Julie Sakai

CSD 380

5/17/25

Module 12.2 Assignment

Assignment: Compliance

The authors in the case study on “Providing Compliance in Regulated Environments” explain that ensuring regulatory compliance in cloud environments creates interesting challenges, especially for large enterprises operating under strict regulations. Traditional audit methods rely on manual sampling of production servers. These methods are ineffective for dynamic infrastructure where autoscaling constantly changes the system. This gap between conventional auditing and modern DevOps workflows makes proving compliance more difficult.

To overcome these challenges, businesses must shift from outdated methods like screenshots and CSV files to real-time telemetry systems like Splunk and Kibana. These tools enable auditors to retrieve compliance data and improve transparency and efficiency. Companies enhance accountability by automating compliance monitoring and integrating audit-friendly tools while simplifying verification processes. It is important to provide clear and accessible audit logs to strengthen compliance efforts and risk mitigation.

Another main point mentioned in the case study is understanding specific regulatory requirements and translating them into operational controls. This

understanding requires collaboration between compliance officers, security sexperts, and DevOps teams. Organizations can meet legal requirements more effectively by refining control designs to ensure a smoother audit verification process. In the case study “Relying on Production Telemetry for ATM Systems,” the author explains that financial institutions have historically depended on code reviews to identify security vulnerabilities, but this method has significant drawbacks. The author mentioned how a developer inserted a backdoor into ATM systems, allowing unauthorized cash withdrawals by manipulating maintenance mode. Even with the security measures implemented, such as separating developments and operations, the fraud went unnoticed until operational review meetings revealed the unusual system behavior.

The main point of this case is the necessity for real-time production telemetry. Static security reviews cannot always detect inside threats, but monitoring can quickly flag irregular activity. As in this case study, even with structured security controls, vulnerabilities can still occur which is why additional safeguards are required. When utilizing live transaction tracking and system behavior analysis, banks can detect fraud before formal audits reveal discrepancies.

Both case studies highlight the need to modernize compliance and security practices as technology advances. Traditional audit methods rely on manual reviews, which are no longer effective in today’s fast-paced environments. Instead, organizations must integrate automation, real-time monitoring, and data-driven audits. This improves efficiency, enhances fraud detection, and maintains compliance with evolving regulations.

In highly regulated industries, cross-team collaboration is essential for developing security controls that meet legal requirements while smoothly integrating into daily operations. Security and compliance teams should work closely to design systems that fulfill legal obligations, monitoring, and proactive risk management. By leveraging modern technologies and best practices, businesses can minimize vulnerabilities, streamline audits, and reinforce their security framework.

Organizations must evolve to embrace continuous telemetry and automated compliance systems to enhance security and improve transparency in audit processes. These technologies provide real-time insight into system performance and compliance status, allowing enterprises to detect and address risks before they become critical. By adopting these advanced approaches, businesses can stay ahead of regulatory changes, protect sensitive data, and maintain operational integrity in an increasingly complex environment.

References

Kim, G., Humble, J., Debois, P., & Willis, J. (2021). The DevOps Handbook (2nd ed., pp. 215-217). IT Revolution.