CHANGE TYPES: STANDARD VS. NORMAL VS. EMERGENCY CHANGE

It's no surprise that many people ask themselves, "What is the difference between normal, standard, and emergency change types?" The terms are not always clearly understood, yet in change management, clarity is vital.

Before we go further down the rabbit hole of change management, let's make sure we're on the same page of what we mean when we refer to change.

What is change?

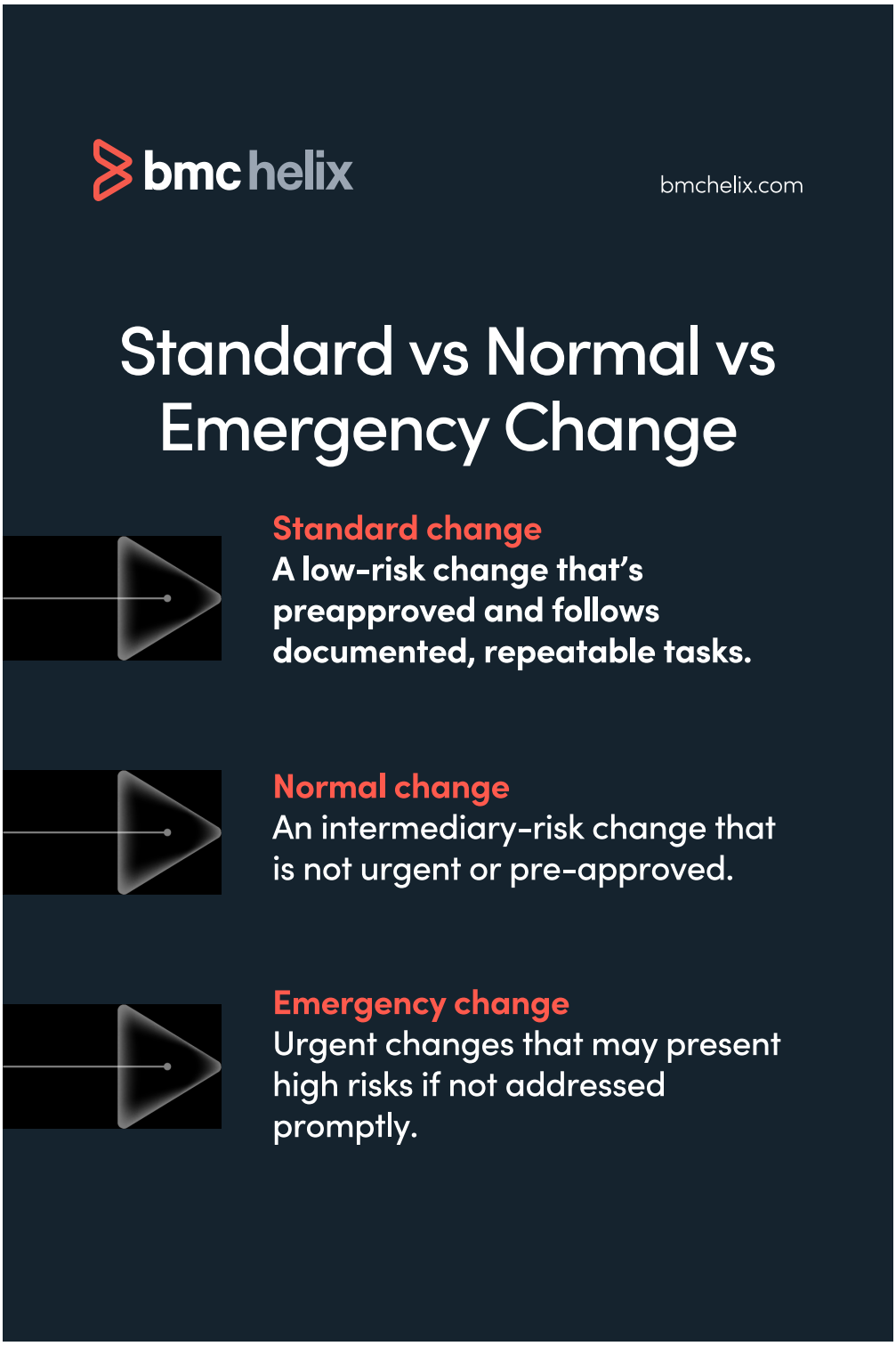
In the context of the IT business world and, more specifically, the world of ITIL management, change refers to modifications to the organization's software applications whether those are internal applications or client-facing products. Change in this context includes updates to existing code and systems that are tested and implemented into live environments.

This process of change management is handled by the Change Manager and Change Advisory Boards (CABs). The CAB generally handles two main types of changes about which they gather information before giving the final go-ahead for implementation to occur:

- Standard change
- Normal change

These specific definitions and designations might change from one organization to the next depending on their needs, but there are some general rules under which they tend to operate. Let's start exploring these processes by examining a standard change.

(Emergency changes, which we'll go over later, are changes that are more pressing and sensitive, handled by the Emergency Change Advisory Board or ECAB, which is typically a subset of the CAB.)



What is a standard change?

Standard changes, sometimes called Routine changes, tend to be pre-authorized changes that are considered to have little to no risk associated with them. They are fairly common occurrences that have specific guidelines and procedures which they follow. Standard changes are implemented often with repeatable steps that seldom require modifications. The CAB usually doesn't review each case of a Standard change and instead establishes protocol and overviews the guidelines for enacting Standard changes.

Standard changes are often areas where automation can be implemented to help speed up the process and increase efficiency. These changes have been refined into a neat, ordered systematic approach that reliably results in success. Automating aspects of these Standard changes can drastically reduce time wasted on the process and free up man hours for work that requires a bit of human ingenuity.

ITIL change management defines Standard Change as:

> *"A pre-authorized change that is low risk, relatively common and follows a procedure or work instruction".*

Consider standard as the services that IT offers to its end users. Services such as:

- Lifecycle replacement of hardware
- Software patching and updates
- Firewall changes
- New DNS entries

These are all examples of pre-authorized tasks that IT can follow immediately once a change request or requirement arises. Following the authorization of such changes, minimal planning is required to perform a change request fulfillment. These changes typically arise as service requests from end-users and are well-anticipated in advance, not necessarily in terms of a specific time frame.

Standard changes may also include operational changes that follow a specific schedule, such as refresh cycles of printers, workstations and networking devices.

The change implementation procedure is straightforward and rarely introduces an issue or risk. A thorough risk assessment procedure is executed prior to the authorization of standard changes. Only a business change or IT incident would require re-evaluation of the risks associated with standard changes.

It is described as a Standard Change since the approval and pre-authorization is at the discretion of the organization or the service provider. The procedure involved in change implementation is well-documented. The associated risks are calculated and accounted for, well in advance. The necessary risk mitigation measures are taken as part of the change implementation procedure. Once the change request is received, no additional approval is required from the decision makers or the Change Advisory Board (CAB).

Having an IT service request as a Standard Change has its advantages from an IT Service Management (ITSM) perspective. The change process flows with minimal friction, especially when

information and departmental silos can cause unnecessary delays and limitations in change implementation. Having pre-authorization, documented implementation procedure and extensive risk assessment already in place allows IT to deliver the requested service efficiently and effectively, which is exactly the goal of the ITIL framework associated with change management.

There may be times when the CAB steps in and realizes that items need to be added to or removed from the list of Standard changes that require very little oversight. Generally, a Standard change goes off without a hitch during a scheduled maintenance window and has little, if any, impact on live services. This is in direct contrast to Emergency changes which require direct oversight and careful consideration.

What is an emergency change?

Emergency changes are basically the exact opposite of Standard changes. ITIL defines Emergency Change as:

"A change that must be introduced as soon as possible".

Examples of Emergency Change include:

- Implementing a security patch to a zero-day exploit
- Isolating the network from a large-scale Distributed Denial of Service (DDoS) attack

These changes typically represent a crisis or an opportunity that must be addressed without undue risk. An acceptable level of risk is therefore expected and specific procedures are followed as a risk mitigation strategy. Specific approvals and authorization is also required before implementation of an Emergency Change.

This does not mean lengthy meetings between CAB members, but a high-level oversight over the change management process. The process must follow swift action from all stakeholders at every stage of the change management process. As a result, the Emergency Changes are not thoroughly tested and appropriate decisions are made as a balanced tradeoff between risk and reward.

The agility of the organization determines how well it can manage Emergency Changes. It follows a similar change management process flow as Normal Changes, but at an accelerated timescale according to the ITIL guidelines. Successful handling of an Emergency Change determines the stability of the IT services provided to end-users. Therefore, the impact of an Emergency Change should be documented and evaluated for future improvements in the change management process.

You should also include a remediation or back-out process in the Emergency Change management protocols. This is so you can restore the original state when change implementation activities introduce additional risk and issues.

They don't come at expected times and are anything but run-of-the-mill. Emergency changes are brought about as a response to unforeseen obstacles such as security flaws and exploits. Emergency changes are brought to the immediate attention of a Change Manager and are then sent on to the ECAB for further analysis. It is the duty of the ECAB to assess the risk of the proposed Emergency changes and weigh the danger that the underlying issue poses to the organization and its services.

The ECAB seeks to find a quick but effective remedy to the newly discovered issue and works on a tight deadline that leaves no room for the typical red tape involved in most change operations.

Information must be quickly gathered and analyzed to decide upon the best course of action for remedying the issue at hand. Emergency changes are tested quickly and implemented immediately when necessary. The goal of Emergency changes is to impact live services as little as possible and stop the bleeding as quickly as possible. This leaves little opportunity for standard procedures as out of the box solutions are most often required.

What's left somewhere in the middle of Emergency change and Standard change is Normal change.

Are you ready to meet the next generation of Service Management? ›

What is a normal change?

Most organizations define Normal changes as any change that is NOT an Emergency change or Standard change. Normal changes are not pre-authorized like Standard changes are, but they also don't operate on the stricter timeline and more Wild West nature of Emergency changes that require freedom from red tape and constricting guidelines. Normal changes go through the CAB process for each change that is made.

This allows oversight on the changes and provides the CAB with an opportunity to assess whether this Normal change occurs with enough frequency that it can be given repeatable guidelines which could convert it into a Standard change. Each Normal change is processed as a Request for Change (RFC), which is fed to the CAB and ultimately approved or shot down by the Change Manager.

Normal changes are fairly common but typically require somewhat unique or novel approaches, unlike Standard changes which can generally be accomplished through the use of step by step guides or some basic outlines. Normal changes undergo self review where the team analyzes the change within the scope of the assignment and assesses its viability before they push it through to the CAB. The CAB then goes over the proposed change and ensures it meets compliance and all security protocols before it is finally handed onto the Change Manager for final approval.

ITIL defines Normal Change as:

"A change that is not an emergency change or a standard change. Normal changes follow the defined steps of the change management process".

These are the changes that must be evaluated, authorized and then scheduled according to a standardized process. These changes are anticipated and planned in advance and appropriate standardized change management controls may be devised accordingly. However, the Normal Change is implemented only after formal authorization and approval is received. Low risk changes may require authorization from local IT teams while high risk changes may require approval from the CAB or senior business and IT executives. All activities within the change management process controls are practiced for the Normal Changes.

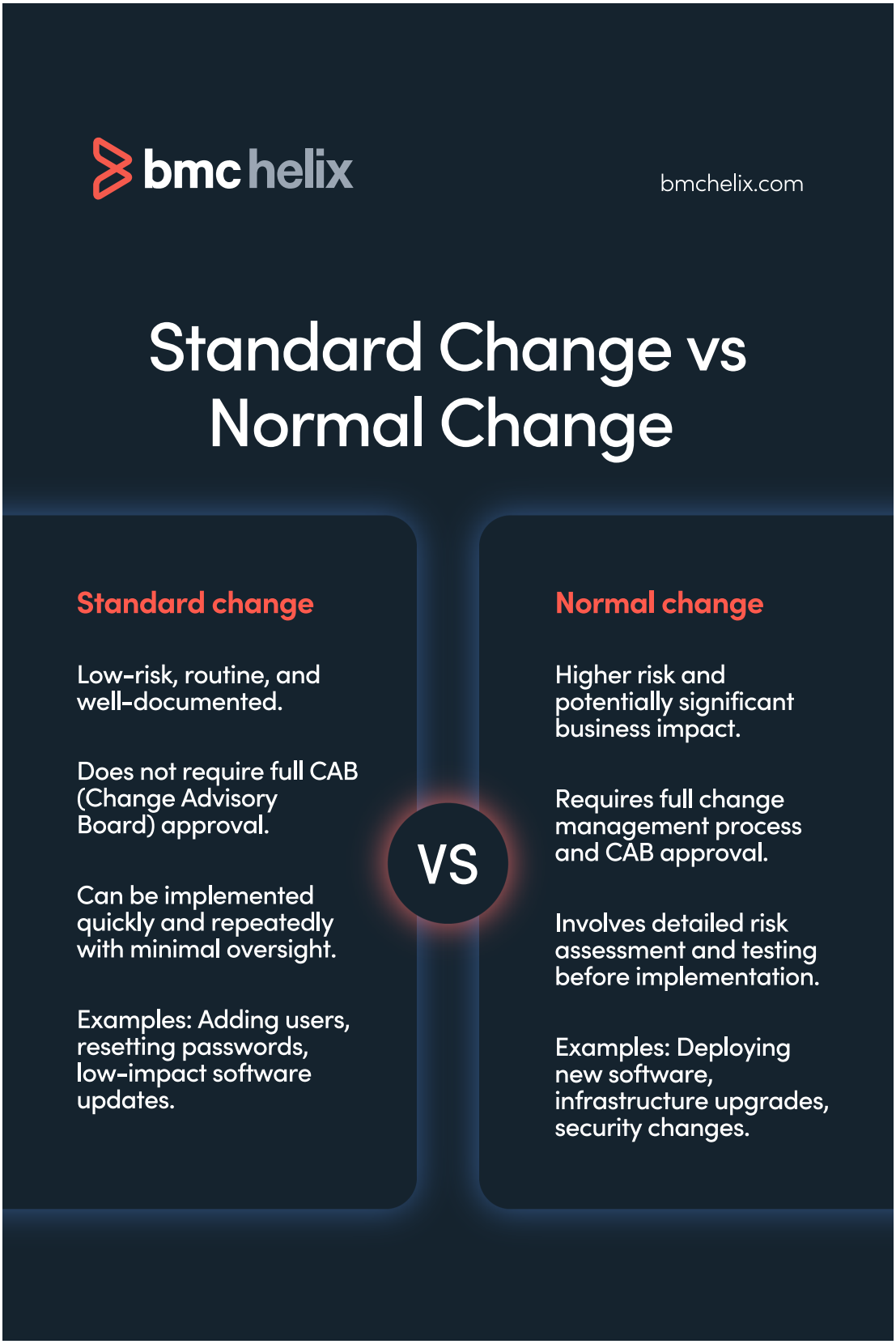
Examples can include migration of critical information resources, applications and workloads from on-premise servers to cloud data centers.

Defining changes as Normal reduces the risk for the organization and IT service providers, since planning for each change ensures that risks are carefully mitigated and change requests produce

desired outcomes. However, implementation of Normal Changes is also a lengthy and time consuming process. In addition to the approval and authorization process, the service provider needs strong visibility and control into the change process, subjected systems and the associated dependencies.

Management and implementation of Normal Changes therefore requires advanced ITSM technologies to carefully analyze, test, manage, and execute the change process and systems. Once the Normal Change is implemented, IT evaluates the implementation success and future requirements of similar changes. Ideally, IT matures its change management process, tooling and capabilities to transform a Normal Change into a Standard Change. This reduces the burden on IT and the service providers to manage changes while also gaining control over the change management process as achieved for Standard Changes.

Standard Change vs. Normal Change



Though wrongly considered synonyms, standard changes and normal changes are not the same thing. They address different risk levels and go through different approval processes, leading to important differences in implementation.

A standard change is one that is routine, well-documented, has little impact and thus is low risk. This kind of change doesn't need to go through a full CAB approval, so it can be quickly implemented. Routine tasks, like adding a new user, resetting passwords, or installing low-impact software updates are examples of changes that fall into the standard category.

A normal change is one that isn't an emergency, but that could potentially have a major impact. These kinds of changes need to go through the full change management process to reduce the risk that something would go wrong. A full risk evaluation is required, along with robust testing. They can't just be automatically implemented like a standard change, but they don't have to be fast-tracked like an emergency change. Examples include deploying new software or making a significant update, changing system infrastructure components, and implementing new security protocols.

The importance of change management

This process of change management helps to increase the success of implementations while reducing risk and minimizing downtime. The different types of change and their categorization aids the smooth operation of the entire change process. Standard changes are made with little to no oversight while Emergency changes require careful management and detailed analysis. Normal changes sit happily in between those two extremes.

The distinction between Standard, Normal, and Emergency Change should be observed from a conceptual perspective, beyond differences in the naming convention. The terms Standard and Normal may appear synonymous but the underlying differences represent the efficacy of change management procedures and controls. It's therefore important to have a strong change enablement practice in discriminating between the three change types through careful assessment of the change requests and incidents leading to a change requirement.

These three types of change help organizations to address issues as they occur while maintaining the constant pace expected of modern DevOps organizations.

Related reading

- BMC Service Management Blog
- Types & Levels of Change Management
- Change Management in the Cloud
- Organizational Change Management (OCM): A Template for Reorganizing IT
- Facilitating Change through Effective Communication