The Dangers of Change Approval Processes

In the rapidly evolving landscape of software development, the DevOps methodology has emerged as a powerful framework that bridges the gap between development and operations. DevOps emphasizes collaboration, automation, and continuous delivery to accelerate software development and deployment. However, the integration of change approval processes within DevOps can pose significant challenges and dangers, potentially undermining the very principles that make DevOps effective. This paper explores the dangers associated with change approval processes in DevOps, drawing on current literature and industry experiences.

One of the core principles of DevOps is the acceleration of the software delivery lifecycle through automation and continuous integration/continuous deployment (CI/CD) pipelines. Traditional change approval processes, often characterized by manual reviews and bureaucratic procedures, can significantly slow down this process. Research indicates that organizations with manual change approval processes deploy code 255 times less frequently than those with automated processes.1 This delay can hinder the ability to quickly respond to market demands and customer feedback, reducing the competitive edge. DevOps fosters a culture of experimentation and rapid iteration. Change approval processes that require multiple layers of approval can stifle innovation by discouraging developers from making frequent changes. The fear of lengthy approval times and potential rejections can lead to risk aversion among development teams, ultimately inhibiting creativity and agility. A study by Kim, Humble, and Debois in 2016 highlights that organizations with less stringent change approval processes report higher levels of innovation and faster time-to-market.2 Moreover, it is important to note that centralized change approval processes can create bottlenecks, particularly when approvals are dependent on a small group of individuals or committees. This not only slows down the deployment process but also introduces single points of failure. If key approvers are unavailable, the entire deployment pipeline can come to a halt, causing significant delays. In 2018, Forsgren notes that decentralized and automated approval processes can mitigate these risks by distributing responsibility and enabling continuous flow.1

The presence of cumbersome change approval processes can negatively impact team morale and productivity. Developers may feel frustrated by the constant delays and rework required to meet approval standards, leading to disengagement and burnout. This is particularly detrimental in a DevOps environment, where team collaboration and motivation are crucial for success. In 2019, Kerzner emphasizes that streamlined and automated processes not only enhance productivity but also improve job satisfaction and team dynamics.3

While change approval processes are often implemented to enhance security and compliance, they can sometimes have the opposite effect. Manual approval processes are prone to human error and oversight, potentially leading to security vulnerabilities being missed. Automated processes, on the other hand, can integrate security checks and compliance validations into the CI/CD pipeline, ensuring consistent and reliable enforcement. In 2016, Kim argues that integrating security into the DevOps workflow (DevSecOps) can enhance both security and compliance without the need for separate approval processes.2

While change approval processes are intended to ensure the quality, security, and compliance of software changes, they can pose significant dangers in a DevOps environment. The potential for slowed deployment speeds, inhibited innovation, bottlenecks, decreased team morale, and security concerns highlights the need for a re-evaluation of traditional approval methods. By embracing automated and decentralized approval processes, organizations can better align with DevOps principles, fostering a culture of continuous improvement and agility.