Eliminating Chaos: How a Bank Got Its IT Change Management Back on Track
A medium-sized bank in India decided to manage its infrastructure operations and application development by implementing IT service management (ITSM). So, the bank’s IT team adopted a phased approach and focused on three ITIL processes - incident management, request fulfillment, and change management. First, the IT team designed a best practice approach based on the ITIL framework for all three processes, trained other employees, documented an RACI and a matrix for the processes, and arrived at agreed key performance indicators (KPIs) to track performance. Then, the bank bought a service management tool to follow workflows or processes based on the best practices embedded in the ITSM tool.

In the next three months, the tool brought quite a difference to the organization. The process and compliance head reviewed the metrics and KPIs and indicated that incidents and service requests were handled well, but not the change requests.

Here are the snapshots of the changes recorded in the three-month period.

As shown in Fig A, the standard changes were few, while the normal and emergency changes continued to increase. In addition, there were several failed changes, and the business started losing hope on IT.
A core team comprising the head of infrastructure, head of application development, change manager, and service desk manager was formed to set right the situation. This team interviewed the support and development teams, analyzed the data to understand the reasons for the unsuccessful changes, performed a gap analysis, and suggested practical solutions.

The infrastructure and application teams were under pressure to improve performance, upgrade servers, and improve the turn around time for all changes moving into production. They did not have visibility of the upstream and downstream relationship of components that were undergoing changes. For example, when an exchange server was down, the infrastructure team couldn’t locate the information on the ITSM tool. The team had to rely on subject matter experts (SMEs) or the exchange server team. And when the SMEs were not available, the team went ahead with the changes using standalone procedures. As a result, the changes were not analyzed and the change review team could not conclusively predict the impact of the changes.
How did the core team address this?

The core team understood the need to build a configuration management system (CMS) to capture the complete infrastructure and application topology with attributes and relationships.
The team listed critical business services and built a service tree structure embedding attributes for various devices, along with the associated parent and child relationships, as shown in Fig D. The team identified the complete topology and got it signed off from the server, storage, and network SMEs and imported it to the service management tool.

Furthermore, the teams had no visibility of the planned, scheduled, and deployed changes. There was no proper mechanism to publish the forward schedule of changes or track the planned changes and their release dates.

www.servicedeskplus.com
What did the core team do to streamline the change workflow and ensure visibility?

The core team discovered that changes were often submitted at the last minute, without sufficient time to evaluate and execute the changes. This was due to the lack of proper discipline and governance to address the intake and execution of changes.

**Defining Change Management Norms and Standards**

To avoid last minute changes, they communicated the implications, rationale, and business impact to the heads of business and got mandatory approval on the following conditions:

- All normal changes should go into production once in 15 days.
- All changes have to be bundled with the release once in 15 days, with no exception for normal changes.
- All requests for change (RFCs) have to be submitted at least two weeks in advance. Any RFC that is required within a week’s time will be rejected with the requester’s manager in the loop.
- Any request to expedite normal changes, even in extreme cases, had to get through three levels of approval from the management. The approvals were tracked by the IT team to govern the changes being raised.
- Emergency changes would only be entertained in two scenarios:
  - To resolve an unplanned outage, major disruption, or incident.
  - A full-fledged release not deployed due to unavoidable reasons.
Defining the Different Types of Change

Standard change and normal change

Standard changes are low-risk, pre-approved changes that happen frequently and have a quick turnaround time. Standard changes can be implemented quickly and help manage risks.

Examples of a standard change:

- Desktop or standalone equipment movement.
- A standard patch that is applied to the servers once a month during the agreed maintenance window.

What is a standard change?

When a normal change is successfully implemented a few times, the associated processes like planning, scheduling, and implementation are established and become predictable and controlled. That is, the change becomes a routine task and therefore standard.

A few examples of normal changes:

- Upgrading the exchange server or any other hardware
- Setting up high availability or cluster for vital business functions (VBF)
- Roll out of a new release to address the reported issues

Expedite or fast track changes

- Expedite changes are raised due to a pressing need such as a legal or a business requirement. These changes are not related to restoring a service.
Emergency change vs expedited change

The change advisory board (CAB) defined clear rules and regulations to qualify emergency and expedited changes and communicated these rules across the organization.

Change Calendar for Better Visibility

The core team used the change calendar within the service management tool to report planned maintenance, changes, and releases and to ensure better visibility for the involved teams.

Fig E: Change calendar with downtime, maintenance, change, and release schedule
Defining the Key Performance Indicators

To assimilate the efficiency and effectiveness of the change management process, the core team identified the following KPIs.

- Number and percentage of failed changes for standard, normal, and emergency changes
- Number of incidents and service downtime caused by normal and emergency changes
- Number or percentage of unplanned or emergency changes
- Average time to implement changes
- Number and percentage of changes rejected by the CAB
- Number and percentage of unauthorized changes

The first four KPIs were taken from the service management tool, while the fifth and sixth required intervention from experts.

Change Advisory Board Ensures Better Change Reviews

The core team ensured that the CAB met once a week on Thursday between 7 P.M. and 9 P.M. local time. Representatives from the infrastructure, application, service desk, and release management teams reviewed all planned changes. However, the change manager was the final deciding authority.

The CAB rejected changes mainly due to non-compliance with the expected steps and protocols of assessment, review, and BIA (Business Impact Analysis). The change owners were held accountable for the failure. The core team was forced to adopt strict measures to prevent such occurrences in the future. The changes were assessed from all possible scenarios before the CAB meeting.
Handling Unauthorized Changes

During its discussion with stakeholders, the core team observed that about 20% of the changes were completed without authorization, mainly because the infrastructure team was under pressure to get the changes done quickly. As a result, many changes were done without a request for change or going through the review and approval processes.

To deal with this situation, stage gatekeepers were appointed for infrastructure, application, and database teams to ensure that the steps were not skipped when a change is made. The stage keepers had a go-ready list that comprised the test results, approvals, signatures from all the concerned teams, and a back-out plan. In case of violation, the stage gatekeepers owned responsibility that affected their appraisal and performance measures.

Another reason for the unauthorized changes was because the application teams updated the CMDB or CMS after the roll out of the release.

The core team ensured that audits were performed every week to compare the current state of CMS with the associated RFC and any deviation was highlighted to the CI owner and service owner for immediate action. In turn, the service owner closed the loop and took firm action. This process went on for four to six weeks, and the team made it a habit to follow the rule without exceptions.

Communication Roll Out and Training

After the core team implemented appropriate controls, the communication process was streamlined so that the involved teams can be notified of the new change. So, the heads of business rolled out the formal change management process, which was followed by awareness sessions and training programs.

The execution in the next three-month period showcased visible improvements, as seen in Fig F.

www.servicedeskplus.com
Lessons Learned (CSI)

- The bank’s IT team understood that building a robust configuration management system with up-to-date information of all IT components is essential for a successful change and release management process.

- Forward schedule of changes, planned maintenance window, and release plans are critical to manage the volume and duration of changes and to ensure smooth deployment.

- Enforcing a policy requires practicality, diligence, and buy-in. The new policies were fewer in number but were important for the success of the change management process (for example: CAB, unauthorized changes, and PIR).

- Relevant and practical KPIs help teams become efficient and effective.

- Process and tools have to work in tandem and absence of one or the other will severely impact continual service improvement (CSI).

- Post-implementation review of key changes and implications provided valuable insight on potential areas to improve and control changes.
Bottom Line:

The bank improved its overall efficiency and effectiveness of the change management process by ensuring good governance, implementing process and tool alignment, and offering strong leadership.

This case study gives you the necessary tools to structure, implement, and execute organizational changes smoothly. If you have an interesting experience with the change management process, do share it with us in the comments section.

www.servicedeskplus.com