Change Management: Best Practices

Contents

1 Executive Summary

This document presents leading practices in change management. It is intended for managers, network operations personnel and practitioners in IT service management.

The objective of the change management process is to minimize service downtime by ensuring that requests for changes are recorded and then evaluated, authorized, prioritized, planned, tested, implemented, documented and reviewed in a controlled and consistent manner.

1.1 Introduction

Organizations in all industries—particularly financial services, retail, and communications—are increasingly dependent upon IT and a highly available network to meet their business objectives. In particular, the advent of online business transactions has made the network a critical business component that is expected to function properly with little or no downtime. As customer expectations and demands rise, network operations teams are focusing on IT service-quality improvement and achieving higher levels of availability by re-examining processes and procedures—particularly in the area of change management—because changes to the network are often a source of downtime.

1.2 Business Needs

The purpose of the change management process is to ensure that:

- Standardized methods and procedures are used for efficient and prompt handling of all changes
- All changes to service assets and configuration items are recorded in the configuration management system
- Business risk is managed and minimized
- All authorized changes support business needs and goals

Changes should be managed to:

- Reduce risk exposure
- Minimize the severity of any impact and disruption
- Be successful on the first attempt

1.3 Target Market

This paper provides information on the change management process and provides guidance that is scalable for:

- Different kinds and sizes of organizations
- Simple and complex changes required at each lifecycle stage
- Changes with major or minor impact
- Changes in a required timeframe
- Different levels of budget or funding available to deliver change

1.4 Description and Requirements

This paper presents a change management process that meets the following requirements:

- Responds to the customer's changing business requirements while maximizing value and reducing incidents, disruption, and rework
- Responds to the business and IT requests for change that will align with the business needs

While this paper reflects leading practices assembled from various publications and the collective experience of Cisco subject matter experts, the practices are consistent to a large extent to the Information Technology Infrastructure Library Version 3 (ITIL V3) best practices, in particular Service Transition.

2 Leading Practice

A service change is any addition, modification, or removal of authorized, planned, or supported service or service component and its associated documentation. The need for changes arises both proactively and reactively for a variety of reasons:

Proactively (for example, seeking business benefits such as reducing costs, improving services, or increasing the ease and effectiveness of support)

Reactively as a means of resolving errors and adapting to changing circumstances

A change can involve any configuration item or element of IT infrastructure. Some types of changes are:

- Application changes
- Hardware changes
- Software changes
- Network changes
- Environmental changes
- Documentation changes

All changes should be tracked in a change management system. The change is documented in the change tracking system when the change initiator has completed the required level of technical verification and completes a change request. The following status codes can be used to reflect the status of a change request:

- Open: The change has been received and accepted but has not been assigned.
- In-Progress: The change has been received, acknowledged, and assigned. Work is in progress to fulfill the change request.
- Approved: The business and technical assessments have been completed and the change has been approved and committed to the change scheduler.
- Rejected: The change has been rejected and will be routed back to the requester with an explanation and a recommended course of action.
- Closed: The change request has been closed.
- Canceled: The change request has been canceled.

2.1 Roles and Responsibilities

There are four major roles involved with the change management process, each with separate and distinct responsibilities. In the order of their involvement in a normal change, the roles are:

- Change initiator
- Change manager
- Change advisory board
- Change implementation team (operations)

2.1.1 Change Initiator

The change initiator is the person who initially perceives the need for the change and develops, plans, and executes the steps necessary to meet the initial requirements for a Request for Change (RFC).

Some examples of change initiators are:

- A product manager in a line of business desiring a new or changed feature on an application
- A network architect replacing obsolete network hardware with newer-generation hardware with improved functionality
- A network engineer upgrading the capacity of a device or link to handle increased traffic
- A service manager who discovers a change in vendor contacts or procedures and must update documentation
- A Tier 1, 2, or 3 support engineer who needs to replace a defective part in a network element
- A security manager requesting a configuration and documentation change in response to a newly discovered vulnerability

2.1.2 Change Manager

Larger organizations require a dedicated change manager who is responsible for the following:

- Updating and communicating change procedures
- Leading a team to review and accept completed change requests with a focus on higher-risk changes
- Managing and conducting periodic change review meetings
- Compiling and archiving change requests
- Auditing network changes to ensure that:
  - Change was recorded correctly with work matching the RFC
  - Change had appropriate risk level
  - Configuration items were updated appropriately
  - Documentation was updated appropriately
- Change communication and notification
- Managing change postmortems
- Creating and compiling change management metrics

2.1.3 Change Advisory Board

The change advisory board (CAB) is a body that exists to support the authorization of changes and to assist change management in the assessment and prioritization of changes. When a CAB is convened, members should be chosen who are capable of ensuring that all changes within the scope of the CAB are adequately assessed from both a business and a technical viewpoint.

The CAB may be asked to consider and recommend the adoption or rejection of changes appropriate for higher-level authorization and then recommendations will be submitted to the appropriate change authority.

To achieve this, the CAB needs to include people with a clear understanding across the whole range of stakeholder needs. The change manager will normally chair the CAB. Typically, there are “standing” members on the CAB, and the change manager will recruit others as needed in order to ensure stakeholder representation. Potential members include:

- Customers
- User managers
- User group representatives
- Applications developers/maintainers
- Specialists/technical consultants
- Services and operations staff, such as service desk, test management, continuity management, security, and capacity
- Facilities/office services staff (where changes may affect moves/accommodation and vice versa)
- Contractors’ or third parties’ representatives, in outsourcing situations, for example
- Other parties as applicable to specific circumstances (such as marketing if public products are affected).

No change should be considered unless the change initiator or requestor and SMEs in the potentially impacted areas review the change.

It is important to emphasize that the CAB includes representation from all stakeholder groups and:

- Will be composed according to the changes being considered
- May vary considerably in makeup even across the range of a single meeting
- Should involve suppliers when that would be useful
- Should reflect the views of SMEs, users, and customers
- Is likely to include the problem manager and service-level manager and customer relations staff for at least part of the time

When the need for emergency change arises, such as when there may not be time to convene the full CAB, it is necessary to identify a smaller organization with authority to make emergency decisions. This body is the emergency change advisory board (ECAB). Change procedures should specify how the composition of the CAB and ECAB will be determined in each instance, based on the criteria listed previously and any other criteria that may be appropriate to the business. This helps ensure that the composition of the CAB will be flexible in order to represent business interests properly when major changes are proposed. It will also help ensure that the composition of the ECAB will provide the ability, both from a business perspective and from a technical standpoint, to make appropriate decisions in any conceivable eventuality.

Many organizations are running CABs electronically without frequent face-to-face meetings. There are benefits and problems from such an approach. Much of the assessment and referral activities can be handled electronically with support tools or e-mail. In complex, high-risk, or high-impact cases, formal CAB meetings may be necessary.

Handling the change reviews electronically is more convenient time-wise for CAB members but is also highly inefficient when questions or concerns are raised such that many communications go back and forth. A face-to-face meeting is generally more efficient, but poses scheduling and time conflicts among CAB members as well as significant travel and staff costs for widely dispersed organizations.

Practical experience shows that regular meetings combined with electronic automation is a viable approach for many organizations. It is generally a good practice to schedule a regular meeting when major projects are due to deliver releases. The meetings are used to provide a formal review and sign-off of authorized changes, a review of outstanding changes, and, of course, to discuss any impending major changes. Where meetings are appropriate, they should have a standard agenda.

A standard CAB agenda should include:

- Review of failed changes, unauthorized changes, backed-out changes, or changes applied without reference to the CAB by incident management, problem management, or change management
- RFCs to be assessed by CAB members—in structured and priority order
- RFCs that have been assessed by CAB members
- Scheduling of changes and update of change schedule and projected service outage (PSO)
- Change reviews
- The change management process, including any amendments made to it during the period under discussion, as well as proposed changes
- Review of change metrics on a monthly or quarterly basis
- Change management wins/accomplishments for the period under discussion, such as a review of the business benefits accrued by way of the change management process
- Outstanding changes and changes in progress
- Advance notice of RFCs expected for review at next CAB
- Review of unauthorized changes detected through configuration management

CAB meetings represent a potentially large overhead on the time of members. Therefore all RFCs, together with the change schedule and PSO, should be circulated in advance, and flexibility allowed to CAB members on whether to attend in person, to send a deputy, or to send any comments.

Many organizations do not review the technical content of the changes during the CAB meetings. Consequently, the change management process must include a technical review and signoff of each RFC prior to the CAB review (see section 2.2.1.7 for more details).

Note that the CAB is an advisory body only. If the CAB cannot agree to a recommendation, the final decision on whether to authorize changes, and commit to the expense involved, is the responsibility of management (normally the director of IT or the services director, services manager, or change manager as their delegated representative). The change management authorization plan should specifically name the person(s) authorized to sign off RFCs.

2.2 Change Process Models

Organizations will find it helpful to predefine change process models and apply them to appropriate changes when they occur. Such a model provides the framework for defining the steps needed to handle changes consistently and effectively.

The change process model includes:

- The steps that should be taken to handle the change, including handling issues such as exceptions and unexpected events
- The chronological order in which these steps should be taken, with any dependencies or co-processing
- Responsibilities; who should do what
- Timescales and thresholds for completion of the actions
- Escalation procedures; who should be contacted and when
- Approval authority
- Quality or performance measures and objectives

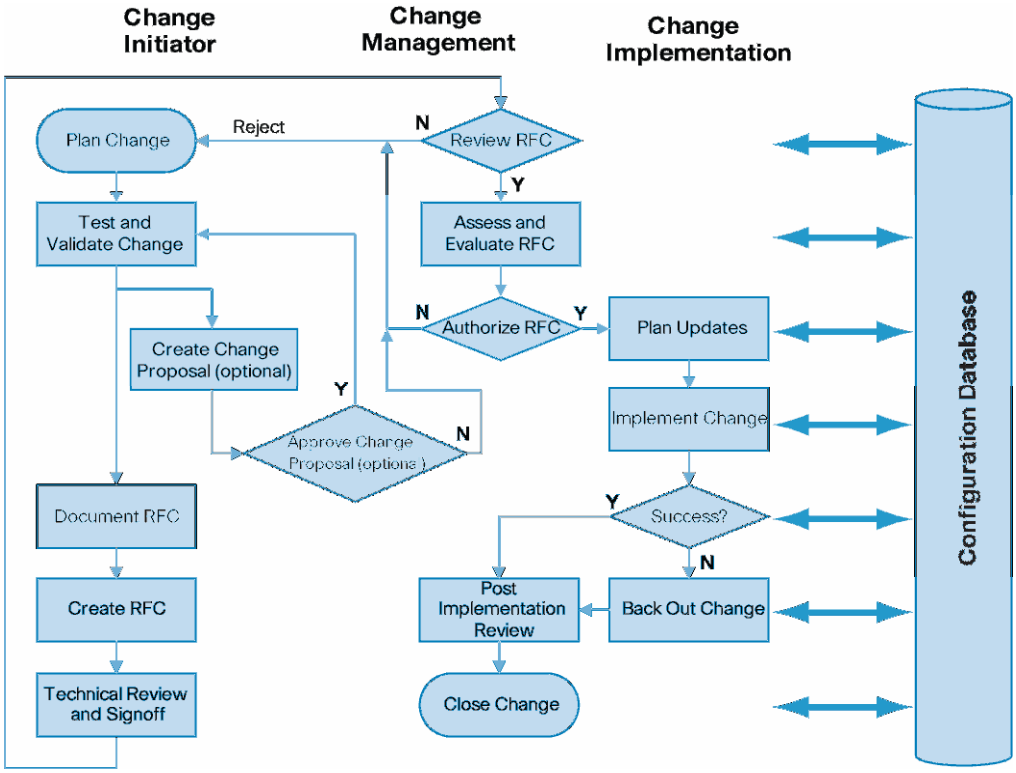
These models are usually input to the change management support tools in use and the tools then automate the handling, management, reporting, and escalation of the process. Change models may include:

- Normal change
- Significant (high-risk) change
- Major change
- Minor change
- Standard (pre-approved) change
- Expedited (short-interval) change
- Emergency change

2.2.1 Normal Change

The following activities are part of the normal change process flow. A subset of these activities will be used in other types of changes, such as standard or emergency.

Figure 1. Normal Change Process Flow



2.2.1.1 Plan the Change

Once the requirement for a change has been determined, the change is planned in terms of schedule and necessary resources, such as testing environment and time, personnel, budget, etc.

2.2.1.2 Test and Validate the Change

The testing starts with a summary laboratory validation of the proposed change. The goals of this test are to assess the feasibility and the costs (effort, resources) of the change.

At this point some organizations may require approval of a change proposal, as per the next two steps (see 2.2.1.3 and 2.2.1.4). The reason for this approval is to avoid unnecessary costs in testing and documenting changes that do not meet business needs or are deemed too risky.

If the change proposal is not required or has been approved, the testing continues in a laboratory replicating the production environment. The testing should include procedures to install the proposed change, to back out from the change in the event it cannot be successfully implemented, and to verify the success of the change after it has been implemented. A complete back-out or remediation plan must be documented, including procedures to back out at various stages of the change for each change deemed risky enough to require it. The need for a back-out plan, from a process standpoint, is usually tied to the level of risk calculated for a given change. The plan must also include a verification procedure to check that the environment has been restored to the initial configuration that existed prior to the change attempt and that there are no negative side effects resulting from the attempted change.

At the end of this stage the change initiator proceeds to document the change request, as per step 2.2.1.5.

2.2.1.3 Create Change Proposal

Based on the validation testing, the change proposal will contain information required in assessing the goals, costs, and risks associated with the change, including:

- Description of the change
- Benefits of applying the change
- Costs and risk of not applying the change
- Costs associated with the change
- Risk assessment of the change

The change proposal must be entered in the change management tool just like any Request for Change (RFC).

2.2.1.4 Approve Change Proposal

Change management will evaluate the change proposal and reject it if it does not meet business goals or the costs and/or risks associated with the proposed change are deemed to high compared to the benefits achieved by applying the change.

2.2.1.5 Document the Change Request

All the procedures for preparation, installation, verification, and back-out must be documented in detail. Impact and risk analysis of the change must also be recorded, in particular the worst-case impact, analyzing the situation of a failed change and a failed back-out procedure. Other information related to the change must also be included in the documentation, such as prerequisites for the change, proposed schedule, required resources, engineering and design documentation, physical diagrams, etc.

2.2.1.6 Create the Request for Change

The following list is an example of the information that can be captured and recorded for a proposed change in no particular order. The level of detail collected depends on the size and impact of the change. Some information is recorded when the change request is initiated and some information is collected or updated as the RFC progresses through its lifecycle. Some information is recorded directly on the RFC form and details of the change may be recorded in other documents and referenced from the RFC, such as engineering documents and impact assessment reports. It is a good idea to keep the RFC form simple especially at the beginning of implementing change management in order to encourage compliance with the process.

- Unique identifier that can be coded for type of change (such as hardware, software, application), network, site, technology, etc.
- Cross-reference to the related incident ID or problem ID, if necessary
- Description of change, including procedures for preparation, implementation, verification, and remediation
- References to external change documentation (such as engineering documentation or methods of procedure [MOPs])
- Items to be changed
- Reason for change

- Effect of not implementing the change
- Contact information for the initiator
- Date and time when the change was initiated
- Change type (normal, emergency, standard)
- Change category (major, significant, minor)
- Physical location
- Predicted timeframe, resources, costs, and quality of service
- Priority
- Risk assessment and risk management plan
- Potential customers impacted
- Back-out or remediation plan
- Impact assessment and evaluation—resources and capacity, cost, benefits
- Proposed change approvers
- CAB decision and recommendations accompanying the decision
- Authorization signature (could be electronic)
- Authorization date and time
- Target baseline or release to incorporate change into
- Target change plan(s) for change to be incorporated into
- Scheduled implementation time (change window, release window, or date and time)
- Location/reference to release/implementation plan
- Contact information for change implementer
- Change implementation details (success/fail/remediation)
- Actual implementation date and time
- Review date(s)
- Review results (including cross-reference to new RFC where necessary)
- Closure summary

2.2.1.7 Technical Review and Signoff

Generally the change management (CAB) assessment of the RFC does not include a review of the technical content of the change. Consequently, prior to submitting the RFC for CAB review, each RFC must undergo a technical review. This review checks the following aspects of the proposed change:

- Correctness of all technical information, including preparation, implementation, verification, and back-out procedures
- Completeness of change, testing procedures, and documentation
- Feasibility of the change
- Potential side effects and impact on other services or infrastructure
- Worst-case impact (both change and back-out procedure fail)

This review is performed by the technical resources familiar with the area affected by the change as well as other technical resources with general knowledge, such as architects, service managers, etc. It is important that authorization following the technical review is a formal sign-off recorded in the change log.

2.2.1.8 Review the RFC

Change management should briefly consider each request and filter out any that seem to be:

- Totally impractical
- Repeats of earlier RFCs
- Incomplete submissions, such as those with an inadequate description, or without necessary budgetary approval or justification

These should be returned to the initiator, together with brief details of the reason for the rejection, and the log should record this fact.

2.2.1.9 Assess and Evaluate the RFC

The potential impact to services and service assets and configurations needs to be fully considered prior to the change. Generic questions (such as the “seven Rs”) provide a good starting point.

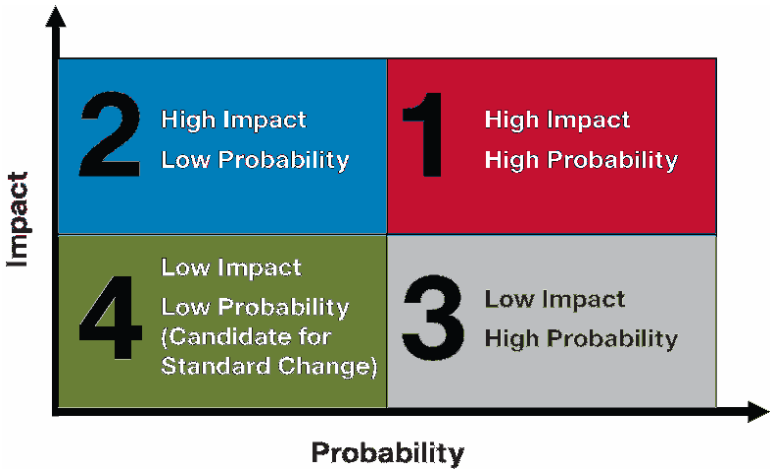
- Who raised the change?
- What is the reason for the change?
- What is the return required from the change?
- What are the risks involved in the change?
- What resources are required to deliver the change?
- Who is responsible for the building, testing, and implementation of the change?
- What is the relationship between this change and other changes?

When conducting the impact and resource assessment for RFCs referred to them, change management should consider relevant items, including:

- The impact that the change will make on:
  - The customer’s business operation
  - The infrastructure and customer service
  - Other services that run on the same infrastructure
  - Continuity plan, capacity plan, security plan, regression test scripts, and data and test environment
- The effect of not implementing the change
- The resources required to implement the change
- The current change schedule and projected service outage (PSO)
- Additional ongoing resources required if the change is implemented

Many organizations use a simple matrix like the one shown in Figure 2 to categorize risk. Sometimes, risk levels are categorized as High (1), Medium (2 or 3), and Low (4). In this scenario, the category of changes that has low impact in the event of failure and low probability of failure becomes a candidate for automation or at least a streamlined approval path.

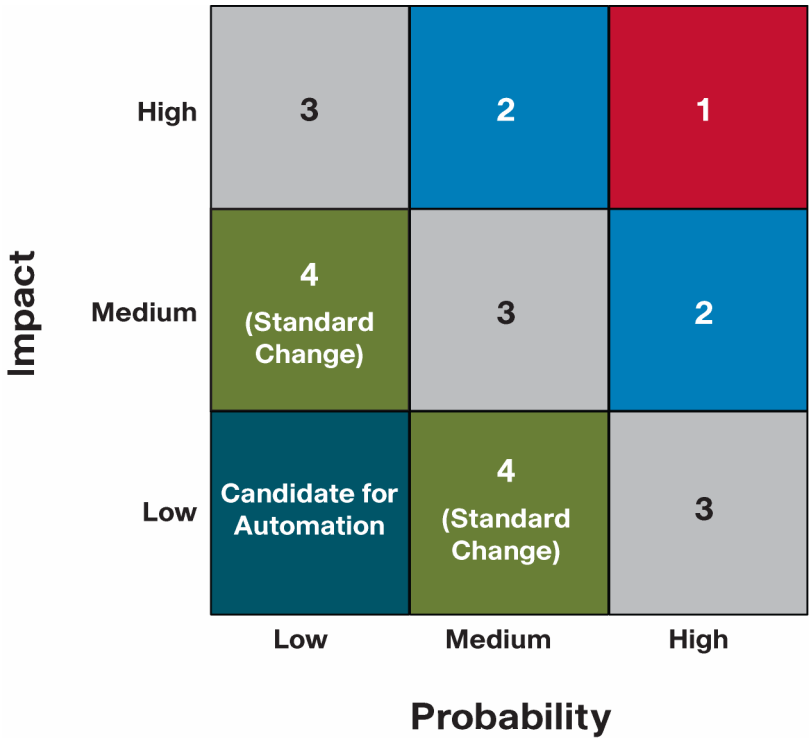
Figure 2. Risk Matrix



All members of the change authority should evaluate the change based on impact, urgency, risk, benefits, and costs. Each will indicate whether they support approval and be prepared to argue their case for any alterations that they see as necessary. In particular, subject matter experts (SMEs) in a particular discipline must evaluate the potential impact of the change on their area of expertise. For example, network SMEs are charged to examine the affect of the change on network resiliency, performance, and security.

The priorities of proposed changes should be established based on the assessment of the impact and urgency of the change. Initial impact and urgency will be suggested by the change initiator but may be modified in the change authorization process.

Figure 3. Risk Based Change Priorities (HML)



Impact is based on the beneficial change to the business that will follow from a successful implementation of the change, or on the degree of damage and cost to the business due to the error that the change will correct. The impact may not be expressed in absolute terms but may depend on the probability of an event or circumstance; for example a service may be acceptable at normal throughput levels, but may deteriorate at high usage, which may be triggered by unpredictable external items.

The urgency of the change is based on how long the implementation can afford to be delayed.

Table 1 lists examples of change priorities:

Table 1. Change Priority Examples

Priority	Corrective Change
Immediate Treat as emergency change	Putting life at risk. Causing significant loss of revenue or the ability to deliver important public services. Immediate action required.
High To be given highest priority for change building, testing, and implementation resources	Severely affecting some key users, or impacting on a large number of users.
Medium	No severe impact, but rectification cannot be deferred until the next scheduled release or upgrade.
Low	A change is justified and necessary, but can wait until the next scheduled release or upgrade.

2.2.1.10 Authorize the Change

Formal authorization is obtained for each change from a change authority. Depending on the size of the organization and the volume of changes, the authorizer may be a role, person, or a group of people. The levels of authorization for a particular type of change should be judged by the type, size, or risk of the change; for example, changes in a large enterprise that affect several distributed sites may need to be authorized by a higher-level change authority such as a global CAB or the Board of Directors.

Table 2 shows examples of change authorities:

Table 2. Change Authority Examples

Scope/Type of Change	Change Authority
Standard change	Local authorization
Minor change	Change manager
Emergency change	Emergency CAB
Normal change	CAB
Large or high-risk change	Executive board

2.2.1.11 Plan the Updates

Many changes may be grouped into one release and may be designed, tested, and released together if the amount of changes involved can be handled by the business, the service provider, and its customers and there is little risk of interference between the changes.

A common mistake in the implementation of changes is for business requirements to be overlooked. For example, change management should schedule changes to meet the needs of the business rather than for the convenience of IT. Change authorizers are charged with the responsibility to ensure that all pertinent needs are accounted for and considered prior to authorizing a change.

Pre-agreed and established change and release windows help an organization improve the planning throughout the changes and releases. Major releases may need to be scheduled with the business and stakeholders at a predetermined time. Wherever possible, change management should schedule authorized changes into target release or deployment packages and recommend the allocation of resources accordingly.

Change management coordinates the production and distribution of a change schedule and projected service outage (PSO). The change schedule contains details of all the changes authorized for implementation and their proposed implementation dates. The PSO contains details of changes that will impact SLAs and service availability. These documents are agreed upon in advance with the relevant customers within the business, service-level management, the service desk, and with availability management. Once agreed upon, the service desk should use established procedures to communicate any additional downtime that will result from the change to the user community.

2.2.1.12 Implement the Change

Authorized RFCs should be passed to the relevant technical groups for building of the changes. Best practices dictate that a formal work order process/system is used so that the changes can be tracked. Change management has responsibility for ensuring that changes are implemented as scheduled.

The following tasks are performed during this stage:

- Build the change
- Pre-test the change
- Complete change deployment plan
- Implement the change
- Test IT infrastructure post-change

Remediation procedures should be prepared and documented in advance for each authorized change so that if errors occur during or after implementation, these procedures can be quickly activated with minimum impact on service quality. Authority and responsibility for invoking remediation is specified in advance in the change documentation.

Change management has an oversight role to ensure that all changes are thoroughly tested. In all cases involving changes that have not been fully tested, special care needs to be taken during implementation. In such cases it is advisable to use a phased implementation approach, starting with a small pilot in the production environment until the behavior resulting from the change can be established. Once observations are made and confidence increases, additional phases can be rolled out.

Testing may continue in parallel with early live usage of a service—looking at unusual, unexpected, or future situations so that further correcting action can be taken before any detected errors become apparent in live operation.

The implementation of such changes should be scheduled when the least impact on live services is likely. Support staff should be available to quickly respond to any incidents that might arise.

2.2.1.13 Post Implementation Review

On completion of the change, the results should be reported for evaluation to those responsible for managing changes, and then presented as a completed change for stakeholder agreement (including the closing of related incidents, problems, or known errors).

A review should also include any incidents arising as a result of the change (if they are known at this stage). If the change is part of a service managed by an external provider, details of any contractual service targets will be required (for example, no priority 1 incidents during the first week following implementation).

A post-implementation review (PIR) should be carried out to confirm that the change has met its objectives, that the initiator and stakeholders are happy with the results, and that there have been no unexpected side effects. Lessons learned should be factored into future changes. Small organizations may opt to spot-check changes rather than conduct a large-scale PIR; in larger organizations, sampling will have a value when there are many similar changes taking place.

Change management must review new or changed services after a predefined period has elapsed. This process will involve CAB members, because change reviews are a standard CAB agenda item. The purpose of such reviews is to establish that:

- The change has had the desired effect and met its objectives
- Users, customers, and other stakeholders are content with the results (if not, the review should identify any shortcomings)
- There are no unexpected or undesirable side effects to functionality, service levels, or warranties, such as availability, capacity, security, performance, and costs
- The resources used to implement the change were as planned
- The release and deployment plan worked correctly (the review should include comments from the implementers)
- The change was implemented on time and to cost
- The remediation plan functioned correctly, if needed

Where a change has not achieved its objectives, change management (or the CAB) should decide what follow-up action is required, which could involve raising a revised RFC. If the review is satisfactory or the original change is abandoned (for example, when the circumstances that required the change are no longer current and the requirement disappears) the RFC should be formally closed in the logging system.

2.2.1.14 Close the Change

The change is closed and documented in the configuration database. It is important to note that every step of the change process and every status change of the RFC must be documented in the configuration database.

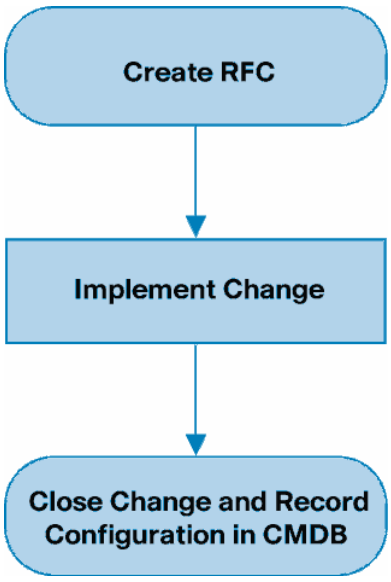
The change success, failure, related plans, etc. are communicated to all stakeholders. In fact such communication must take place throughout the RFC lifetime. This can be automated by having the change management tool send status updates to a predefined distribution list.

2.2.2 Standard (Preauthorized) Change

A standard change is a change to a service or infrastructure for which the approach is preauthorized by change management. A standard change has an accepted and established procedure to provide a specific change requirement.

- The crucial elements of a standard change are that:
- Approval of a standard change will be granted by the delegated authority for that change
- There is a defined trigger to initiate the RFC
- The tasks are well known, documented, and proven
- Authority is effectively given in advance
- Budgetary approval will typically be preordained or within the control of the change requester
- The risk is usually low and always well understood

Figure 4. Standard Change Process Flow



2.2.3 Emergency Change

Emergency changes are usually initiated in response to a critical IT situation, often an incident or problem requiring immediate action to restore service or prevent service disruption. Emergency changes are sometimes required and should be designed carefully and tested before use or the impact of the well intended but errant emergency change may be greater than the original incident. Some details of emergency changes may be documented retroactively. Specific procedures should be devised to deal with emergency changes quickly, without sacrificing normal management controls.

The number of emergency changes proposed should be kept to an absolute minimum, because they are generally more disruptive and prone to failure with corresponding negative impacts to network and service availability.

The emergency change category is reserved for changes intended to repair an error in a service that is negatively impacting the business to a high degree.

Effectively, the emergency change procedure will follow the normal change procedure except that:

- Approval will be given by the emergency CAB (ECAB) rather than waiting for a CAB meeting.
- Testing may be reduced, or in extreme cases forgone completely, if considered a necessary risk to deliver the change immediately.
- Documentation, such as updating the change record and configuration data, may be deferred, typically until normal working hours.

2.2.3.1 Emergency Change Authorization

Defined authorization levels will exist for an emergency change, and the levels of delegated authority must be clearly documented and understood. In an emergency situation it may not be possible to convene a full CAB meeting. Where CAB approval is required, this will be provided by the ECAB.

Not all emergency changes will require ECAB involvement; many may be predictable both in occurrence and resolution. For such well understood changes, authority may be delegated, for example to operations teams who will implement, document, and report on the emergency change.

2.2.3.2 Emergency Change Building, Testing, and Implementation

Authorized changes are allocated to the relevant technical group for building. As much testing as possible should be carried out for the emergency change to minimize the chances of unforeseen negative impacts to the network. Completely untested changes should not be implemented if at all avoidable. Remediation must also be addressed.

This means that the greater the chances are that the change will be successful, the more reasonable it may be to reduce the degree of testing in an emergency. When only limited testing is possible—and presuming that parallel development of more robust versions of the change or solution continues alongside the emergency change—then testing should be targeted toward:

- Aspects of the service that will be used immediately
- Elements that would cause the most short-term inconvenience

Change management will give as much advance warning as possible to the service desk and other stakeholders of emergency changes and arrange for adequate technical presence to be available, to support service operations.

2.2.3.3 Emergency Change Documentation

It may not be possible to update all change management records at the time that urgent actions are being completed (for example, during overnight or weekend working). It is, however, essential that temporary records are made during such periods, and that all records are completed retroactively, at the earliest possible opportunity.

Incident control staff, computer operations, and network management staff may have delegated authority to restore or repair certain types of incident (such as hardware failure) without prior authorization by change management. Such circumventions should be limited to actions that do not change the specification of service assets and that do not attempt to correct software errors. The preferred methods for circumventing incidents caused by software errors should be to revert to the previous trusted state or version, as relevant, rather than attempting an unplanned and potentially dangerous change to an untested version. Change approval is still a prerequisite.

2.2.4 Expedited Change

An expedited change is a normal change that must be implemented in the shortest possible time for business or technical reasons. While it is not as critical as an emergency change, it must be processed in a faster manner than a normal change. Organizations may choose to deal with such changes by assigning high priority to them, or by creating a separate change model.

2.3 Change Management Tools

A change ticketing tool will help ensure that:

- All of the requirements for a proposed change are collected and available for evaluating risk
- The change is scheduled for implementation
- Status updates are communicated to stakeholders
- Users can generate change reports that can be used to govern the change process itself and provide change management with actionable feedback on change activity

Other features that can be very useful are:

- Improve operational efficiency by providing integration opportunities with other systems including trouble-ticketing tools, problem-management tools, and the configuration database, which can be useful in troubleshooting and evaluating the potential impact to the network
- Allow parent/child relationships between changes (i.e. a “parent” change is composed of a number of related “child” changes)

2.4 Continuous Process Improvement

2.4.1 Process Improvement Program

In order to continuously assess and improve the change management process, a process improvement program (PIP) must be implemented. This program must be:

- Formal
- Documented
- Continuous and periodic (various activities may have different intervals)
- Used by management for key business decisions

The goal of the PIP is to achieve the following critical success factors (CSFs):

- A repeatable process for making changes
- Make changes quickly and accurately (driven by business needs)
- Protect services when making changes
- Deliver process efficiency and effectiveness benefits

The main activities of the PIP are:

- Process measurement
- Process reporting
- Process assessment
- Process improvement

2.4.1.1 Process Measurement

Process measurement is performed on a weekly or monthly basis. During change management process design, a number of key performance indicators (KPIs) are established. The corresponding measurements are collected on a regular basis and are used for trending and summarizing (see the next section).

2.4.1.2 Process Reporting

Process reporting is performed on a monthly or quarterly basis. The report is intended for change management staff as well as management (service, IT, business). The report should present summary information in the form of a dashboard or a balanced scorecard, by rolling up collected KPIs. The report should include trend analysis and potential process issues. The “raw” data of periodic KPI measurements provides little value to management, but it can be included as backup information.

2.4.1.3 Process Assessment

Process assessment is performed on a semi-annual or annual basis. While improvement activities can take place anytime, it is important that a full formal assessment is carried out regularly. The assessment will cover people, process, and technology. The following tasks should be performed during process assessment:

- Audit a sample of changes for compliance to the process
- Audit the change management process for completeness, efficiency, and effectiveness
- Evaluate against the previous assessment period
- Benchmark against industry best practices
- Compare current status with CSFs
- Establish improvement actions
- Re-evaluate CSFs for next assessment period

2.4.1.4 Process Improvement

All the improvement actions established during process assessment must be documented in the PIP. The plan should list deliverables, due dates, implementation resources, and people responsible for completion. One useful technique for process improvement is the Deming cycle: Plan, Do, Check, Act.

2.4.2 Key Performance Indicators and Measurements

Change management must ensure that measures have specific meaning. Measures taken should be linked to business goals wherever practical—and also to cost, service availability, and reliability. Any predictions should be compared with actual measurements.

Meaningful measurements provide management with actionable feedback that results in timely and accurate decision-making. For example, reporting on the number of changes is meaningless. Reporting on the ratio of authorized changes implemented versus RFCs received provides an efficiency rating. If this rating is low, management can easily see that changes are not being processed in an efficient or effective manner and then take timely action to correct the deficiencies causing this.

2.4.3 Examples of Measures

Some examples of the types of measures used within organizations are listed here. Most of the listed measures can be usefully broken down by category, organizational division, geography, supplier, etc.

2.4.3.1 Operational Metrics

- Number of disruptions, incidents, problems/errors caused by unsuccessful changes and releases
- Inaccurate change specifications (such as technical, customer, business)
- Incomplete impact assessment
- Unauthorized business/customer change by business/IT/customer/user asset or configuration item type, such as application data
- Percentage reduction in time, effort, cost to make changes and releases (for example, by service, change type, asset type)
- Service or application rework caused by inadequate change specification
- Percentage improvement in predictions for time, quality, cost, risk, resource, and commercial impact
- Percentage improvement in impact analysis and scheduling of changes safely, efficiently, and effectively reduces the risk of changes affecting the live environment
- Percentage reduction in unauthorized changes

2.4.3.2 Workloads

- Frequency of change (by service, business area, etc.)
- Volume of change

2.4.3.3 Process Measures

- People's satisfaction with the speed, clarity, and ease of use
- Number and percentage of changes that follow formal change management procedures
- Ratio of planned versus unplanned changes (urgent, emergency)
- Ratio of accepted to rejected change requests
- Number of changes recorded and tracked using automated tools
- Time to execute a change (from initiation through each stage in the lifecycle of a change, ending in completion):
  - By lifecycle stage
  - By service
  - By infrastructure platform
- Staff utilization
- Cost against budget

2.4.4 Example KPIs

The following KPIs can be used to measure the performance of the change management process. The next section indicates how KPIs relate to metrics and CSFs.

- Change efficiency rate
- Change success rate
- Emergency change rate
- Change reschedule rate
- Average process time per change (days)
- Unauthorized change rate
- Change incident rate
- Change labor workforce utilization
- Change management tooling support level
- Change management process maturity

2.4.5 Summarizing Measures

The metrics above can be rolled up in key performance indicators (KPIs) and critical success factors (CSFs). The KPIs and CSFs can then be reported to management via the dashboard or balanced scorecard. For instance the KPI “change success rate” can be computed as:

“Number of failed changes” / “Total changes implemented”

Furthermore, various KPIs can be used to calculate the CSFs listed in 2.4.1. For example the CSF “Protect services when making changes” is calculated using the following KPIs: “emergency change rate,” “unauthorized change rate,” and “change incident rate.”

3 Conclusion

Change management is one of the most important service management processes. Any organization—no matter its size—will experience a large volume of changes in order to accommodate new business requirements, to correct faults in the infrastructure or the services, or for other reasons (such as legal requirements). All changes have a disruptive potential for the business, hence controlling the release of changes is critical. Change management is even more effective in reducing service disruptions in concert with other service management processes, in particular configuration management, release management, problem management, and incident management.

4 References

- Office of Government Commerce (OGC): ITIL V2, The Stationery Office (TSO)
  - Service Support, 2000, ISBN 0 11 330015 8
  - Planning to Implement Service Management, 2002, ISBN 0 11 330877 9
- Office of Government Commerce (OGC): ITIL V3, The Stationery Office (TSO)
  - Service Transition, May 2007, ISBN 9780113310487
  - Continual Service Improvement, May 2007, ISBN 9780113310494
- ISO/IEC 20000:2005:
  - Part 1: Specification

  - Part 2: Code of Practice
- IT Governance Institute: COBIT 4.1, 2007
- ITSM Community: Sample: Change Management Process Guide, http://www.itsmcommunity.org/Resources/templates
- Randy A. Steinberg: Measuring ITIL, Trafford Publishing, Jan. 2001, ISBN 978-1412093927

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C11-458050-00 03/08