Jose Franco

07/08/2025

CSD-380

Module 8.2 Assignment

The Dangers of Change Approval Processes

In software development, change approval processes are often implemented to reduce risk and maintain system stability. However, recent research and real-world incidents reveal that these processes, particularly when overly rigid or centralized, can create more harm than good. One of the most well-known examples is the Knight Capital deployment failure in 2012. A fifteen minute error resulted in a $440 million trading loss and nearly destroyed the company. Despite the presence of change control processes, the issue wasn’t detected or mitigated in time, highlighting the failure of traditional approval models.

As described in The DevOps Handbook, John Allspaw points out two common narratives following major incidents like Knight Capital: one blames change control failure, and the other, testing failure. While each may appear valid, both approaches, when implemented in low-trust, command and control environments, can paradoxically increase the risk of failure. Gene Kim recounts his conversation with Allspaw and Jez Humble as a pivotal moment in understanding that traditional change and testing controls might actually do more harm than good.

This realization led to further study in the 2014 State of DevOps Report, where findings confirmed that performance improves not with stricter approvals, but through building high-trust teams, faster feedback loops, and strong automation (Kim et al., 2021). These findings are echoed by DevOps Research and Assessment (DORA), which identifies manual change approval processes as one of the weakest predictors of success in modern software delivery (DORA, n.d.).

According to LaunchDarkly, heavy change management introduces delays that harm innovation and responsiveness. Waiting on approval from external bodies such as Change Advisory Boards (CABs) leads to bottlenecks, especially when reviewers lack full context (LaunchDarkly, 2019). Octopus Deploy also criticizes CABs for contributing to outages rather than preventing them, arguing that these systems often delay recovery more than they help with prevention (Octopus Deploy, 2019).

In high performing DevOps teams, responsibility for change is decentralized. Automation, peer reviews, and robust CI/CD pipelines replace manual gatekeeping. This model supports faster, safer deployments and encourages accountability and continuous learning. Rather than relying on outdated control mechanisms, organizations should focus on engineering rigor, transparency, and trust.

In conclusion, the dangers of traditional change approval processes are well documented. From real world failures like Knight Capital to research from DORA and industry leaders, the evidence supports a shift toward automation, decentralization, and trust based culture. Manual, centralized approval processes often delay progress, reduce ownership, and do little to improve reliability. Embracing modern DevOps practices is essential for delivering safer, faster, and more resilient software.

# References

DORA. (n.d.). Streamlining change approval. Retrieved from <https://dora.dev/capabilities/streamlining-change-approval/>

Kim, G., Humble, J., Debois, P., Willis, J., Forsgren, N., & Allspaw, J. (2021). The DevOps handbook: How to create world‑class agility, reliability, & security in technology organizations (2nd ed.). IT Revolution Press.

LaunchDarkly. (2019, April). The downsides of heavy change management. Retrieved from <https://launchdarkly.com/guides/reconciling-change-management-and-continuous-delivery/the-downsides-of-heavy-change-management/>

Octopus Deploy. (2019, June). Change Advisory Boards don’t work. Retrieved from <https://octopus.com/blog/change-advisory-boards-dont-work>