

6 STEPS TO IMPLEMENTING **CHANGE MANAGEMENT** THAT WORKS





TABLE OF CONTENTS

- 1 -- Introduction
- 3 -- Identify why you want to implement change management
- 4 -- Sell the value of change management
- 5 -- Define what a change is
- 8 -- Assign roles and responsibilities
- 11 -- Define a process for handling changes
- 14 -- Define Key Performance Indicators
- 15 -- Conclusion
- 16 -- About ManageEngine
- 17 -- About the author



Introduction

Everyone knows change is never easy, but often quite necessary. The statement is never truer than in IT.

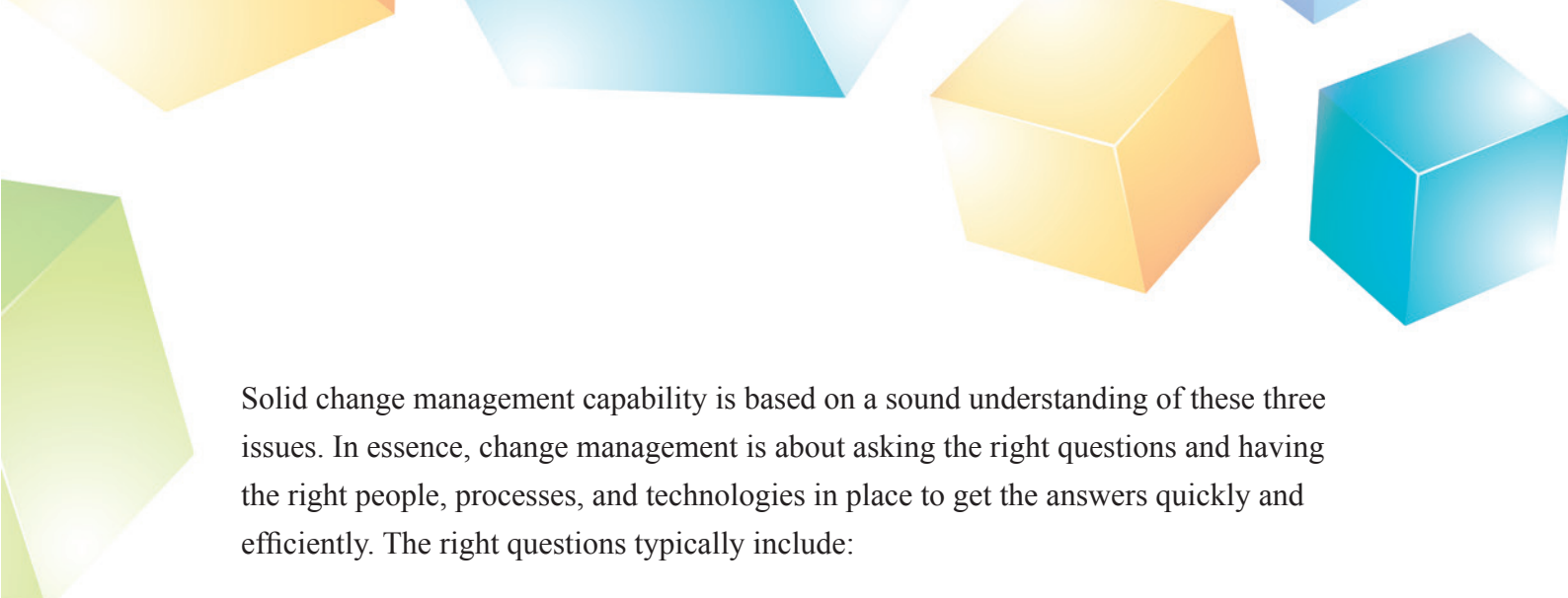
Solid change management capability will help you boost your ITSM maturity, break out of the “firefighting mode,” align IT activity with business objectives, and transform IT from a service provider to a business innovator. However, these benefits don’t come easily. Change management is one of the most difficult ITIL processes to get right. Why? Because change management is an ITSM process that needs the right mix of people, processes, and technologies.

Think of change management as a three-legged stool. If one of the legs is weak, the stool will fall. ITIL guidance focuses a lot on terminologies and processes but contains little practical advice on the actual implementation of each process. This white paper lists the steps involved in implementing a solid change management process.

First, a quick definition of change: *The addition, modification, or removal of anything that could have an effect on IT services.*

This definition raises three change-related issues:

- **Why:** The reason for the change. What is the business benefit you hope to achieve with the change?
- **What:** Is it hardware, software, system architecture, a process, documentation, or a combination of these that will be subjected to change?
- **Impact:** What are the possible negative consequences of the change (bearing in mind the complex interdependencies of today’s computer systems) – and how to avoid these consequences?



Solid change management capability is based on a sound understanding of these three issues. In essence, change management is about asking the right questions and having the right people, processes, and technologies in place to get the answers quickly and efficiently. The right questions typically include:

- What is the cost of making the change?
- Does the benefit outweigh the cost?
- What is the business priority of the change?
- How do we implement the change?
- Who will implement the change?
- When should we implement the change?
- What do we do if the change goes wrong? Do we have a backup plan in place?

Answering these questions reliably is the hard part; implementing the changes is easier.

Change management and configuration management

ITIL recommends implementing change management in conjunction with configuration management, but you don't need to implement 100% of configuration management before you can get started with change management. The key is to understand the touch points between the two. In simple terms, change management needs a view of the infrastructure to assess the impact of a change. Configuration management needs changes to be recorded, so that the configuration management database (CMDB) is kept up-to-date and always represents the live environment.



Step 1

Identify why you want to implement change management

To begin, you need a clear idea of what you want to do and why. All of the activities involved in implementing change management should be focused on achieving the above-mentioned objectives. If something can't be linked back to one of these objectives, it's probably not a priority. It might help to write a bullet-point summary of why you need to do change management, print it big, and stick it to a wall where everybody can see it.

Critical Success Factors:

- Get executive buy-in for your change management implementation by selling the benefits and the objectives at a high level.
- Agree to a high-level change policy that prohibits unauthorized changes and gives the change management function the authority to make decisions and handle resistance.

Step 2

Sell the value of change management

If you want to improve infrastructure stability, service quality, and IT agility, change management is a “necessary evil.” It’s unpopular because it’s fundamentally about asserting control. IT people already think they’re often told how to do their jobs, so adding something like a cumbersome change control process will just slow them.

Implementing change management is more about organizational change than changing technical operations. Like any other organizational change, you have to sell the value to the stakeholder groups who will be affected by the implementation and get them on board. Identify the WIFM factor. Each individual is asking “what’s in it for me?” It’s important to answer this question to get a buy-in. A good starting point is to make a list of the distinct groups that will be affected by the implementation. Next, analyze what they do, how they do it, and what will change for them. Then, let each of these groups know what will be expected of them and how they will benefit.

Critical Success Factors:

- Communicate the “why” before you communicate the “what.”
- Answer the question, “what’s in it for me?” for each stakeholder group.

Step 3

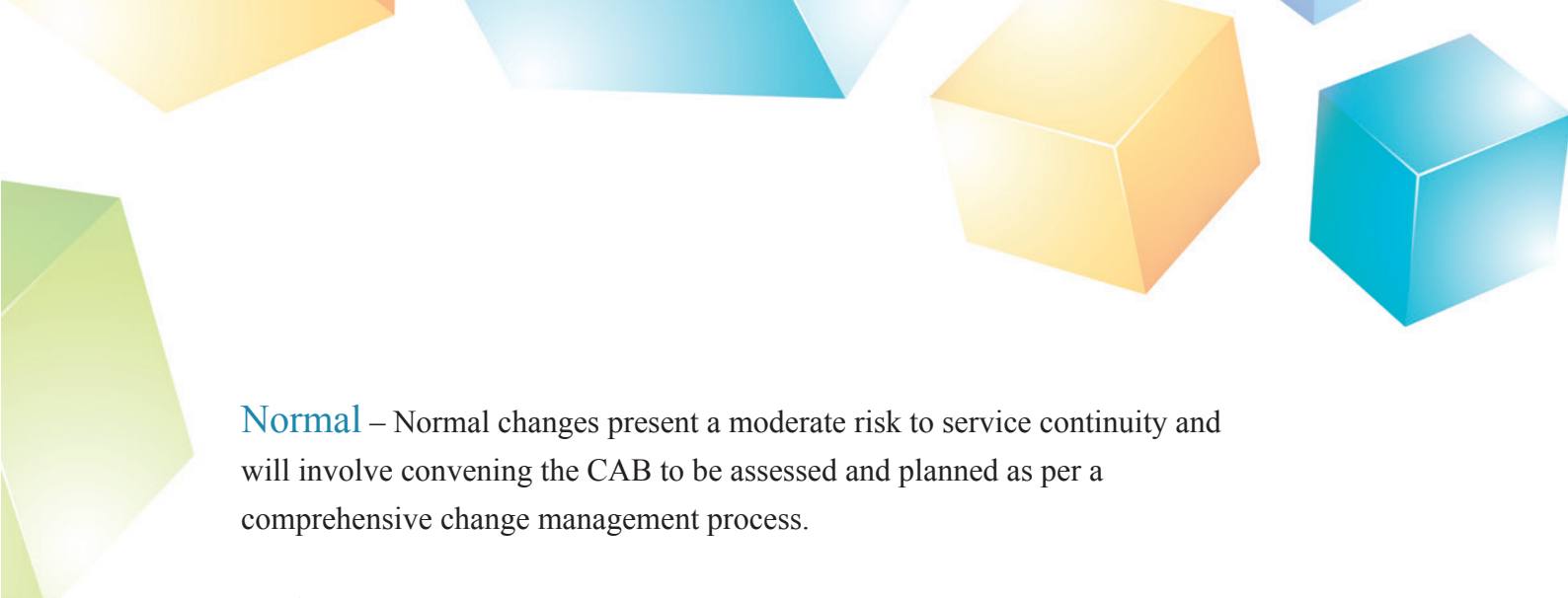
Define what a change is

Don't expect everybody to be on the same page when you use the word "change." It means different things to different people, so it's essential to have a clear definition of a change model. ITIL recommends defining a change model that separates changes into groups according to scope, impact, and urgency.

Change management is about balancing progress with risk, so a change model is an essential part of efficient change management, enabling low-risk changes to be applied quickly with minimal cost and resource usage. Without this distinction, all changes (no matter how minor) must go through the full process, which can mean tying people up with trivial changes, while larger, more transformative changes may be delayed. Typical levels in a change model might include the following, but this can be adapted to suit your organization:

Standard – Simple, low-risk changes and service requests with a well-defined procedure for execution do not require assessment by change management and might only require the approval of the requester's line manager. The simplest types of change (e.g. a password reset) might not require any authorization at all. Standard changes do not generate Request for Changes, because change management does not assess them. Instead, for maximum efficiency, an automated service request system or service catalogue should handle standard changes with requests automatically triggering a workflow that routes implementation actions to the relevant technical groups.

Minor – Minor changes are relatively low risk, but have some limited potential impact. Therefore, they will require a formal RFC and invoke a simple change management process that balances the level of risk against cost and resources. For such changes, planning and approval may be handled entirely by the change manager and not involve the Change Advisory Board (CAB).



Normal – Normal changes present a moderate risk to service continuity and will involve convening the CAB to be assessed and planned as per a comprehensive change management process.

Major – Major changes are significant in terms of business benefits, scale, and risk. The level of importance and risk is known to be high, so a major change will involve a large number of people to assess, plan, and execute it. Due to the high risk, a major change would usually be escalated to a higher change authority for approval.

Emergency – Emergency changes are those that must be performed quickly in response to an immediate need, such as an issue that is disrupting business operations. Consequently, emergency changes bring not only the greatest risk to business, but also the greatest benefit (e.g., restoring business continuity).

The Emergency CAB (ECAB) will be convened to deal with such emergencies quickly and decisively. The process for handling emergency changes will be streamlined and focused on making a change as quickly as is practically possible while accounting for the risk of compounding the problem. As such, some testing will be performed before implementation, but more comprehensive testing and tweaking may continue for some time afterwards.

When categorizing changes according to your change model, it is better to err on the side of caution. Map changes with unknown risk and impact to a high level in the change model (e.g., normal or major) to ensure the potential impact is fully and thoroughly assessed. At the tail end of the process, the evaluation stage will identify whether the change category can be moved down a level in the model, e.g., become a standard change that can be handled more quickly and efficiently next time around.



Critical Success Factors:

- Communicate a management-sanctioned policy to ensure all changes to IT infrastructure and services run through change management and unauthorized changes stop.
- Implement a change model to ensure cost and agility is balanced against risk.

Change management requires a disciplined approach to controlling change, reinforced by official policy and executive backing. The change management function needs the authority to enforce the process across the whole organization.

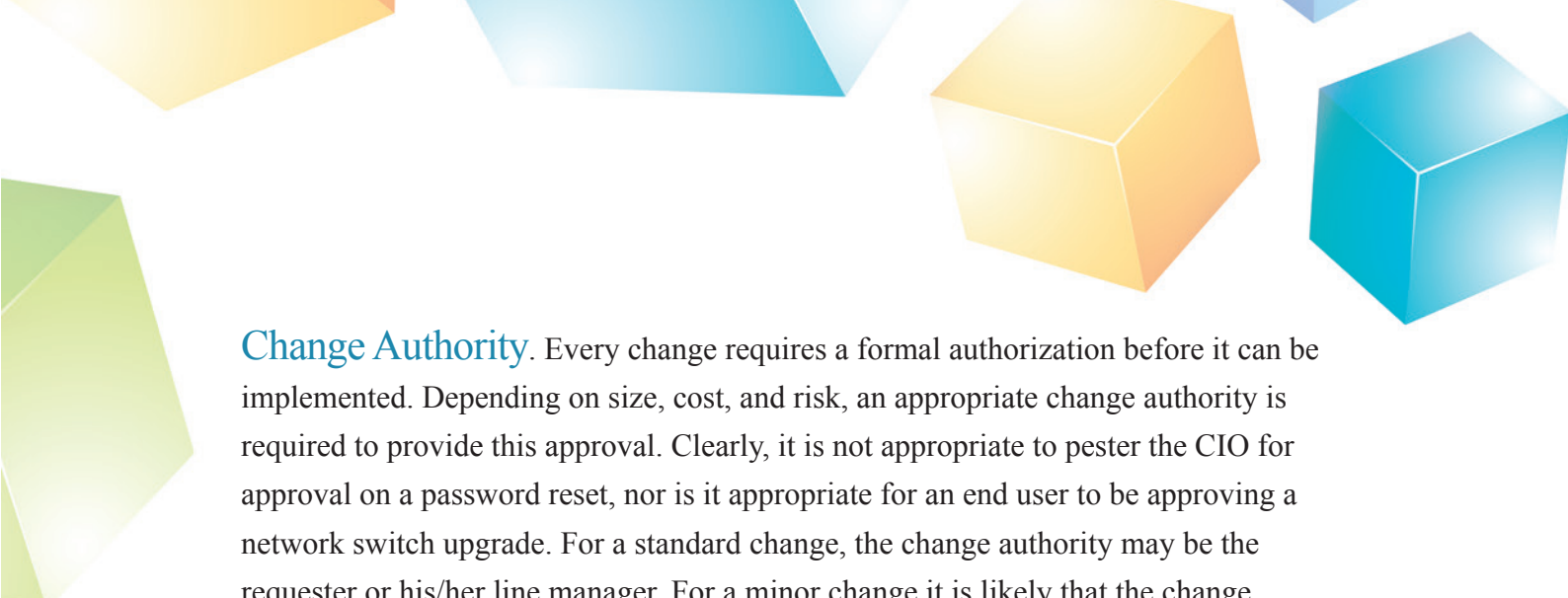
Step 4

Assign roles and responsibilities

Processes need people to take actions and make decisions. That is, clearly defined roles and responsibilities are a must-have to ensure ownership is maintained and execution is smooth. So, who will you need to support your change management process?

Change Manager. The change manager is not a popular function (particularly in the early stages of an implementation), so it takes a certain type of person to fill the shoes of a change manager. Those who seek popularity and positive feedback need not apply. In small and mid-size organizations, the change manager is not necessarily a dedicated role. Sometimes the problem manager or the configuration manager might assume this role, although there are some potential risks involved when one person has authority over changes and updating the CMDB. The incident manager/service desk manager shouldn't be nominated as change manager due to conflict of interests between the two roles. In larger organizations, the change manager role may take the form of a steering group, headed up by a change leader who has final say on authorization. Generally, the change manager needs to be highly organized, communicative, diplomatic, understanding, decisive, and most of all, thick-skinned.

Deep technical skills are not essential but will certainly help when communicating with technical teams. The change manager is responsible for reviewing submitted RFCs, scheduling CAB meetings, authorizing changes, updating change records, coordinating the build/test/implementation of changes, reviewing implemented changes, producing reports, and improving the change process.



Change Authority. Every change requires a formal authorization before it can be implemented. Depending on size, cost, and risk, an appropriate change authority is required to provide this approval. Clearly, it is not appropriate to pester the CIO for approval on a password reset, nor is it appropriate for an end user to be approving a network switch upgrade. For a standard change, the change authority may be the requester or his/her line manager. For a minor change it is likely that the change manager will be the suitable change authority. For normal changes, the CAB and the change manager will collectively form the change authority. And for major changes – those with a significant scale, cost, benefit, and potential business impact – the change authority may be a director, c-level manager, or indeed, the board of directors.

Change Advisory Board (CAB). It is the CAB's responsibility to assess each change from a business, technical, and financial viewpoint and make recommendations on the impact, planning, and approval. CAB membership is flexible and draws in people from IT operations, development, and business to ensure all angles are represented when discussing the implementation of an individual change. The change manager will decide which CAB members will attend a meeting depending on the nature of the change (or changes) in question. CAB meetings around individual changes can be done virtually, but a core CAB team should also meet periodically to review policies and procedures, on-going changes, and change backlog.

Emergency Change Advisory Board (ECAB). The ECAB (referred to by ITIL as the CAB Emergency Committee or CAB/EC) is a smaller, core group of CAB members that is available on short notice to respond to emergency changes that must be made on a short notice (perhaps also outside of normal working hours) to remedy an urgent issue. The ECAB is the change authority for emergency changes and must have the power to make decisions in an emergency without escalation.



Critical Success Factors:

- Clearly defined roles and responsibilities.
- Strong skills in organizational change management.
- Executive sponsorship to deal with resistance to change.
- The CAB must represent all stakeholder groups across both IT and business, including business managers, end users, developers, system administrators, the service desk, customers, and suppliers, as appropriate to each individual change.
- A clear interaction and a good understanding among staff is needed when interactions related to change management and other service management processes happen.

Step 5

Define a process for handling changes

RFCs need to go through a managed process to guide decision making and execution toward a successful outcome. A formal change management process is critical to implementing change in a fast, resource-efficient, low-risk manner.

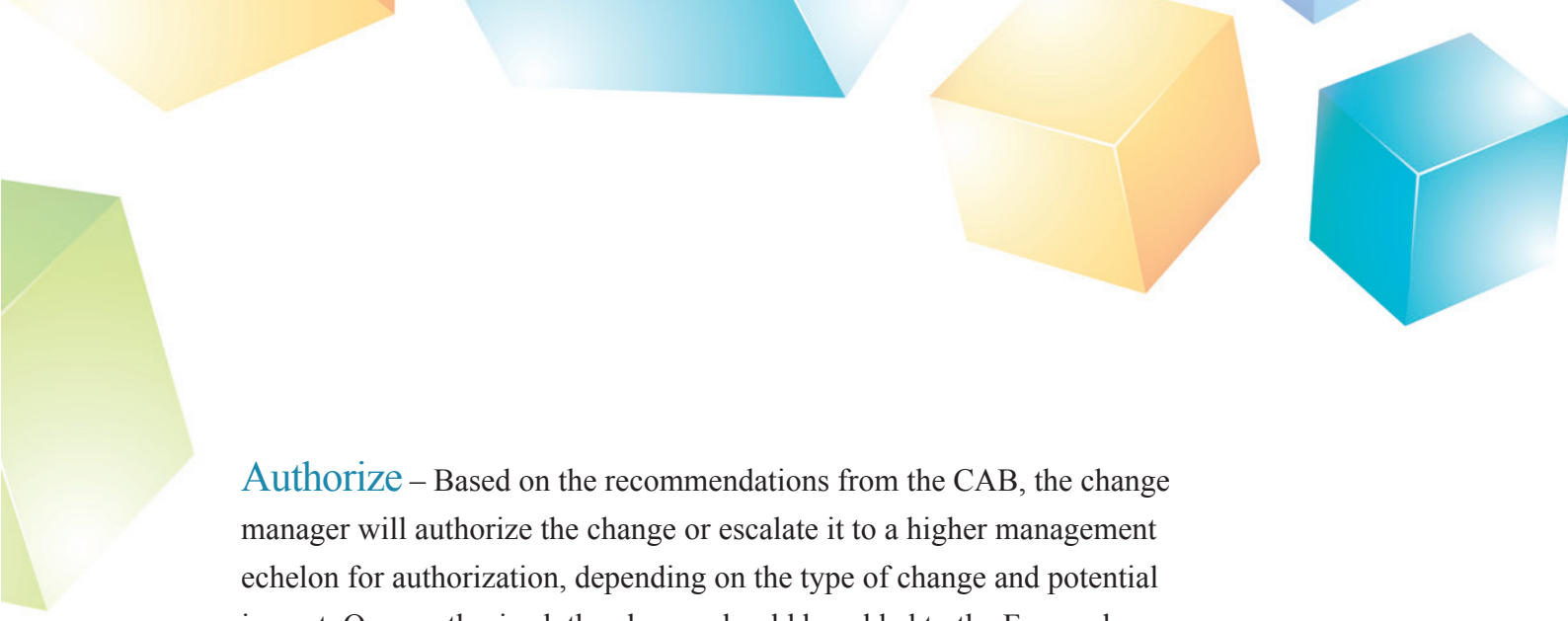
The change management process will never be 100% right the first time around, but some process is better than no process. If the initial process is insufficient for managing changes, you will still see a high incidence of failed changes. Failed changes means extra work for IT, impact on business productivity, and lost revenue. If you look back at the end of your change management process and how well it performed, you can tweak it for the next time round. Over time, it will become more efficient and effective.

ITIL focuses heavily on the process side of change management, so it is wise to consult the ITIL V2 Service Support or ITIL V3 Service Transition volumes, but the typical process that ITIL recommends is as follows:

Record – All changes to the infrastructure must be recorded by submitting a Request for Change (RFC).

Review – The change manager acts as gatekeeper and will make a quick review of each RFC to decide whether it should proceed. Is it valid, specific, beneficial, feasible, and necessary? If so, the RFC will be accepted and classified. Otherwise, it might be rejected and returned to the requesting party.

Assess – The change manager and the CAB (containing appropriate representatives from the business, user community, development, support, and any appropriate third parties) will assess the costs, resources, benefits, and risks (including impact on services) and will plan the execution of the change, including a back-out procedure.



Authorize – Based on the recommendations from the CAB, the change manager will authorize the change or escalate it to a higher management echelon for authorization, depending on the type of change and potential impact. Once authorized, the change should be added to the Forward Schedule of Changes (FSC).

Coordinate implementation – It is the responsibility of the change manager to coordinate execution of the change plan, including ensuring build, testing, and implementation actions in the right manner and at the right time as agreed and published in the FSC.

Evaluate and close – If the change has been successful, the RFC will be closed and the Post Implementation Review (PIR) will commence to assess the benefits of the change and how well the change process supported the implementation. The PIR will answer questions such as did the change achieve the objective? Is everybody satisfied with the results? Were there any side effects? Did the implementation exceed planned costs, resource usage, or downtime? It is here that continual improvement of the change management process happens. Any lessons learned from the experience can be fed back into the process to make it more efficient and effective.



Critical Success Factors:

- Communicate the change process to IT and the business to improve understanding and reduce the number of unauthorized changes circumventing the process.
- Most organizations will need tools to log RFCs, perform automated classification, trigger and manage process workflows, and support impact assessment with a service-oriented view of the infrastructure.
- Publish an FSC – a calendar of all authorized changes – in a place that is accessible to everybody in the business.
- Ensure each RFC is logged with a unique reference number and date-stamp that contains as much detail as possible on what the change is and why it is required also references the project or problem record from which it originates.
- Don't implement any change without a back-out plan that can be used to quickly roll back to a stable configuration if the change fails.
- Ensure changes and back-out plans are tested in a safe environment, e.g., a sandbox that mirrors the live environment as closely as possible.
- Embed continual improvement in the evaluation stage to refine the process over time.

Step 6

Define Key Performance Indicators

Change management is one of the most difficult ITIL processes to implement, but also one of the most valuable and critical to increasing IT maturity. To maintain momentum, it is important to report on the business value that the change management function is delivering. Key performance indicators (KPIs) will vary from one organization to the next, but the following metrics generally indicate how well change management is working and the value it is bringing to service management and the business.

Key performance indicators refer to:

- Number of successful changes
- Number of failed changes that were rolled back
- Number of changes in the backlog
- Number of incidents caused by change
- Number of emergency/out-of-hours changes
- Number of unauthorized changes identified
- Resources used and funds spent on changes
- Percentage of changes that happened as per the FSC

Critical Success Factors:

- Define a set of KPIs that are relevant to your organization.
- Use KPIs to communicate the value of change management to the business and specific IT groups on a regular basis.



Conclusion

A solid change management process means IT can safely say “yes” to more requests for change from the business and IT might shake off its image as “The No Department.” Through change management, IT can quickly improve infrastructure quality, reduce service disruption, and be more responsive to the business. The business will undoubtedly notice the difference.

By following this 6-step process of implementation, you can improve your chances of a successful implementation, shorten the time-to-value, and gain support for further ITSM process work.

1. Identify why you want to implement change management
2. Sell the value of change management
3. Define what a change is
4. Assign roles and responsibilities
5. Define a process for handling changes
6. Define key performance indicators (KPIs)



About ManageEngine

ManageEngine is the leader in low-cost enterprise IT management software.

The ManageEngine suite offers enterprise IT management solutions including Network Management, Help Desk & ITIL, Bandwidth Monitoring, Application Management, Desktop Management, Security Management, Password Management, Active Directory reporting, and a Managed Services platform. ManageEngine products are easy to install, set up and use and offer extensive support, consultation, and training. More than 90,000 organizations from different verticals, industries, and sizes use ManageEngine to take care of their IT management needs cost effectively. ManageEngine is a division of Zoho Corporation. For more information, please visit www.manageengine.com.



About the Author

Arvind Parthiban has over 8 years of experience in ITSM and ITIL. He has specializations in worldwide service desk implementations and consulting. Arvind has been an advocate for innovative approaches to learning and change throughout his career and has assisted 100+ global companies like DHL Global, Wolters Kluwer, Urban Outfitters, Pre Corp USA, Smart Tech CA, Stroz Inc, Franklin University in their IT needs. He works currently as a Senior Marketing Manager for ManageEngine where he strategizes and markets ITSM group of products at ManageEngine and also oversees the complete implementation cycles in various environments while understanding and solving new problems and potential setbacks faced by IT administrators to deliver best results. He has authored the capstone book ‘CMDB Implementation: A Tale of Two Extremes’ where he talks about simplifying the process of implementing CMDB. In his whitepaper, “When Reality Hits ITIL Implementations,” Arvind insists that it is very important to understand the environment and get the basics in ITIL right before proceeding any further. He also shares his crazy experiences in his blog page: itilism.com. When not slaving over a hot Apple Mac, he enjoys outdoor life; playing football and travelling.