**Compliance - Assignment 12.2**

Robert Minkler

College of Science & Tech, Bellevue University

CSD 380 DevOps

Professor John Woods

May 18, 2025

**Proving Compliance in Regulated Environments**

How can modern DevOps pipelines comply with industry regulations? The Proving Compliance in Regulated Environments case study examines how DevOps teams can comply with industry regulations while moving to modern tools and practices. Regulatory auditing practices were developed around traditional datacenter infrastructures and production pipelines. How can a modern production environment comply with existing regulations and successfully meet an auditor’s requirements?

The traditional approach to auditing often required a sample of production servers with screenshots showing the relevant settings to ensure each of the servers meets the requirements. With modern cloud architectures, services are constantly being deployed and shut down as production needs change. How large a sample is sufficient when the number of services is constantly changing? What benefit is there in documenting the settings of a service that has been shut down? Are there more effective ways to ensure compliance is met while meeting the auditor’s needs?

Designing new systems to ensure regulatory compliance is possible. Coordinating with the auditors when designing controls ensures that the controls and telemetry sufficiently meet the requirements of the auditor. In addition, engineering requirements should be derived from the corresponding regulations. Combining this knowledge allows an organization to build telemetry and tools that fully meet the regulatory requirements and systems that provide the needed data for the auditors to perform their work.

The telemetry captured and logged should conclusively demonstrate that all necessary controls exist, are in place, and are functioning properly. All this data can then be sent to a telemetry system such as Splunk or Kibana, allowing an auditor free rein to examine any data they wish to view over any period they need to examine. Instead of a team collecting thousands of screenshots to present to an auditor and the auditor having to examine all of them to ensure compliance, an auditor can quickly request what they need with a command and receive it immediately. This saves both the auditor and the organization’s compliance team countless hours.

Management must be prepared to address concerns and objections from an auditor. Control attestation and artifacts demonstrate a control’s effectiveness in maintaining regulatory compliance that cannot easily be disputed. With the right tools in place, regulatory compliance can be met, audits can run smoothly, and systems are more robust since they are monitored continuously for issues that may break compliance.

**Relying on Production Telemetry for ATM Systems**

The case study on Relying on Production Telemetry for ATM Systems discusses how modern telemetry detected an anomaly faster than traditional methods. Code reviews were the traditional method for detecting fraudulent activity from within an organization. Instead of relying solely on code reviews, modern telemetry should play a more dominant role in detecting fraud. Years ago, a corrupt developer planted some code into ATM machines. This code placed the ATM into maintenance mode, which allowed a knowledgeable attacker to pull cash from the machine without documenting the withdrawal. Code reviews failed to detect the fraudulent code before it was deployed. However, telemetry alerted teams to the ATM machines across the city being placed into maintenance mode at the same time. While an ATM being placed into maintenance mode was not a red flag, all the ATMs going into maintenance mode at once was.

This clearly demonstrates that layers of protection must be in place for highly secure systems. Code reviews, automated testing, monitoring controls, and change approvals all play a role in protecting a system from malicious code commits. Any of these alone is insufficient.