Mason Buller

Module 12.2 Assignment

December 22, 2024

Compliance audits occur when an auditor does a formal review of an organizations procedures to ensure that they are compliant with internal rules, regulations, policies, decisions, and procedures. Audits can be done internally or externally. Internal audits are typically done to identify potential risks and ensure that the company is following internal rules. External audits are done by third parties to ensure that the company is compliant with state, federal, or corporate rules and regulations.

When doing audits with a company that uses DevOps practices, they must change some things around in order to have a successful audit. Rather than auditing in the production stage, it occurs in all stages. The DevOps process is built around auditing so that the data is more accessible. Code is checked for compliance requirements at every stage. This also allows errors to be identified right from the source. Thorough documentation is what helps you have a successful audit and allows external auditors to easily access necessary data.

A principal security solutions architect assists companies in proving that they are compliant with any relevant laws and regulations that may pertain to them. Auditors who test for compliance aren’t trained to work with DevOps work patterns. To work around this, one architect has allowed the auditor to work with the teams during their control design processes. Designers address one control in each sprint so that they can focus on building audit evidence. All this data is then sent to a telemetry system so that instead of requesting a sample, auditors can access this system and locate all the audit evidence they may need. This method allows them to turn all their work into evidence that the auditor will easily recognize and that they can use it. The DevOps Audit Defense Toolkit helps describe the end-to-end narrative of the compliance and audit process for a fake company. This tool can be useful for identifying different methods that you could use in your own process to help auditors when reviewing your application.

There is a belief that auditors put too much reliance on code reviews and instead, they should be relying on production monitoring controls alongside automated testing, code reviews, and approvals. Monitoring can occur much more often than audits. If you wait for an audit to occur to catch errors, those errors can exist for a lot longer than necessary if you implement regular monitoring. You should never rely on one source to solve something when it comes to code. It is much more efficient to use multiple tools, and some tools may find issues that another tool did not.

Both studies show that using thorough documentation and monitoring can help find errors much better than without them. Documentation can help bridge any gaps that may occur either in the DevOps process or the auditing process and allows everyone to gather a decent understanding of how everything works together. Putting auditing at the forefront of your DevOps practices can help you have more successful and faster audits in the long run.

Sources

*Compliance Audit*. (n.d.). Retrieved from Compliance Quest: https://www.compliancequest.com/compliance-audit/#:~:text=A%20compliance%20audit%20is%20a,policies%2C%20decisions%2C%20and%20procedures.

Kelley, K. (2023, July). *Compliance Audit*. Retrieved from Tech Target: https://www.techtarget.com/searchcio/definition/compliance-audit

Kim, G., Humble, J., Debois, P., & Willis, J. (2021). *The DevOps Handbook* (Second ed.).

Srivastava, S. (2024, August 28). *DevOps Compliance - The Answer to Enterprise Compliance*. Retrieved from Appinventiv: https://appinventiv.com/blog/devops-for-compliance/#:~:text=Historically%2C%20auditing%20of%20software%20used,meets%20the%20necessary%20compliance%20requirements.