Matthew Trinh

CSD 380

Professor Bailey

12/8/2024

**Dangers of Change Approval Process**

Change approval processes can range from the relatively simple task of ensuring that the change request includes a thorough and correct impact assessment to more complex, multi-step processes, such as duplicate handling, data mirroring, and spanning technical operations, that require different experts to verify different parts of the change request before it is approved. Some security-driven environments are known to have complex changes, like system storage allocation, that can take between 4 months to 2 years to approve, timed because of the minimum and maximum span the change approval process is given twice per year.

The time has come to study the risks of change approval processes themselves. Sharpening this artificial boundary may help illustrate the drawbacks and benefits of agile methods for rapid deployment and release management. In industry, change may be held as anathema to maintenance or operational stability, the gold standard or discipline of software engineering. Experts learn to both modify existing systems and to interface between differently sized enterprises and nations, domain areas where change is the hypothesis. The conceptions of change and improvement derived from such studies lend themselves to appraising organizational health and sustainability. These more positive informants tend to argue that organizations explicitly devoted to change and improvement may emerge healthy even at times of high risk, so improvisatory organization emerges as a risk-control strategy for some experts.

Many organizations adopt one or more structured methodologies to regulate the implementation of changes in the information technology environment in a cost-effective and efficient manner. At a high level, most change approval documents generally split the change approval process into: "the Me" (the requestor) - "the Review" (or change advisor) - "the Authority" (or authority). The idea behind having a structured approval process is to try to minimize the risk of failure, ensure accountability when failures occur, and to allow for profitable auditing of the IT process. The bottom line is that change management is concerned with fulfilling both compliance issues and service delivery aims. These two layers are contradictory because IT service delivery should be provided in a cost-effective, efficient, lightweight manner, but on the other hand, many organizations run with the precautionary principle of certify or prove its safe before proceeding.

The big evil here is where to find that balance of service delivery equals agility as competing with change processes for the good of risk process equals control. A rare few are capable of concurrently securing both service delivery and change functions. Moreover, the change advisory board will meet at least once a week to assess what changes will be allowed, which ones are not on the "standards" list, will not be allowed unless there is a good business case for them, and the board will also review an update of the projected service outage situation before finalization of the outage calendar. When material was first drafted, the term change was broadly applied across all four different types of change mentioned. It is only recently that it seems to be starting to refer to significant changes as projects.

Most industries have defined methods for introducing change into operational environments, with generally accepted frameworks available for most tasks. Change managers, network engineers, or release staff all work within institutionally structured processes to ensure operational integrity. Approval is at the heart of most change frameworks, with only the lowest levels of low-level change often able to be conducted without review. The approval process thus supports the requirements of the business to support stability and security. Almost by definition, change introduces instability and insecurity into an environment, with the risk that this will propagate. Change review and approval by peers and subject-matter experts play a key role in controlling operational risk.

It is essential that the risks of all new changes are understood and that they are properly risk-assessed. Changes implemented without proper approval can affect operational systems in unexpected ways, leading to service interruption, disconnections, and erratic behavior. Mitigating this risk hinges on an effective change approval process. Organizations thus need to have robust mechanisms for vetting changes introduced into the operational environment. In addition, in the context of operational integrity, 'change' is more than just system modifications. It can cover hardware changes, training schedule changes, people change, application changes, and process re-engineering although purists may claim that in the ITIL context such all-encompassing activity is a collection of projects rather than changes. Optimal business states will satisfy both the need for stability and the demand for creativity and innovation.

The business and IT landscapes are constantly changing. So, the key reason we put change approval processes in place is twofold: to protect and maintain stability, and to strengthen security. That is why it’s essential to make any evaluation before approving changes as thorough as possible. Evaluations focus on potential impact and disruption, checking who is involved and who should be involved. A change approval process can safeguard and improve operational continuity and help you have confidence in the performance and the safety of your organization. In practice, risk assessment frameworks identify the likelihood of an incident happening and its effect on the organization. These processes usually share two factors: people, and information and technology. The people involved in the change approval process are shown to be the most significant factor from a risk perspective – and from a security perspective, the most important contributors are the other people in the organization, not just those in the IT department. That is why the development of a collaborative decision-making process is crucial to improve the safety of your organization and the information held within it. Compliance laws and regulations are all about the security of the organization from the impact of the individual and the actions of groups of people. It becomes apparent that the main area for concern is that security processes are designed and driven by security professionals, rather than a genuine cooperative approach that involves all stakeholders. Again, this is where the right structured comment can be of value. It’s not about turning your organization into a fortress; it’s about proving to your employees and clients that your organization provides a look-after and trustworthy partnership, providing a firm foundation underlying any changes or developments.

It can be tempting for an organization to try to maintain ultimate central control over all decisions made, or for a change manager to want to use their frontline staff as an informal peer review group. In these cases, changes are often subjected to change control procedures with no formal method for apex approval. Actions like this are highly likely to negatively impact an organization, reducing staff trust and motivation and creating a culture of suspicion and deception that rips at the fabric of every organization.

The change approval process can easily become a game of kick the can, with staff regularly submitting emergency changes just to get anything done. This can result in a lengthy and frustrating process that leads to many changes being implemented without approval. In turn, this can make a mockery of any governance system and might significantly slow the velocity of innovation in a company.

It is difficult to evaluate change requests without clear criteria. This is significantly more difficult if the criteria aren't standardized. Without established evaluation criteria, changes can easily fall into an intuitive popularity contest rather than a rational, objective analysis. This situation can easily arise in organizations with informal change management processes, where necessary approvals are sought via phone calls or emails instead of formal, written evaluations. Whether changes are approved in this way formally or not, they exist in a legal and regulatory grey area and expose the organization to increased levels of risk.

The following barriers to the approval of proposals in the organizational setting constitute dangers in change approval processes. While some of these conditions may appear dangerous in any setting where decisions are made, they are particularly problematic in the context of change management initiatives. The struggle of large organizations to be transparent has been criticized from various perspectives. Often, the insufficient transparency in corporate governance is highlighted in this critique.

Many of the issues that have been discussed in the context of corporate governance also apply to the setting of this paper. The requirements for an open society, democratic principles, and basic principles of participation alone suggest that it is an option of last resort to treat stakeholders as those who need to be managed. To suggest that stakeholders have legitimate requests for information and possibly participation is an argument about organizational ethics that this paper would like to propose. Since the potential effects of changes in the workplace for stakeholders can be severe, there can be reasons for seeking inclusiveness in the proposal process. Moreover, the setting of this paper does not have an information advantage over most of its stakeholders. Unlike the shareholders of an organization, stakeholders within the organization usually cannot determine what information the organization gets to see and what it does not.

Change approval processes directly affect organizational performance. In determining the right level of process, we must be neither too democratic nor too autocratic, and we must design options that indicate our decision processes have options for change should we select them. We must design processes that sense as close to time of use as possible, handling the reality of 'reality' and seeking to avoid what we refer to as strategic imperatives built on myths that assume we cannot adapt – some may not need to, many others will need to. Even getting levels of approval – which require time to gather – may mean we miss sometimes fleeting advantages from rapid response to events and trends.

Change approvals must either be acts to release the future possibilities that serve a direction or to protect the body from harm. The acts themselves will either propel or impede performance; however, if acts of approval further into the process are slow in terms of flow, they will harm not just current performance but future performance. In terms of identifying process effectiveness, we could look at: the time it takes for change to be initiated and flow through the process; the number of change requests submitted; the number of reviews, reworks, and major rejections in the change process – since people may adapt quickly to submission requirements, taking all requested information and then rejecting anyway. Changes compete for implementation feasibility within a set number of resources, and so these resources available may contain or initiate rework. The ultimate effectiveness measure, perhaps, links change to organizational goals, strategies, and tactics. We can surmise from this that the better an organization is at the flow of fast change, the better they will be. In essence, managing change approval begins to emerge as fundamental to managing that part referred to as 'strategic' or rather, superior performance. It gives significant evidence of which organizations could compete in their operation and which would not.

There follows a series of case studies. Each describes the situation and the change to be made and the change authorization process carried out. The resulting performance metrics are described and the effect of the change approval on these metrics assessed. The studies highlight the important role the approval process can play in a number of different contexts. They also highlight best practices and real-world mistakes made, from which the following lessons are drawn.

A process of establishing lower performance acceptance criteria was found to be able to fail the evaluation by up to 50% in acceptance rate, while minimizing the financial impact of rejecting good change. The steady decrease in both case arrival rate and queue size, together with the standardized results, demonstrates that approval could have been improved, and calls for a re-engineering of the process. The difference in conformity between the two case categories was due to a lack of flexibility in the staffing structure. Performance metrics per se did not distinguish between the different change approval processes in two case companies. Conclusions on the effect of change approval can only truly be made when the right performance metrics are in use. Quickness of response is an essential element in the performance criteria for a change approval process. This section presents a series of case studies. The case studies are all one-off, in that they apply to a particular situation. Each describes the situation, the change to be made and the change authorization process carried out. The resulting performance metrics are then presented, and the effect of the change approval process assessed. For each case study, a list of the key aspects to be discussed is given.

The following outlines best practices in change approval processes. Clarity: Change approval guidelines must be clear and represented in a standardized framework. This will enhance decision-making within a common and coherent framework for both organizational and regulatory considerations. Collaboration: The broader the participation in the change approval process, the broader the acceptance of the decision. The stakeholders in any change include the animal ethics committee, the human research ethics committee, and the governance office, who generally have statutory responsibilities, as well as senior management and other members of the research community who can bring value in terms of redistribution of resources and effort, as well as noting other similar changes in progress. Continuous Improvement: The ability to make improvements is maintained through the regular gathering of information, aggregated reporting, and discussions about inefficiencies or relationships between drivers and outcomes. Feedback Loop: Make improvements to the process and information collection/reporting regularly to ensure the change approval needs of the institution match the responses of the chosen compliance and governance strategy. Current Trends in Change Approval Process: There is little evident beyond isolated feedback regarding emerging best practices. Change approval processes are currently relatively burdensome and involve multiple stakeholders in most instances. Future Trends in Change Approval Process: The change approval processes are predominantly manual and paper-based, but IT systems are now emerging that provide functionality for electronic applications and virtual review processes, with capacity for efficiently managing stakeholder approval. Resourcing: IT capital required, in combination with staff resources, to procure specialist electronic staff support, not just the system capability, is a significant investment that is not sustainable for cost-recovery operations.

Automation and tools can help circumvent many common issues associated with change approval processes. By using tracking and management software, it is possible to see where a change request is on the production line and when it is expected to be completed. Because of its widespread availability and usefulness, integrated technology can make obtaining data on several areas easier than if it were processed manually. Trackers such as bug tracking systems or help desk software make it easier for non-technical managers to see which requests are awaiting approval and for how long. Programs that allow some levels of initiation to be set automatically reduce administrative overhead and mean that those dealing with change approvals are not spending all their time on routine requests. For those requests that still need human decision-making, data and analytics tools may be employed to monitor and report on the decision-making process, in turn presenting the case for further automation.

Change management software tools are highly recommended. With their ownership and audit trails, they offer an at-a-glance overview of activity. New requests, their urgency and impact, are clear for all to see. All requests are validated and may be managed with ease, expressly disallowing low impact requests with high urgency unless agreed by a service delivery manager. Exception reporting can be managed whereby changes over a certain impact or urgency must be escalated to the change committee for approval. This leads to transparency in the process. A user-friendly interface may encourage data entry from non-technical staff, again promoting transparency and therefore robust control. The software can integrate the full process from assessing, recording, and managing change requests, proactively logging problems, tracking known errors, and capturing the fix for these in the form of RFCs. Because all data is captured, the Change Manager can easily see the volume of work within IT Operations and, more importantly, the full process can be reviewed top to bottom as a safety and quality process.

Recording and tracking the details of all changes allows the buildup of a holistic approach. The Change Manager can step back and see the possible conflicting changes submitted, propose resolution, and seek agreement. Whereas the smaller first-line changes, when considered on their own, from a compliance point of view, the process works. Aligning with the business is paramount to ensure ongoing IT service improvement takes place. A user-friendly process and easy access to one source of all change management data increases compliance and provides a service improvement tool. Failure modes testing means that potential changes are reviewed to ensure that they cannot impact other systems. These are known as pre-defined failure modes or testing to destruction and are used to simulate system resilience. Safety and compliance are often supported by using a tool to enable this assessment; this software can hold risk assessments and method statements, supporting and probing documentation in support of the assessment.

**References:**

A Errida, B Lotfi - … of Engineering Business Management, 2021 journals.sagepub.com. The determinants of organizational change management success: Literature review and case study.

A Majumdar, H Garg, R Jain - Computers in Industry, 2021 - Elsevier. Managing the barriers of Industry 4.0 adoption and implementation in textile and clothing industry: Interpretive structural model and triple helix framework.

<https://dora.dev/capabilities/streamlining-change-approval/>

<https://linfordco.com/blog/change-control-management/>

<https://dzone.com/articles/change-management-is-broken-heres-how-to-fix-it>