Change Management

IT change management is a standardized process for planning, communicating, and implementing technical changes to information systems. IT Support professionals are often responsible for installations, updates, upgrades, migrations, etc. to an organization's software, hardware, network security policy, data storage policy, cloud platforms, and more. IT Support staff are expected to make these changes while also minimizing disruptions to the organization's IT services. By following IT change management best practices, IT Support professionals can create robust plans for change rollouts that protect business continuity. The change management plan is often reviewed by change board approvals, management teams, and/or project stakeholders for risk assessment, feedback, and plan approvals or rejections.

IT change management plans

Each organization will have their own change management policies, processes, and procedures. However, there are several common items that should be included in change management plans as a best practice. When proposing a change, IT professionals may create documentation or use change request forms to detail the following elements:

- **Person/team responsible for the change:** Names at least one person as the responsible party for overseeing the change management plan.
- **Change priority:** States the urgency of the change. For example, critical security patches would have a high priority and need to be scheduled ASAP. Whereas, a software update that merely adds new features might be a very low priority and can be scheduled for a convenient future date.
- **Change description:** Gives an overview of the planned changes. The change description should also provide a list of the planned changes. For example, if the change involves updating firmware on several router models, the description should include which routers and models will be updated. Additionally, the plan should list the old firmware versions currently on the routers along with the new firmware versions to be applied during the update.
- **Purpose of the change:** Explains why the change is necessary. For IT Support professionals, the most common reasons for changes are operating system, software, driver, and firmware patches and updates, as well as hardware and peripheral upgrades. Installations, implementations, and redesigns of software and hardware systems are also common IT changes. IT Support professionals should regularly evaluate the need for improvements and changes to network security policies and procedures. Laws, regulations, and company policies may also require changes to how organizations store, transmit, and protect data.
- **Scope of the change:** Describes the extent of the changes. The documentation should include a list of all IT systems (hardware, software, etc.), locations, departments, individuals, vendors, partners, customers, and others the changes affect, whether directly or indirectly. Any changes to policies, processes, or procedures should also be recorded.
- **Date, time, and duration of the change:** Indicates when the change is scheduled to take place and the duration of the change rollout. If the change is expected to create service outages, the person or team responsible for managing the change should inform all affected staff about the outage before the systems are taken offline. IT changes are often implemented outside of normal business hours, when systems can be taken offline with minimal disruption. For organizations with traditional Monday through Friday, 8 a.m. to 5 p.m. business hours, changes are usually planned to begin in the early evening on a Friday, after end users have logged out for the weekend. The change implementation process should include plenty of contingency time before the next business day in order to test, troubleshoot, repair, and roll-back any changes that are not successful. When an unsuccessful change occurs, IT Support professionals may need to work through the night and into the next morning. Organizations and IT departments may opt to hire a vendor to perform overnight system changes to adhere to company overtime policies and labor laws.
- **Change rollback or backout plan:** In case of primary plan failures, details a rollback plan to return the affected systems back to their original state before the changes were attempted. Additionally, a secondary or alternative plan may be included. This could be a plan to activate a failover system to replace any problemed systems until they are repaired. IT Support professionals should detail the steps involved in the rollback and/or alternative plans, including the original configuration settings and software, patch, driver, and/or firmware versions. Files needed to rollback updates and patches should be downloaded and stored in an accessible location to simplify rollbacks. Cloud-based virtual systems can be restored in seconds by simply using clones of saved previous VM states.
- **Technical evaluation:** Records the results of any testing performed on the proposed changes in a lab or sandboxed environment. The testing environment should be as similar to the target environment as possible. For example, the same operating system versions, hardware parts, drivers, firmware, etc. of the target system should be reflected in the lab/sandbox testing environment. Setting up a testing sandbox for cloud platforms should be as simple as cloning the virtual system(s) targeted for updates. The plans should also include metrics for evaluating if a change is successful or not.
- **Systems affected by the change:** Lists all IT resources (including hardware, software, networked, and cloud systems) that will experience direct or indirect changes as a result of the change rollout.
- **Anticipated impact of changes:** Describes how the planned changes are expected to impact the affected systems. For example, if the change involves adding new servers to a resource pool, the plan might describe that this increase in load capacity will result in system performance improvements and faster server response times.
- **Resources needed to implement the change:** Lists the human resources, budget, time, management oversight, subject matter expert (SME) consultations, training, equipment, hardware, software, parts, systems, tools, insurance policies, and any other resource needed to complete the planned changes.
- **Training for users impacted by the change:** Outlines any training needs to help users adapt to the changes. This might include classes on how to use new software applications, hands-on practice with new hardware, a company-wide announcement for security procedure changes, and more.
- **Risk level for change:** Describes how much risk is involved in making the proposed changes. Some changes are high risk and might cause catastrophic failures if the plan goes wrong. For example, an upgrade involving a single point of failure on a critical system could create a system-wide outage. In this case, it would be wise to implement a redundant failover system for that critical system before attempting any other changes.
- **Change instructions:** Details each step of the planned changes. This should be formatted as an instruction manual for the IT Support professionals to follow to ensure there is no guesswork involved in implementing the changes.

Change board approvals

Some large organizations may have a Change Advisory Board (CAB). The CAB is a board of directors appointed to oversee all implemented IT changes in the organization. The CAB can be the official governing body to approve or deny change management plans. They may advise on needed adjustments to the plan to meet business goals or to comply with regulatory compliance criteria. The CAB may also assist with mitigating risk brought about by proposed changes.

User acceptance

Including a user acceptance process for information system changes is a best practice in IT change management. IT change management plans can include a beta testing period similar to software development user acceptance testing. This plan might include several days of testing by a select group of users to ensure that the changes have been successful and that there are no hidden surprises caused by the changes. The change management team for the plan should develop user acceptance criteria forms for the beta testers to complete. The criteria normally includes common activities that all end users should be able to perform successfully in the new or changed environment. A period of time should be reserved for fixing any problems the beta testers find. When beta testing is successful and the changes have been accepted/approved by the users, the changes should become available to all appropriate end users.

Mark as completed

Like **Dislike** **Report an issue**