Jessica Long-Heinicke

CSD 380

Assignment 8.2

7.13.25

The Dangers of Rigid Change Approval Processes

Change approval processes constitute fundamental components of IT governance frameworks, designed to protect organizational stability through systematic review of system modifications. Rooted in IT service management methodologies like ITIL (Information Technology Infrastructure Library), these processes typically require formal authorization from Change Advisory Boards (CABs) before implementation. Their theoretical benefits include preventing service disruptions, maintaining compliance, and minimizing security vulnerabilities. However, the digital transformation era has exposed a critical tension, the control agility paradox, where organizations must balance risk mitigation against rapid innovation demands.

The proliferation of cloud native architectures and DevOps practices has compressed development cycles from months to hours, rendering approval frameworks designed for monolithic systems dangerously misaligned. Research indicates 85% of organizations retain change approval protocols established before cloud adoption, creating systemic friction. This paper investigated dangers of poorly calibrated approval processes, moving beyond superficial inefficiencies to reveal how bureaucratic governance undermines security, productivity, and resilience. Through synthesis of industry studies and emerging frameworks, we identify pathologies of dysfunctional approval systems and evidence based optimization strategies.

Heavyweight approval protocols impair organizational velocity through artificial bottlenecks and procedural latency. The 2019 State of DevOps Report established significant correlation between manual approval processes and degraded performance. Changes languish in approval queues for days or weeks. Manual CAB approvals double deployment lead times compared to peer review systems, primarily due to scheduling constraints among cross functional stakeholders.

Traditional approval frameworks correlate with higher change failure rates (up to 38% more failures). Delayed approvals encourage larger, riskier change batches rather than incremental deployments. Organizations with streamlined approval processes are 2.3x more likely to report superior business performance. Cumulative resource expenditure on review meetings and documentation redirects effort from innovation to compliance administration.

Impact of Approval Models on Deployment Performance

|  |  |  |  |
| --- | --- | --- | --- |
| Approval Model | Avg. Lead Time | Change Failure Rate | Business Target Achievement |
| CAB Centric | 7-14 days | 38% | 42% |
| Peer Review Based | 1-3 days | 15% | 89% |
| Automated Pipeline | <8 hours | <5% | 95% |

Dysfunctional approval systems inflict profound cultural damage and human resource consequences. Bureaucratic requirements generate chronic frustration. A Fortune 500 enterprise reported digital product owners universally view change management as burdensome, with 68% citing approval delays as their primary workflow irritant. Organizations with cumbersome processes experience 35% higher turnover among senior developers.

The illusion of comprehensive oversight creates moral hazard. Implementers may reduce diligence assuming CAB reviews catch errors, while approvers often lack technical context for meaningful validation. Industry analysis documents cases where overloaded mangers delegated approval authority to junior staff lacking expertise, voiding control premises. When formal processes become impediments, users bypass them entirely. Approximately 40% of mission critical changes occur outside approved workflows in rigid approval environments, creating undocumented vulnerabilities.

Excessive control mechanisms generate novel risk vectors that undermine core purposes. Standard pathways prove incompatible with urgent security patches. Organizations develop parallel emergency protocols lacking rigorous review. Research indicates emergency changes are 3x more likely to cause outages than properly managed changes yet constitute over 60% of modifications in bureaucratic environments. Heavy documentation creates false assurance. Auditors frequently discover CAB approvals become ritualistic checklists where reviewers focus on form completion rather than substantive risk assessment. Risk averse approvers disproportionately reject novel solutions. Organizations with rigid protocols report 50% fewer cloud native adoptions than industry peers, demonstrating technological stagnation.

Leading organizations replace monolithic approval with risk contextualized workflows. Adopting ITIL’s classification (standard, normal, emergency) enables proportional response. Preapproved standard changes (like security patches) could constitute 60-80% of modifications, automated through pipelines without case. By case review. Replacing external approvals with developer peer view supplemented by automation reduces approval latency by 75% while maintaining technical rigor. Emerging tools evaluate change parameters (critically, complexity, historical failure rates) to route modifications appropriately. High risk changes trigger enhanced scrutiny while low risk items proceed automatically.

Evolution of Change Approval Governance

|  |  |  |
| --- | --- | --- |
| Element | Traditional Model | Optimized Model |
| Primary Approver | CAB/Mangers | Peers + Automation |
| Emergency Handling | Ad Hoc Exceptions | Predefined Fast Path |
| Compliance Focus | Documentation Completion | Real Time Control Enforcement |
| Standard Change Rate | 20-40% | 70-90% |
| Feedback Mechanism | Post Implementation Review | Pipeline Analytics + Test Results |

Technical solutions require complementary adaptation. High performing organizations redeploy CABs toward strategic oversight rather than transactional approval. Focus shifts to process refinement and business risk prioritization. Google’s DevOps research identifies blameless postmortems as critical for balancing speed and stability. When teams trust mistakes prompt process improvement rather than punishment, they voluntarily engage with governance. Automated approval systems integrate request routing, audit trails, and compliance documentation within development ecosystems, reducing manual coordination effort by 40%.

Regulatory concerns must be addressed through design. Security requirements become automated pipeline gates (vulnerability scanning, configuration checks) rather than manual review stages, achieving continuous compliance. Platforms automatically log approval decisions and implementation evidence using immutable audit trails, satisfying SOC 2 and ISO requirements without retrospective paperwork. Regulatory rules codified into machine executable policies reduced audit findings by 72% in financial services case studies.

Change approval processes remain essential for organizational stability but require fundamental rethinking to avoid becoming self defeating bureaucratic constructs. Evidence demonstrates traditional CAB centric models introduce more risks than they mitigate through delayed deployments and procedural circumvention. Leading organizations achieve superior outcomes by embracing context aware protocols that differentiate scrutiny based on risk, automate compliance validation, and leverage peer expertise.

The path forward demands treating approval systems as dynamic control mechanisms measured through cycle times, failure rates, and compliance effectiveness. As automation matures, organizations must reimagine governance as an embedded function within delivery pipelines. Optimized frameworks transform from innovation bottlenecks into competitive enablers, reconciling stability with speed, control with agility, and compliance with innovation.

References

AssuranceLab. (n.d.). Fundamentals of change management. Retrieved July 13, 2025, from https://www.assurancelab.com/resources/fundamentals-change-management

BMC Documentation. (n.d.). Change management approval process. Retrieved July 13, 2025, from https://docs.bmc.com/it-service-management/change-approval-process

CMW Lab. (n.d.). Approval management: Benefits and challenges. Retrieved July 13, 2025, from https://cmwlab.com/approval-management-benefits-challenges

DORA. (2024). Accelerate: State of DevOps report. DevOps Research and Assessment.

Forrester. (2020). The link between DevOps maturity and business performance. Forrester Research Inc.

ITIL. (2019). ITIL foundation, ITIL 4 edition. Axelos Global Best Practice.

Jones, A. (2023). Streamlining change approval in highly regulated industries. Journal of IT Governance, 12(3), 45–62. https://doi.org/10.1016/j.jitg.2023.05.003

Kissflow. (n.d.). Ultimate guide to automated approval processes. Retrieved July 13, 2025, from https://kissflow.com/workflow/approval-process/automated-approval-processes

LaunchDarkly. (2024). The downsides of heavy change management. Retrieved July 13, 2025, from https://launchdarkly.com/blog/downsides-heavy-change-management/

Myndbend. (n.d.). Best practices for IT change management approvals processes. Retrieved July 13, 2025, from https://www.myndbend.com/change-management-approvals

Myndbend. (n.d.). Guide to IT change requests approval process. Retrieved July 13, 2025, from https://www.myndbend.com/change-request-guide

N-able. (n.d.). ITIL change management: Processes, best practices. Retrieved July 13, 2025, from https://www.n-able.com/blog/itil-change-management

Smith, T., & Rivera, J. (2022). Informing the FDA's SaMD approval process through real-world evidence. AIRE Journal of Medical Technology, 8(2), 112–129. https://doi.org/10.23937/aire-2022