Jonah Aney 12/06/25 CSD380 Module-8.2 Assignment: The Dangers of Change Approval Processes

The Dangers of Change Approval Processes

Change approval processes have long been viewed as essential safeguards within IT organizations. Originating from traditional ITIL and audit-driven practices, these processes are intended to ensure oversight, reduce operational risk, and prevent unauthorized or harmful changes. However, research and industry experience increasingly show that conventional change approval mechanisms, especially those centered around Change Advisory Boards (CABs) and manual reviews, can create new concerns that undermine both system stability and performance. Using information and insights from DORA, Myndbend, N-able, and DZone, this paper discusses how change approval processes may inadvertently increase risk and reduce overall reliability.

Traditional change approval workflows follow a structured sequence that includes submitting a request, assessing the potential impacts, obtaining tiered or multi-level approval, implementing the change, and documenting final results. Myndbend describes several approval models such as single approver, multi-approver, or CAB-based approval, that vary depending on the perceived risk level of a change. N-able notes that these processes are designed to ensure accountability and communication across stakeholders. While the intent behind approval structures is sound in theory, the actual practice often introduces significant operational challenges.

One major danger is inefficiency caused by delays and bottlenecks in the approval process. Myndbend highlights that overworked reviewers often face long queues of pending changes, which leads to slow turnaround times or rushed “rubber-stamp” approvals. DORA’s research reinforces this by showing that external approvals and CAB reviews consistently correlate with slower deployment frequency, longer lead times for changes, and delayed incident recovery. Rather than reducing risk, these delays create additional pressure to bundle multiple updates into large releases, which in turn makes failures more severe when they occur.

A second danger is the false sense of security that manual approvals create. DZone argues that change control processes do not reliably prevent incidents and may even obscure actual risks. Organizations tend to believe that if a change has been approved, it must be safe, however, this assumption often proves to be incorrect. DZone references real-world failures, such as the Swedbank outage, to illustrate how both unapproved changes and ineffective oversight can result in significant operational damage. A heavy, involved manual review process does not necessarily always equate to an accurate outcome.

Jonah Aney 12/06/25 CSD380 Module-8.2 Assignment: The Dangers of Change Approval Processes

Another recurring issue is that approval processes frequently fail to differentiate between low-risk and high-risk changes. DORA emphasizes that treating all changes the same not only slows delivery but also misallocates attention. Low-risk, routine changes may wait unnecessarily for approval while higher-risk changes pass through without sufficient scrutiny. Similarly, Myndbend notes that lack of clarity about who should approve what can lead to confusion, unauthorized changes, or incomplete documentation. All of these also increase overall risk. N-able also argues that poor coordination and insufficient documentation make it harder to troubleshoot issues or assess the true impact of a change.

These dangers are compounded by cultural and legacy factors. DZone explains that many organizations still rely on outdated change processes built for slower, less complex systems. Compliance pressures reinforce this reliance, even when evidence shows that traditional CAB-driven models do not produce meaningful safety improvements. As a result, organizations often maintain processes that are inefficient and ineffective simply because they are familiar or required for audit purposes. Employees fall in to the trap of, “this is what we’ve always done.”

More effective approaches exist and rely on integrating safety into the development and deployment workflow rather than gatekeeping changes at the end. DORA recommends engineering-based safeguards such as peer review at commit time, automated testing, continuous integration and deployment pipelines, along with strong observability. These methods emphasize early risk detection and reduce reliance on manual approvals. DZone and DORA also support deploying smaller, more frequent changes to minimize the blast radius of potential failures. Myndbend and N-able both recommend risk-based categorization, automated workflow routing, clear accountability structures, and improved documentation to maintain oversight without imposing unnecessary delays.

While change approval processes aim to reduce risk, traditional approaches can create inefficiency, encourage large and dangerous changes, and foster a false sense of security. The information provided from DORA, Myndbend, N-able, and DZone indicates that the safest and most reliable systems are built not through manual gatekeeping but through automation, continuous delivery practices, and thoughtful risk-based decision making. To truly manage risk, organizations must modernize their change management strategies and shift from process-driven oversight to engineering-focused safety.

Jonah Aney 12/06/25 CSD380 Module-8.2 Assignment: The Dangers of Change Approval Processes

Sources:

DORA. (2025, October 30). *Streamlining change approval*. https://dora.dev/capabilities/streamlining-change-approval/

DZone. (2025). *Change Control Doesn't Work: When Regulated DevOps Goes Wrong*. https://dzone.com/articles/change-control-doesnt-work

Myndbend. (n.d.). *Guide to the IT change requests approval process*. https://www.myndbend.com/guide-to-the-it-change-requests-approval-process/

N-able. (2025). *Effective ITIL change management: Minimize risks and secure IT infrastructure*. https://www.n-able.com/blog/effective-itil-change-management-minimize-risks-and-secure-it-infrastructure