The Dangers of Change Approval Processes

Introduction

Change approval processes are designed to reduce risk and ensure that modifications to systems, applications, or infrastructure are carefully reviewed before implementation. In traditional IT environments, formal approval boards and documented procedures have long been considered necessary to maintain stability and compliance. However, in modern DevOps and continuous delivery environments, overly rigid or poorly designed change approval processes can introduce new risks. Instead of improving reliability, they may slow down innovation, create bottlenecks, and even reduce overall system performance.

As organizations adopt agile and DevOps practices, it becomes important to evaluate how change approval processes can unintentionally cause harm. While governance and oversight are important, heavy approval structures can conflict with speed, automation, and collaboration. This paper explores the dangers of change approval processes, including delays, reduced performance, employee resistance, and conflict with continuous delivery principles.

Understanding Change Management and Approval Processes

IT change management refers to structured methods used to manage changes to systems and services to minimize disruption (ServiceNow, n.d.). Traditionally, organizations establish change advisory boards (CABs) to review and approve proposed changes before they are deployed. The goal is to ensure that risks are assessed, documentation is complete, and stakeholders are informed.

On the surface, this approach seems responsible and necessary. However, problems arise when approval processes become overly bureaucratic or disconnected from modern development practices. In fast-paced DevOps environments, teams rely on automation, frequent updates, and continuous testing. When every change requires lengthy reviews and multiple layers of approval, it slows down the delivery pipeline. Instead of enabling safe change, the process can become an obstacle. When approval systems are too rigid, they discourage experimentation, delay critical fixes, and create frustration among development teams.

Delays and Bottlenecks in Software Delivery

One major danger of heavy change approval processes is the creation of delays and bottlenecks. In continuous delivery models, small and frequent updates reduce risk because changes are easier to test and roll back. However, when teams must wait days or weeks for approval, they often

bundle multiple changes together to save time. This increases the size and complexity of deployments, which actually raises risk.

According to LaunchDarkly (n.d.), research from the State of DevOps Report found that heavily changing management practices are associated with worse software delivery and operational performance which means that strict approval gates do not necessarily improve stability. Instead, they can slow down deployment frequency and increase recovery times when failures occur. When urgent fixes must wait for formal approval meetings, organizations may experience longer outages and customer dissatisfaction so that way the approval process itself becomes a source of operational risk rather than protection.

Resistance and Poor Change Management Outcomes

Another danger of strict approval processes is employee resistance and poor adoption of change. Change management strategies often fail when organizations focus too much on control and not enough on communication and collaboration. Harvard Professional Development (n.d.) explains that change initiatives frequently fail due to lack of leadership support, poor communication, and insufficient employee engagement.

When change approval processes are seen as barriers instead of safeguards, employees may try to bypass them. Developers might implement "shadow changes" or work around official systems to meet deadlines which undermines governance and increases hidden risks. Additionally, overly complex processes can reduce morale and productivity. Teams that feel micromanaged or distrusted may disengage from improvement efforts so instead of promoting accountability, excessive approvals can create tension between operations and development teams, which directly contradicts the collaborative goals of DevOps culture.

Conflict with Continuous Delivery and Automation

Modern DevOps practices rely on automation, monitoring, and rapid feedback to manage risk where sutomated testing, continuous integration pipelines, and feature flags allow teams to deploy safely without relying solely on manual approvals. Heavy approval processes can conflict with these practices by reintroducing manual checkpoints that slow progress.

LaunchDarkly (n.d.) highlights that elite-performing DevOps organizations focus on smaller batch sizes and automated controls rather than rigid approval gates. When systems are designed with automated testing and monitoring, risk is reduced through technical safeguards rather than paperwork. If organizations continue to depend heavily on manual approval boards, they may fail to fully benefit from DevOps capabilities. Instead of enabling innovation, outdated approval models can prevent companies from competing in fast-moving digital markets.

Balancing Governance and Agility

Although changing approval processes can be dangerous when misused, eliminating governance entirely is not the solution. Organizations must find a balance between oversight and agility, an example where ServiceNow (n.d.) emphasizes that effective change management includes standardized procedures and risk assessment, but it should also be adaptable and supported by automation.

A modern approach may involve risk-based approvals, where low-risk, automated changes move quickly through the pipeline while higher-risk changes receive additional review. Clear communication, leadership support, and employee involvement are also essential to prevent resistance (Harvard Professional Development, n.d.). By aligning approval processes with DevOps principles, organizations can maintain stability without sacrificing speed where the goal should be enabling safe change, not preventing change altogether.

Conclusion

Changing approval processes are intended to reduce risk and protect IT systems, however, when they become overly complex, slow, or disconnected from modern DevOps practices, they can create serious dangers. Heavy approval structures can cause delays, increase deployment risks, reduce team morale, and conflict with continuous delivery models. Research shows that excessive change management controls are linked to poorer software delivery performance rather than improved stability.

Organizations must rethink traditional approval models to remain competitive and by incorporating automation, risk-based decision-making, and strong communication, businesses can balance governance with agility. Ultimately, the danger lies not in change itself, but in processes that prevent organizations from adapting quickly and safely. Effective change management should empower teams to innovate while maintaining accountability and operational excellence.

References

Harvard Professional Development. (n.d.). *7 reasons why change management strategies fail and how to avoid them*. https://professional.dce.harvard.edu/blog/7-reasons-why-change-management-strategies-fail-and-how-to-avoid-them/

LaunchDarkly. (n.d.). *The downsides of heavy change management*. https://launchdarkly.com/guides/reconciling-change-management-and-continuous-delivery/the-downsides-of-heavy-change-management/

OpenAI. (2026). *ChatGPT (February 22 version) [Large language model]*. https://chat.openai.com/
(Used for grammar review, formatting assistance, and organization support.)

ServiceNow. (n.d.). *What is IT change management?* https://www.servicenow.com/products/itsm/what-is-it-change-management.html