IT change management

Process Definition Document (PDD): template and worked example

Example company (fictional): Marlowe Brandt Energie GmbH, a regional energy supplier in Münster, Germany (about 1,200 employees and 90 business applications).

Document control

Field	Value
Process name	IT change management
Process owner	[Name, role]
Prepared by	[Name]
Reviewed by	[Names of the people who do the work]
Approved by	[Name, date]
Version	1.0 (as-is)
Status	Draft

How to use this template

This is a complete process definition document (PDD) for IT change management, also called the change enablement process, request for change (RFC) procedure or change advisory board (CAB) process. It describes how a change to production systems is requested, classified as standard, normal or emergency, assessed for risk and impact, approved, scheduled in a change window, implemented, backed out if it fails, reviewed and closed. The organisation is a fictional energy supplier, so the roles, systems and numbers are realistic but invented.

Use it as a starting point. Replace the company details, keep the sections, and walk through each step with the people who raise, approve and implement changes. Most teams change the classification rules, the risk scoring, the CAB membership and the change windows. If you do not run a CAB, replace step 9 with the approval route you do use. The process follows the shape of the change enablement practice in ITIL, but this is not a claim of ITIL certification or of compliance with any standard, and it must be adapted to your own risk rules.

- Replace the company, the ITSM tool, the pipeline and the calendar with yours. If you do not use ServiceNow, name the form or register where each step happens.
- Define your own classification rules in step 2. The hardest part is deciding which repeatable changes are standard, and that list should come from the last year of changes.
- Set the CAB membership and meeting frequency to match your volume. Teams with fewer than 20 changes a month often meet once a week or approve by email.
- Write down the risk scoring so two reviewers give the same answer for the same change.
- Agree the change windows with the business and publish them. Add the freeze periods that matter in your calendar.
- If your developers deploy many times a day, move low-risk deployments to a standard change template with pipeline checks, and keep the CAB for the rest.
- Check the percentages against a year of change records. The emergency share and the backout rate are the numbers most worth knowing.

1. Purpose and scope

This procedure describes how Marlowe Brandt Energie introduces changes to production IT systems with a known level of risk. It gives requesters, reviewers, service owners, the change advisory board and implementers one shared

description of who approves what, when changes may be made and what happens when a change fails, so that every production change is recorded, assessed, approved before it starts and checked afterwards.

In scope

- Changes to production applications, infrastructure, network and cloud configuration
- Classification as standard, normal or emergency
- Risk and impact assessment, test evidence and backout planning
- CAB review for normal changes and emergency approval for urgent ones
- Scheduling against the change calendar and the agreed change windows
- Implementation, backout, post-implementation review and closure

Out of scope

- Changes to non-production development and test environments, which follow team rules
- Operational technical tasks that are pre-authorised service requests, such as creating a user account
- Software release planning inside the development teams, up to the point of the production deployment
- Changes to operational technology in power plants and substations, which have their own safety process

2. Process at a glance

Item	Description
Trigger	Someone needs to add, modify or remove something in a production IT service.
Starts when	The requester submits a request for change in ServiceNow.
Ends when	The change manager closes the change after implementation and the post-implementation review.
Inputs	Request for change with reason and affected services, Test results and implementation plan, Backout plan, Change calendar and freeze periods, Configuration management database (CMDB) records
Outputs	Approved or rejected change record, Risk and impact assessment, Scheduled change window entry, Implementation and test evidence, Post-implementation review and closed change
Volume	About 780 changes a year: roughly 55% standard, 42% normal and 3% emergency
Working hours	Requests accepted at any time. CAB meets Tuesday and Thursday at 10:00. Standard change window is Tuesday and Thursday 19:00 to 23:00, and a major window is the first Sunday of each month 02:00 to 08:00.

3. Roles and responsibilities

Role	Responsibilities
Requester	The engineer, developer or business owner who needs the change. Describes it, prepares the plans, attends the CAB when asked and confirms the result afterwards.
Change Manager	Owns the process. Screens each request, classifies it, runs the CAB, maintains the change calendar, authorises standard changes and checks the evidence before closure.
Technical Reviewer	A senior engineer from the affected area who checks that the plan is technically sound, estimates the impact and flags the systems that depend on the change.
Service Owner	The business owner of the affected service. Accepts the downtime and the timing, and signs off that the service is working after the change.
Change Advisory Board	A standing group of the change manager, the technical leads, a security representative, the service desk lead and service owners as needed. Reviews normal changes and advises on approval, timing and risk.
IT Director	Approves emergency changes when the CAB cannot meet, and decides on any change the CAB cannot agree on.
Implementation Engineer	Carries out the change in the window, follows the plan, runs the checks, decides with the

Role	Responsibilities
	requester when to back out and updates the CMDB.

4. Systems

- ServiceNow: change records, approvals, the change calendar and the CMDB
- Jira: development tickets and release notes linked to the change
- Microsoft Teams: CAB meeting, the emergency bridge and window communication
- Azure DevOps: deployment pipelines and test results attached as evidence
- Atlassian Statuspage: internal notice of planned downtime
- Excel: monthly change report with success rate and emergency share

5. Process map

Process diagram goes here

Draw one lane per role from section 3, the steps from section 6 in order, and a diamond for each decision in section 7.

6. Procedure, step by step

#	Step	Who	What happens	System	Output
1	Raise the request for change	Requester	Describes what will change, why, which services are affected, the planned start and end, the test evidence and the backout plan. Using the ServiceNow template takes 20 to 40 minutes for a normal change and 5 minutes for a standard change.	ServiceNow	Draft request for change
2	Screen and classify	Change Manager	Checks the request within one working day for completeness and classifies it as standard (pre-approved, repeatable, low risk), normal (needs assessment and CAB) or emergency (needed now to fix or prevent a serious outage). About 12% of requests are returned for missing detail.	ServiceNow	Classified change, or request returned
3	Authorise a standard change	Change Manager	For a change that matches an approved standard template, such as a certificate renewal or a scheduled patch, confirms the match and authorises it without a CAB. This takes about 5 minutes. The templates are reviewed by the CAB every six months.	ServiceNow	Authorised standard change
4	Approve an	IT Director	For an emergency (3% of changes), the	ServiceNow,	Emergency

#	Step	Who	What happens	System	Output
	emergency change		change manager or the on-call lead phones the IT Director, who approves by ServiceNow or by email on the bridge. The assessment is shortened to risk, plan and backout. Paperwork is completed within 2 working days.	Microsoft Teams	approval
5	Assess risk and impact	Technical Reviewer	Reviews the plan, checks the dependent services in the CMDB, and records the likelihood of failure, the effect of failure and the effort. Typical assessment is 30 to 60 minutes and the wait is 1 to 2 working days. About 15% of changes are sent back for a better plan.	ServiceNow, CMDB	Risk and impact assessment
6	Complete the test and backout plans	Requester	Attaches test results from a non-production environment, the step-by-step implementation plan, the time needed and the backout plan, including how long backout takes and what data would be lost. A change without a tested backout plan is not scheduled.	ServiceNow, Azure DevOps	Complete plan with evidence
7	Confirm business impact and timing	Service Owner	Accepts or rejects the expected downtime and the proposed window. Checks the change against business peaks, such as month-end billing and the winter tariff change. About 10% of normal changes are moved to a different window at this step.	ServiceNow	Business impact confirmed, window agreed
8	Score the risk and prepare the CAB	Change Manager	Combines the assessment into a risk score of low, medium or high and adds the change to the next CAB agenda. High-risk changes are scheduled to the monthly major window. The agenda goes out one working day before the meeting.	ServiceNow	Risk score and CAB agenda
9	Review at the CAB	Change Advisory Board	Meets twice a week for 45 minutes, goes through each change on the agenda, asks the requester questions and records one of four outcomes: approved, approved with conditions, deferred or rejected. About 80% of changes are approved, 8% with conditions, 9% deferred and 3% rejected.	Microsoft Teams, ServiceNow	CAB decision recorded
10	Schedule in a change window	Change Manager	Places the approved change in a window, checks for conflicts with other changes to the same services and for freeze periods, and notifies the service desk so that incidents in the window are linked to the change. Conflicts occur for about 7% of changes.	ServiceNow change calendar	Scheduled change with start and end time
11	Run pre-checks and decide go or no-go	Implementation Engineer	Before the window, confirms the prerequisites: a current backup, access, the right people on call and no open major incident on the same service. About 5% of changes are postponed at this point and returned to the scheduling step.	ServiceNow, Microsoft Teams	Go or no-go decision
12	Implement the change	Implementation Engineer	Follows the implementation plan in the window, records the start time and each completed step in the change record, and posts progress on the Teams channel. Most changes take 30 minutes to 3 hours.	Azure DevOps, ServiceNow	Implemented change with step log
13	Test, or back	Implementatio	Runs the agreed checks. If a check fails and	ServiceNow	Test results, or

#	Step	Who	What happens	System	Output
	out	n Engineer	the problem cannot be fixed within the time reserved, carries out the backout plan and records why (about 4% of changes). A failed change is rescheduled as a new change after a review.		backout record
14	Confirm the result with the service owner	Requester	Asks the service owner or a named user to confirm that the service works. For changes made at night the confirmation is done by 09:00 the next working day. Problems found here are raised as incidents linked to the change.	ServiceNow, Microsoft Teams	Confirmed result
15	Hold the post-implementation review	Change Manager	Reviews every emergency, every failed or backed-out change and a sample of 10% of the others, within 5 working days. Records whether the plan was accurate, whether the timing was right and what should change in the template or the rules.	ServiceNow	Post-implementation review
16	Update the CMDB and documentation	Implementatio n Engineer	Updates the configuration item records, version numbers and architecture notes that the change affected. This takes 10 to 20 minutes and is the step most often skipped.	ServiceNow CMDB	Updated CMDB records
17	Close the change	Change Manager	Checks that the implementation record, test evidence, confirmation and CMDB update are present, then sets the close code: successful, successful with issues, backed out or failed. Incomplete changes go back to the requester.	ServiceNow	Closed change with a close code

7. Decision points and business rules

- Is the request complete? No (about 12%): return it to the requester (step 2).
- Is it standard, normal or emergency? Standard matches an approved template and skips the CAB, emergency needs the IT Director, normal goes through assessment and the CAB (steps 2 to 4).
- Is the plan technically sound? No (about 15%): the reviewer sends it back for a better plan (step 5).
- Is there a tested backout plan? No: the change is not scheduled (step 6).
- Does the service owner accept the downtime and timing? No (about 10%): move to another window (step 7).
- Is the risk high? Yes: schedule in the monthly major window (step 8).
- What does the CAB decide? Approved, approved with conditions, deferred or rejected (step 9).
- Does the change conflict with another change or a freeze period? Yes (about 7%): reschedule (step 10).
- Do the go checks pass? No (about 5%): postpone (step 11).
- Did the tests pass in the window? No (about 4%): back out and review before trying again (step 13).

8. Exceptions

- A normal change cannot wait for the next CAB (about 6%): the change manager asks for approval by email from three CAB members and the decision is noted at the next meeting.
- A standard change no longer matches its template (about 3%): it is reclassified as normal and goes to assessment.
- A change overruns its window (about 5%): the engineer asks the service owner for an extension, or backs out at the latest time stated in the plan.

- A change is found in production that was never recorded (about 1%): the change manager records it retrospectively, raises it with the line manager and reviews how it happened.
- A freeze period such as year-end billing applies: only emergency changes and changes approved by the IT Director are allowed.

9. Controls

- No change is implemented before approval, except under the emergency route, which is reviewed in step 15.
- The requester cannot approve their own change and cannot be the technical reviewer of it.
- Every normal change has a tested backout plan before scheduling.
- Standard change templates are reviewed every six months by the CAB and withdrawn if they have caused incidents.
- Deployments to production use the pipeline, which links each deployment to an approved change number.
- Emergency changes are limited to 5% of the monthly total. The change manager reports the share to the IT Director each month.

10. Known issues today

- Requesters raise changes the day before and expect approval, so the CAB spends time on late items.
- Backout plans say 'restore from backup' without a time estimate or a test.
- The CMDB is out of date, so reviewers cannot see which services depend on the system being changed.
- Two teams change the same platform in the same window because the calendar is not checked.
- Emergency changes are used to skip the CAB when the real problem is poor planning.
- Post-implementation reviews are skipped for changes that succeeded, so template problems stay hidden.

11. RACI matrix

R = responsible (does the work), A = accountable (owns the outcome), C = consulted, I = informed.

Activity	Requester	Change Manager	Technical Reviewer	Service Owner	CAB	IT Director	Implementer
Raise the request	A/R	I					
Classify the change	C	A/R				I	
Assess risk and impact	C	A	R	C			
Confirm business impact and timing	C	I		A/R			
Review and approve a normal change	C	R	C	C	A	I	
Approve an emergency change	C	R	C	C	I	A	I
Schedule the change	C	A/R		C			I
Implement and test	C	I					A/R
Confirm the result	R	I		A			C
Review and close	C	A/R	C	I	I		C

12. KPIs

KPI	Definition	Target
Change success rate	Share of changes closed as successful, split by standard, normal and emergency. Today about 94% overall.	[set]
Emergency change share	Emergency changes as a share of all changes in the month. The limit is 5%.	[set]
Changes causing incidents	Number of incidents linked to a change in the 24 hours after	[set]

KPI	Definition	Target
	implementation.	
Backout rate	Share of implemented changes that were backed out. Today about 4%.	[set]
Days from submission to approval	Average calendar days for normal changes between submission and the CAB decision.	[set]
Unauthorised changes found	Number of production changes found with no change record. The target is zero.	[set]

13. Revision history

Version	Date	Author	Change
1.0	[date]	[name]	First as-is version

Free template from processfix.ai. You may copy and adapt it. The company in the example is fictional.