

13.5 Zusammenspiel mit Incident, Problem, Service Configuration Management und Monitoring

“ Kurz erklärt

Change Enablement arbeitet eng mit vielen anderen ITIL Practices zusammen.

Änderungen entstehen häufig aus Incidents oder Problems, beeinflussen Configuration Items und werden durch Monitoring überwacht.

Erst das Zusammenspiel dieser Practices ermöglicht sichere Änderungen, stabile IT-Services und eine kontinuierliche Verbesserung der gesamten IT-Landschaft.

Warum das Zusammenspiel wichtig ist

Ein Change wird selten isoliert durchgeführt.

Vor einer Änderung müssen beispielsweise folgende Fragen beantwortet werden:

- Warum ist die Änderung notwendig?
- Welche Services sind betroffen?
- Welche Configuration Items werden verändert?
- Welche Risiken bestehen?
- Wie wird der Erfolg überprüft?

Diese Informationen stammen aus verschiedenen ITIL Practices.

Zusammenspiel der Practices

Incident



Problem



Change Enablement





Jede Practice liefert wichtige Informationen für die nächste.

Change Enablement und Incident Management

Viele Changes entstehen als Folge eines Incidents.

Beispiel:

Ein Server fällt regelmäßig aus.

Incident Management stellt den Betrieb zunächst wieder her.

Die eigentliche Ursache bleibt jedoch bestehen.

Zur dauerhaften Lösung wird ein Change geplant.

Incident Management arbeitet also häufig kurzfristig,

während Change Enablement eine nachhaltige Verbesserung ermöglicht.

Beispiel





Change Enablement

Der Incident endet mit der Wiederherstellung,
der Change beseitigt anschließend die eigentliche Ursache.

Change Enablement und Problem Management

Problem Management untersucht,
warum Incidents wiederholt auftreten.
Wird eine dauerhafte Lösung gefunden,
führt diese häufig zu einem Change.

Beispiele:

- Software aktualisieren,
- Hardware austauschen,
- Netzwerk erweitern,
- Architektur ändern.

Problem Management liefert also häufig den Anlass für einen Change.

Known Errors

Ein Known Error kann eine empfohlene Änderung enthalten.

Beispiel:

Bekannter Fehler:

Firmware-Version 5.2 verursacht Abstürze.

Empfohlene Lösung:

Firmware-Version 5.3 installieren.

Die eigentliche Umsetzung erfolgt anschließend über Change Enablement.

Change Enablement und Service Configuration Management

Vor jeder Änderung muss bekannt sein,
welche Configuration Items betroffen sind.

Die CMDB liefert beispielsweise:

- betroffene Server,
- Anwendungen,
- Datenbanken,
- Netzwerke,
- Verantwortliche,
- Beziehungen.

Dadurch können Auswirkungen besser bewertet werden.

Impact Analysis

Vor einem Change wird häufig geprüft,
welche Services betroffen sind.

Beispiel:

Firewall

```
|
├─ VPN
├─ Internet
├─ VoIP
└─ E-Mail
```

Ein Firmware-Update betrifft somit mehrere Services.

Diese Information stammt aus der CMDB.

CMDB aktualisieren

Nach erfolgreicher Umsetzung werden unter anderem aktualisiert:

- Versionen,
- Status,
- Beziehungen,
- Dokumentationen,
- Verantwortlichkeiten.

Dadurch bleibt die Configuration-Datenbasis aktuell.

Change Enablement und Monitoring

Monitoring überwacht,

ob Änderungen erfolgreich umgesetzt wurden.

Beispiele:

- Server erreichbar,
- CPU normal,
- Speicher ausreichend,
- Netzwerk stabil,
- keine neuen Alarme,
- Services verfügbar.

Monitoring bestätigt somit den Erfolg eines Changes.

Monitoring vor einem Change

Auch vor einer Änderung liefert Monitoring wichtige Informationen.

Beispiele:

- aktuelle Auslastung,
- bekannte Fehler,
- bestehende Alarme,
- Performance,
- Verfügbarkeit.

Diese Informationen unterstützen die Risikobewertung.

Monitoring nach einem Change

Nach der Umsetzung werden häufig überprüft:

- Erreichbarkeit,
- Antwortzeiten,
- Fehlermeldungen,
- Auslastung,
- Benutzeranmeldungen,
- Dienste.

Erst wenn diese Prüfungen erfolgreich sind,

gilt der Change als abgeschlossen.

Change Enablement und Release Management

Ein Release kann mehrere Changes enthalten.

Beispiel:

Ein Software-Release umfasst:

- neue Funktionen,
- Fehlerbehebungen,
- Sicherheitsupdates,
- Konfigurationsänderungen.

Change Enablement bewertet und genehmigt die Änderungen,

Release Management plant und verteilt das Gesamtpaket.

Change Enablement und Deployment Management

Nach der Genehmigung erfolgt häufig die technische Bereitstellung.

Deployment Management übernimmt beispielsweise:

- Software verteilen,
- Container aktualisieren,
- Images bereitstellen,
- Anwendungen installieren.

Change Enablement steuert den organisatorischen Rahmen,

Deployment Management die technische Umsetzung.

Change Enablement und Information Security Management

Viele Changes dienen der Verbesserung der Sicherheit.

Beispiele:

- Sicherheitsupdates,
- Firewallregeln,
- MFA einführen,
- Zertifikate erneuern,
- Verschlüsselung aktivieren.

Dabei müssen Sicherheitsanforderungen und Serviceverfügbarkeit gleichermaßen berücksichtigt werden.

Change Enablement und Continual Improvement

Erfahrungen aus abgeschlossenen Changes fließen in Continual Improvement ein.

Beispiele:

- Planung verbessern,
- Testverfahren erweitern,
- Dokumentation optimieren,
- Genehmigungen vereinfachen,
- Standard Changes definieren.

Dadurch entwickelt sich der Change-Prozess kontinuierlich weiter.

Praxisbeispiel

Ein Unternehmen stellt fest,

dass nach jedem Betriebssystemupdate ähnliche Probleme auftreten.

Problem Management analysiert die Ursache.

Es zeigt sich,

dass wichtige Regressionstests fehlen.

Change Enablement ergänzt daraufhin den Testplan.

Monitoring bestätigt,

dass zukünftige Updates deutlich störungsärmer verlaufen.

Die neue Vorgehensweise wird anschließend als Standardprozess dokumentiert.

Typische Fehler

Fehler 1

Changes werden unabhängig von Incidents geplant.

Fehler 2

Configuration Items werden nicht aktualisiert.

Fehler 3

Monitoring überprüft Änderungen nicht.

Fehler 4

Problem Management wird nicht einbezogen.

Fehler 5

Release und Change werden verwechselt.

Fehler 6

Deployment erfolgt ohne Genehmigung.

Fehler 7

Auswirkungen auf andere Services werden unterschätzt.

Fehler 8

Erfahrungen aus früheren Changes werden nicht genutzt.

Fehler 9

CMDB und Monitoring liefern widersprüchliche Informationen.

Fehler 10

Verbesserungsmaßnahmen werden nicht dokumentiert.

Checkliste Zusammenspiel

- ☐ Incident analysiert
- ☐ Problem bewertet
- ☐ Change genehmigt

- ☐ Configuration Items geprüft
 - ☐ Monitoring vorbereitet
 - ☐ Dokumentation aktualisiert
 - ☐ Erfolg überprüft
 - ☐ Verbesserungen dokumentiert
-

Checkliste erfolgreicher Change

- ☐ Risiko bewertet
 - ☐ Tests erfolgreich
 - ☐ Rollback vorbereitet
 - ☐ Monitoring aktiv
 - ☐ CMDB aktualisiert
 - ☐ Benutzer informiert
 - ☐ Post Implementation Review durchgeführt
 - ☐ Lessons Learned dokumentiert
-

Bedeutung für Fachinformatiker für Systemintegration

Fachinformatiker begleiten nahezu den gesamten Lebenszyklus eines Changes.

Typische Aufgaben:

- Incidents analysieren,
- Ursachen dokumentieren,
- Configuration-Daten pflegen,
- Monitoring überwachen,
- Änderungen durchführen,
- Rollback vorbereiten,
- Dokumentationen aktualisieren,
- Verbesserungen ableiten.

Dadurch leisten sie einen wesentlichen Beitrag zu einem sicheren und stabilen IT-Betrieb.

Zusammenfassung

“ Incident erkennen



Ursache analysieren



Change planen



Auswirkungen bewerten



Änderung umsetzen



Monitoring prüfen



CMDB aktualisieren



Verbesserungen übernehmen

Merksätze

“ Viele Changes entstehen aus Incidents oder Problems.

“ Die CMDB liefert die Grundlage für Impact-Analysen.

“ Monitoring bestätigt den Erfolg eines Changes.

Deployment setzt Änderungen technisch um – Change Enablement steuert sie organisatorisch.

“ Erfahrungen aus abgeschlossenen Changes verbessern zukünftige Änderungen.

Verwandte Seiten

- 13.1 Ziele und Grundlagen des Change Enablement
- 13.2 Change-Typen und Risikobewertung
- 13.3 Genehmigungen, Change Authority, CAB und Change-Kalender
- 13.4 Umsetzung, Tests und Rollback
- Incident Management
- Problem Management
- Service Configuration Management
- Monitoring and Event Management
- Release Management
- Deployment Management
- Continual Improvement

Quellen und Versionsstand

Offizielle Grundlagen

- PeopleCert – ITIL Practice Guide: Change Enablement
- PeopleCert – ITIL Practice Guide: Incident Management
- PeopleCert – ITIL Practice Guide: Problem Management
- PeopleCert – ITIL Practice Guide: Service Configuration Management
- PeopleCert – ITIL Practice Guide: Monitoring and Event Management
- ITIL Foundation – Version 5

Einordnung

Die dargestellten Zusammenhänge entsprechen den Empfehlungen der ITIL-Practices. Change Enablement koordiniert Änderungen organisatorisch und arbeitet dabei eng mit Incident Management, Problem Management, Service Configuration Management, Monitoring sowie weiteren Practices wie Release und Deployment Management zusammen.

Behandelter Framework-Stand: ITIL Version 5

Zusätzlich berücksichtigt: aktuelle ITIL-4-Practice-Guidance

Fachlicher Stand: August 2026
