

ITSM simplified: Change enablement



Change enablement

Change is inevitable within an organization. But organizations are often unable to move at the speed of change due to heavyweight, complex, and bureaucratic change processes. This is at odds with customer expectations for rapid new features and quick fixes. However, some oversight is needed to reduce risk, improve stability, and track changes for compliance.

We need to speed up change enablement workflows while keeping a background level of documentation. Service configuration management is here to help!

What is change enablement?

Change enablement - also known as change management or change control - is an IT practice designed to minimize risks and disruptions to IT services while making changes to critical systems. A change is adding, modifying, or removing anything that could have a direct or indirect effect on services.

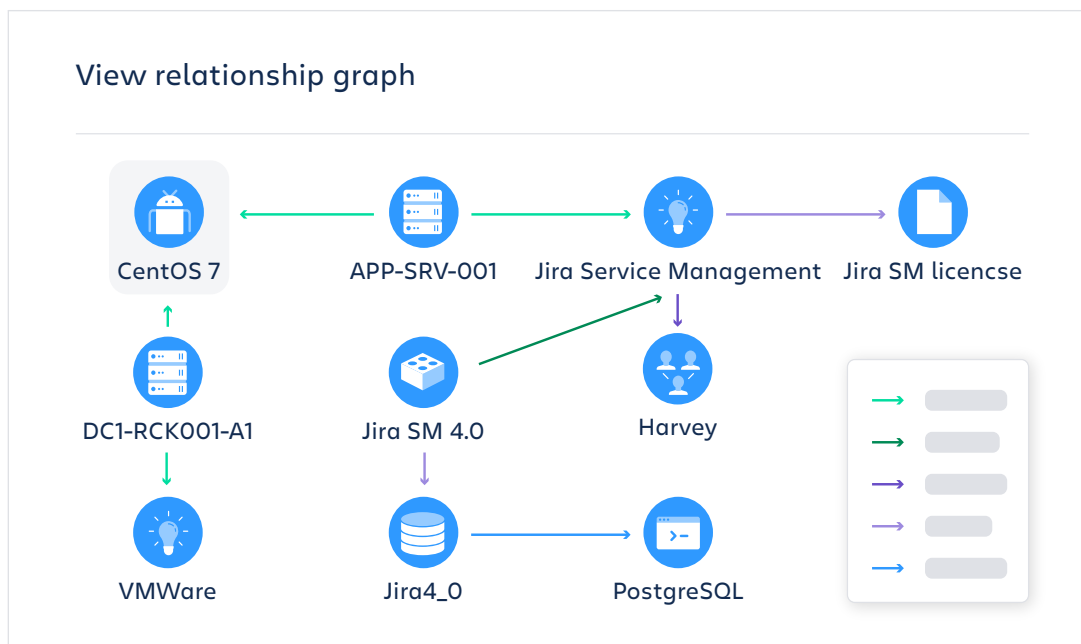
Common types of changes:

- **Standard changes:** pre-approved changes that are low risk, performed frequently, and follow a documented process. For example, adding memory or creating a new instance of a database.
- **Normal changes:** non-emergency changes that require further review and approval by the change advisory board, such as migrating to a new data center or making performance improvements.
- **Emergency changes:** changes that arise from an unexpected error or threat that need to be addressed immediately. Think implementing a security patch or dealing with a service outage.

How does service configuration management speed up change enablement ?

One way to streamline your change practice is to have a way to quickly, but thoroughly, understand the potential risks of a change. A CMDB documenting your services and their dependent CIs will provide this type of valuable insight.

When the CMDB is effectively integrated into your change support practice, the CI (or CIs) that will be changed can be attached to the change request. The change authority can then quickly see which dependencies the CI has and what might be potentially impacted by said change. Once the risks have been identified and assessed, the approval (or not) can be given, and mitigation actions can be implemented to reduce the risks of unplanned downtime.



If your CMDB utilizes discovery tools it can also be used to identify unauthorized changes. These unauthorized changes could have serious consequences for environmental stability and security. But how can we accurately find the cause of an incident if there's a series of changes we don't know about?

Often CMDBs have automations that can trigger an action when a CI is updated. If the network scan result is different to the current CMDB details, then it can trigger an alert for someone to dig into the reason for this undocumented change.



Tips & advice

Having an overview of your services and the infrastructure supporting them is absolutely critical when determining the impact and risk of a change to them. When building a configuration management system to aid change (and incident and problem) management we recommend starting with your services as the top level.

Getting your data into a CMDB can be challenging. It's difficult to know what to include. Sometimes IT organizations try to include too much data and overload the CMDB with bloated information that decreases the value for the support teams that rely on it.

A good practice is to focus on the critical services your teams support. You can take a 'learn as you grow' approach by listing your top services. Mapping out the services, applications and infrastructure that support them takes time.

You can utilize a discovery tools for some of those lower level CIs and many cloud vendors offer integrations

that make it easy to pull in relevant application and infrastructure information for mapping your services.

It's up to you to decide how deep you want, or need, to go per service. Always consider "who needs this information?" as a guiding principle. You also don't need to map all of your services in one go. Start with one or two high value business services or ones that you know have a lot of downtime. Then you can expand overtime to incorporate other services.

Another piece of advice we can share is that when you're building out the relationships between your configuration items, make sure you label what that relationship is in as much detail as you can. A relationship between two CIs could mean "installed on", "owned by", "receives data from", or any number of other things. Being able to see a link between two CIs and quickly understand what that link means is incredibly useful.

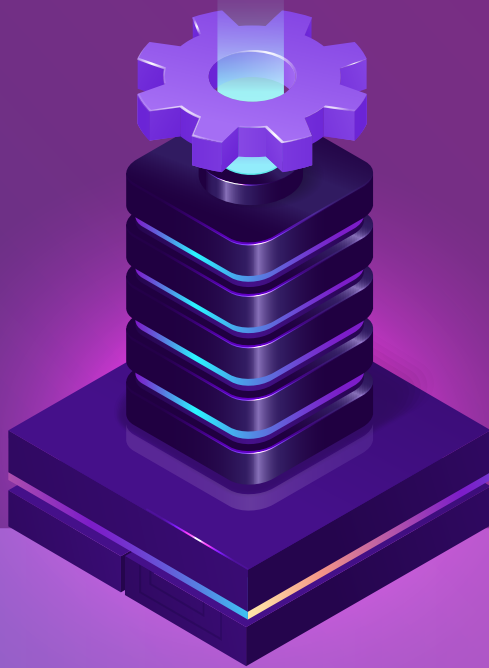
But there's a few more ways you can utilize your CMDB to help you with changes.

You can create a list of types of changes such as "install software patch", "upgrade OS", and "replace hardware" that are added as CIs to your CMDB.

This helps in two ways:

1. It means people can select both the actual CI to be changed and the type of change that they want to make to it. Based on the inputs, automation rules can be used to decide what type of change it is. If it's a standard one it can be auto-approved, if it's a normal or emergency change it can be forwarded to the correct approval group.
2. Having the types of changes as CIs themselves gives you an extra dimension for reporting. If you see that certain types of changes are causing issues then these could be upgraded from standard changes to normal changes to get an approval.

Another way we see organizations setting up their CMDBs to optimize for change management is by setting their change authorities or change advisory boards (CABs) as CIs themselves. These CAB group CIs can also be linked with the various hosts, services, software etc that might need to change. So then if a normal change request comes in, you can automatically route it to the correct people.



Ready to boost your ITSM practices?

Get in touch with TT PSC Atlassian Platinum Solution Partner to learn more. We can set up a custom solution and demo.

We provide a full range of services related to Jira and other Atlassian tools: from business analysis, to advanced customization, implementation and maintenance.

We also handle full support of license agreements (renewal, extension, change to server or cloud version, etc.) for Atlassian products and all applications from the Atlassian Marketplace.

TT PSC

📍 Poland, USA, Germany, Denmark, Taiwan

📧 atlassian@ttpsc.pl

📞 +48 607 300 279

@ <https://ttpsc.com/en/atlassian/>



**Platinum
Solution Partner**
ENTERPRISE



TRANSITION
TECHNOLOGIES