been uncovered by a code review; but the changes made involved effective production telemetry.

I have pushed the idea that compliance as a comparison to platform engineering can help speed up production. But to further that argument of productivity, the delays involved by not meeting regulatory requirements are costly. And so, that’s what’s important, the “mishmash” that is involved with software development independently can appear as absolute roadblocks to a goal, but the key is to understand all the components involved and adapt synchronously (or as best as possible) as this world is continuously evolving in terms of technology and demands.

References:

Debois, P; Forsgren, N; Humble, J; Kim, G; Willis, J . (2021) . The DevOps Handbook: How to Create World-Class Agility, Reliability, & Security In Technology Organizations (Second Edition). IT Revolution