

13.1 Ziele und Grundlagen des Change Enablement

“ Kurz erklärt

Änderungen an IT-Systemen gehören zum Alltag jeder Organisation.

Neue Software wird installiert, Server aktualisiert, Sicherheitslücken geschlossen oder Cloud-Dienste erweitert.

Ziel des **Change Enablement** ist es, diese Änderungen kontrolliert, nachvollziehbar und mit möglichst geringem Risiko umzusetzen.

Dabei sollen notwendige Veränderungen ermöglicht werden, ohne die Stabilität der IT-Services unnötig zu gefährden.

Was ist Change Enablement?

Change Enablement ist eine ITIL Practice zur Steuerung und Unterstützung von Änderungen an Services und Configuration Items.

Sie sorgt dafür,

dass Änderungen:

- geplant,
- bewertet,
- genehmigt,
- umgesetzt,
- überprüft

und dokumentiert werden.

Warum heißt es nicht mehr Change Management?

Frühere ITIL-Versionen verwendeten den Begriff:

“ Change Management

Seit ITIL 4 lautet die offizielle Bezeichnung:

“ Change Enablement

Der neue Name verdeutlicht,
dass Änderungen nicht verhindert,
sondern sicher und effizient ermöglicht werden sollen.

Warum Änderungen notwendig sind

Ohne Änderungen wäre eine moderne IT nicht dauerhaft funktionsfähig.

Typische Gründe:

- Sicherheitsupdates,
- neue Hardware,
- neue Software,
- gesetzliche Anforderungen,
- Fehlerbehebungen,
- Leistungsverbesserungen,
- Cloud-Migrationen,
- neue Geschäftsanforderungen.

Veränderungen gehören zum normalen IT-Betrieb.

Ziele des Change Enablement

Die wichtigsten Ziele sind:

- Risiken reduzieren,
 - erfolgreiche Änderungen ermöglichen,
 - Serviceunterbrechungen vermeiden,
 - Auswirkungen bewerten,
 - Verantwortlichkeiten festlegen,
 - Änderungen dokumentieren,
 - Zusammenarbeit verbessern,
 - kontinuierliche Verbesserungen unterstützen.
-

Was ist ein Change?

Ein Change ist jede geplante Änderung,

die Auswirkungen auf Services oder Configuration Items haben kann.

Beispiele:

- Betriebssystem aktualisieren,
- Firewallregel ändern,
- Benutzerverwaltung erweitern,
- Zertifikat erneuern,
- Server austauschen,
- Netzwerk erweitern,
- Cloud-Service aktivieren,
- Software installieren.

Nicht jede technische Tätigkeit ist automatisch ein Change.

Change ist nicht gleich Incident

Diese Begriffe werden häufig verwechselt.

Incident	Change
ungeplante Störung	geplante Änderung
Ziel: Service wiederherstellen	Ziel: Service verbessern oder anpassen
häufig Zeitdruck	normalerweise geplant
reaktive Tätigkeit	proaktive Tätigkeit

Ein Incident kann später einen Change erforderlich machen.

Beispiel

Ein Server fällt regelmäßig aus.

Incident Management stellt den Betrieb mehrfach wieder her.

Problem Management findet die Ursache.

Zur dauerhaften Lösung wird:

- zusätzlicher Arbeitsspeicher eingebaut.

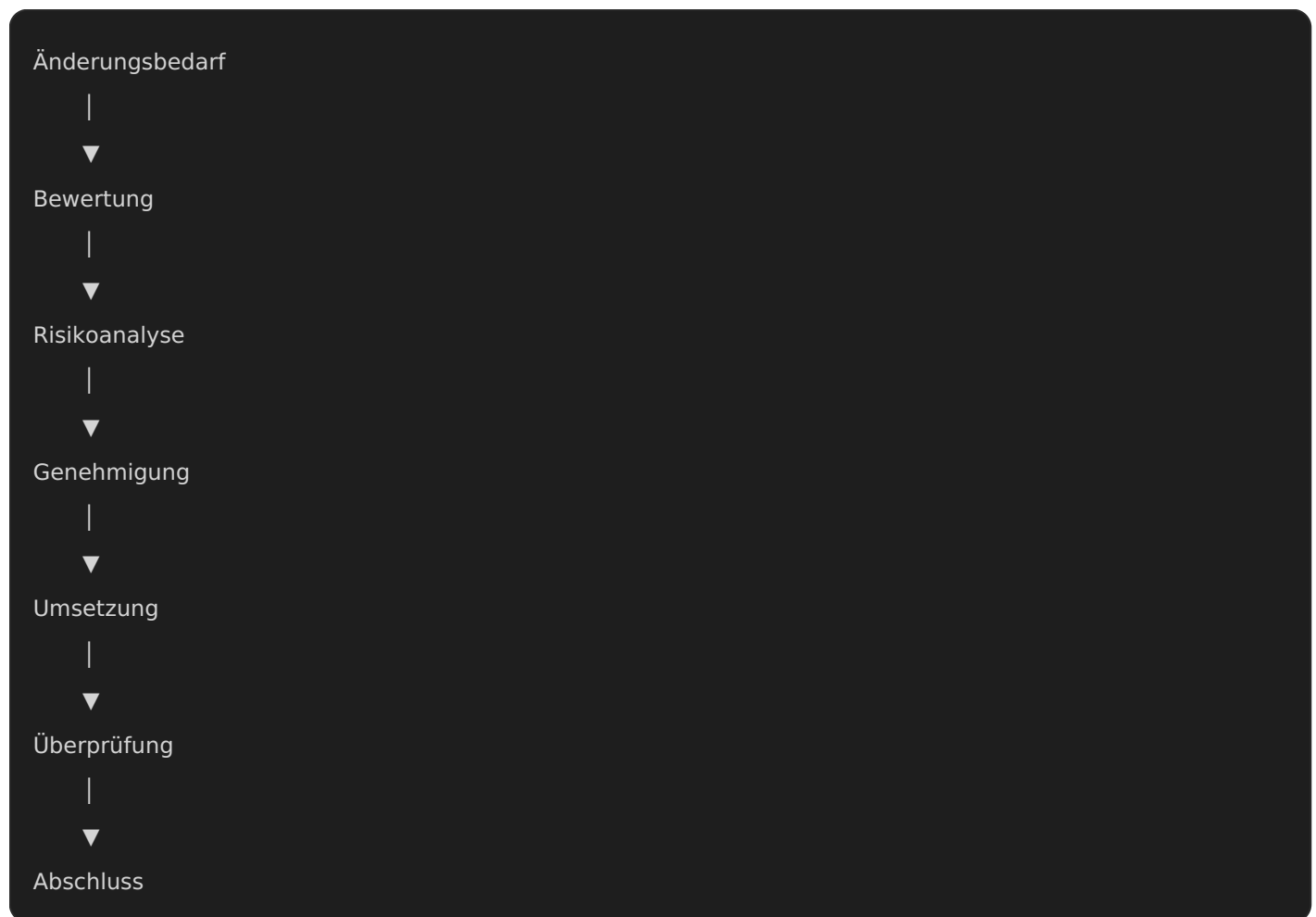
Diese geplante Änderung ist ein Change.

Grundprinzip des Change Enablement

Jede Änderung sollte beantwortete Fragen besitzen:

- Warum ist die Änderung notwendig?
 - Welche Systeme sind betroffen?
 - Welche Risiken bestehen?
 - Wer genehmigt die Änderung?
 - Wann wird sie durchgeführt?
 - Wie wird sie getestet?
 - Wie erfolgt ein Rollback?
 - Wer informiert die Benutzer?
-

Typischer Ablauf



Nicht jeder Change durchläuft alle Schritte mit demselben Aufwand.

Warum Risiken bewertet werden

Jede Änderung kann unbeabsichtigte Auswirkungen haben.

Beispiele:

- Server startet nicht mehr,
- Anwendung funktioniert nicht,
- Netzwerkverbindung fällt aus,
- Benutzer können sich nicht anmelden,
- Daten gehen verloren.

Deshalb bewertet Change Enablement Risiken bereits vor der Umsetzung.

Nutzen strukturierter Changes

Ein geregelter Change-Prozess sorgt unter anderem für:

- weniger Ausfälle,
- bessere Planbarkeit,
- höhere Servicequalität,
- nachvollziehbare Entscheidungen,
- geringere Risiken,
- bessere Dokumentation.

Dadurch steigt die Stabilität der IT.

Nicht jede Änderung ist gleich kritisch

Beispiele:

Geringes Risiko:

- Druckertreiber aktualisieren.

Hohes Risiko:

- Active Directory migrieren.

Je größer die Auswirkungen,

desto sorgfältiger erfolgt Planung und Bewertung.

Verantwortlichkeiten

An einem Change können verschiedene Rollen beteiligt sein.

Beispiele:

- Antragsteller,
- Change Manager,

- technische Spezialisten,
- Service Owner,
- Information Security,
- Management.

Nicht jede Organisation verwendet alle Rollen.

Dokumentation

Jeder Change sollte nachvollziehbar dokumentiert werden.

Typische Inhalte:

- Ziel,
- Umfang,
- Zeitpunkt,
- Verantwortliche,
- Risiko,
- Genehmigung,
- Testergebnisse,
- Rollback,
- Abschlussbewertung.

Eine gute Dokumentation erleichtert spätere Analysen.

Praxisbeispiel

Ein Unternehmen möchte den VPN-Server aktualisieren.

Vor der Umsetzung werden:

- Risiken bewertet,
- Wartungsfenster festgelegt,
- Benutzer informiert,
- Backup erstellt,
- Rollback vorbereitet.

Nach erfolgreicher Aktualisierung bestätigt das Monitoring,

dass der Service wieder ordnungsgemäß funktioniert.

Typische Fehler

Fehler 1

Änderungen erfolgen ohne Planung.

Fehler 2

Risiken werden nicht bewertet.

Fehler 3

Es existiert kein Rollback.

Fehler 4

Benutzer werden nicht informiert.

Fehler 5

Änderungen werden nicht dokumentiert.

Fehler 6

Monitoring prüft das Ergebnis nicht.

Fehler 7

Configuration-Daten werden nicht aktualisiert.

Fehler 8

Changes werden direkt in der Produktion getestet.

Checkliste Change Enablement

- ☐ Ziel definiert
- ☐ Auswirkungen bewertet
- ☐ Risiken analysiert
- ☐ Genehmigung vorhanden
- ☐ Wartungsfenster geplant
- ☐ Rollback vorbereitet
- ☐ Monitoring berücksichtigt

Bedeutung für Fachinformatiker für Systemintegration

Fachinformatiker setzen täglich Changes um.

Typische Aufgaben:

- Updates installieren,
- Server migrieren,
- Netzwerkänderungen durchführen,
- Firewallregeln anpassen,
- Dokumentationen aktualisieren,
- Monitoring prüfen,
- Rollback vorbereiten.

Ein strukturierter Change-Prozess reduziert Ausfälle und erhöht die Stabilität der IT.

Zusammenfassung

“ Änderungsbedarf erkennen

↓

Risiken bewerten

↓

Genehmigung einholen

↓

Änderung umsetzen

↓

Ergebnis überprüfen

↓

Dokumentieren und abschließen

Merksätze

Change Enablement ermöglicht Veränderungen – es verhindert sie nicht.

“Jede Änderung sollte geplant und bewertet werden.

“Je höher das Risiko, desto sorgfältiger die Vorbereitung.

“Ein Rollback gehört zu jeder kritischen Änderung.

“Gute Dokumentation unterstützt zukünftige Changes.

Verwandte Seiten

- 13.2 Change-Typen und Risikobewertung
- 13.3 Genehmigungen, CAB und Change-Kalender
- 13.4 Umsetzung, Tests und Rollback
- 13.5 Zusammenspiel mit Incident, Problem, Service Configuration Management und Monitoring
- Incident Management
- Problem Management
- Service Configuration Management
- Monitoring and Event Management

Quellen und Versionsstand

Offizielle Grundlagen

- PeopleCert – ITIL Practice Guide: Change Enablement
- ITIL Foundation – Version 5

Einordnung

Die dargestellten Grundlagen orientieren sich an der ITIL Practice „Change Enablement“. ITIL definiert Grundprinzipien für die kontrollierte Durchführung von Änderungen, schreibt jedoch keinen starren Prozess vor. Die konkrete Umsetzung richtet sich nach Größe, Risiken und Anforderungen der jeweiligen Organisation.

Behandelter Framework-Stand: ITIL Version 5

Zusätzlich berücksichtigt: aktuelle ITIL-4-Practice-Guidance

Fachlicher Stand: August 2026
