13.2 Change-Typen und Risikobewertung

> **Kurz erklärt**
>
> Nicht jede Änderung besitzt dasselbe Risiko oder denselben Aufwand.
>
> Deshalb unterscheidet ITIL verschiedene Change-Typen.
>
> Je nach Risiko, Auswirkungen und Dringlichkeit unterscheiden sich Planung, Genehmigung und Durchführung.
>
> Ziel ist es, **einfache Änderungen möglichst effizient und risikoreiche Änderungen besonders sorgfältig umzusetzen.**

Warum verschiedene Change-Typen?

Eine kleine Änderung,

wie das Aktualisieren einer Druckersoftware,

benötigt deutlich weniger Planung als die Migration eines Active Directory.

Würden beide Änderungen denselben Prozess durchlaufen,

wäre der Aufwand unnötig hoch.

Deshalb unterscheidet ITIL verschiedene Change-Typen.

Die drei Change-Typen nach ITIL

ITIL Version 5 unterscheidet grundsätzlich:

Change-Typ	Beschreibung
Standard Change	geringes Risiko, vorab genehmigt
Normal Change	individuelle Bewertung und Genehmigung erforderlich
Emergency Change	schnelle Umsetzung wegen dringender Situation

Diese Einteilung richtet sich nach Risiko und Auswirkungen,

nicht nach der technischen Komplexität.

Standard Change

Ein Standard Change ist:

- bekannt,
- dokumentiert,
- risikoarm,
- getestet,
- bereits genehmigt.

Für jede Durchführung ist normalerweise keine neue Genehmigung erforderlich.

Beispiele für Standard Changes

Mögliche Standard Changes:

- Druckertreiber installieren,
- Benutzerkonto anlegen,
- Standardsoftware installieren,
- Zertifikat erneuern,
- Gruppenmitgliedschaft ändern,
- Standard-Firewallregel aktivieren,
- VM nach Vorlage bereitstellen.

Diese Änderungen folgen meist einem festen Ablauf.

Eigenschaften eines Standard Change

Ein Standard Change besitzt:

- klaren Ablauf,
- bekannte Risiken,
- dokumentierte Arbeitsschritte,
- definierte Verantwortlichkeiten,
- erprobte Durchführung,
- festgelegte Rollback-Möglichkeiten.

Dadurch kann er effizient umgesetzt werden.

Normal Change

Ein Normal Change ist die häufigste Form einer Änderung.

Er wird individuell bewertet.

Dabei werden unter anderem betrachtet:

- Risiken,
- Auswirkungen,
- Aufwand,
- Ressourcen,
- Wartungsfenster,
- Genehmigungen.

Beispiele für Normal Changes

Typische Beispiele:

- Servermigration,
- Firewall-Konfiguration ändern,
- neue Anwendung einführen,
- Datenbank aktualisieren,
- Netzwerk erweitern,
- Active Directory ändern,
- Cluster erweitern.

Diese Änderungen benötigen meist eine individuelle Planung.

Emergency Change

Ein Emergency Change dient dazu,

eine akute Gefahr oder Störung schnell zu beseitigen.

Dabei wird der normale Genehmigungsprozess verkürzt,

nicht jedoch vollständig ausgelassen.

Beispiele für Emergency Changes

Typische Situationen:

- kritische Sicherheitslücke,
- Ransomware-Angriff,
- Zertifikat abgelaufen,
- Produktionssystem ausgefallen,
- kritischer Softwarefehler,
- schwerwiegender Netzwerkausfall.

Hier steht die schnelle Wiederherstellung des Betriebs im Vordergrund.

Emergency bedeutet nicht ungeplant

Auch Emergency Changes sollten soweit möglich:

- dokumentiert,
- bewertet,
- getestet,
- nachbereitet

werden.

Lediglich der Zeitdruck ist deutlich höher.

Vergleich der Change-Typen

Merkmal	Standard	Normal	Emergency
Risiko	gering	unterschiedlich	häufig hoch
Genehmigung	vorab	individuell	beschleunigt
Planung	standardisiert	individuell	verkürzt
Dokumentation	erforderlich	erforderlich	ebenfalls erforderlich

---

Risikobewertung

Vor jeder Änderung sollte bewertet werden,

welche Risiken bestehen.

Typische Fragen:

- Welche Services sind betroffen?
- Welche Benutzer sind betroffen?
- Welche Ausfallzeit entsteht?
- Gibt es Redundanzen?
- Existiert ein Rollback?
- Wurde ausreichend getestet?

Die Risikobewertung unterstützt fundierte Entscheidungen.

Risikofaktoren

Beispiele für Risikofaktoren:

- produktive Systeme,
- geschäftskritische Services,
- viele Benutzer betroffen,
- komplexe Infrastruktur,
- neue Technologien,
- fehlende Erfahrung,
- hoher Zeitdruck,
- externe Abhängigkeiten.

Je mehr Risikofaktoren vorliegen,

desto sorgfältiger sollte geplant werden.

Business Impact

Neben technischen Risiken wird auch der geschäftliche Einfluss bewertet.

Beispiele:

Gering:

- Testsystem.

Mittel:

- internes Intranet.

Hoch:

- ERP-System,
- Produktionssteuerung,
- Online-Shop.

Business Impact und technisches Risiko sind nicht immer identisch.

Wahrscheinlichkeit und Auswirkung

Risiken werden häufig anhand zweier Kriterien bewertet:

- Eintrittswahrscheinlichkeit,
- Auswirkung.

Beispiel:

Wahrscheinlichkeit	Auswirkung	Risiko

gering	gering	niedrig
hoch	gering	mittel
gering	hoch	mittel
hoch	hoch	hoch

Diese Bewertung unterstützt die Entscheidung über notwendige Maßnahmen.

Risikomatrix

Eine vereinfachte Risikomatrix:

```
            Auswirkung
          Niedrig  Mittel  Hoch
Niedrig      □□      □□     □□
Mittel       □□      □□     □□
Hoch         □□      □□     □□
```

Je höher das Risiko,

desto umfangreicher sollten Planung und Genehmigung sein.

Risikominimierung

Risiken lassen sich häufig reduzieren.

Beispiele:

- Tests durchführen,
- Wartungsfenster nutzen,
- Backup erstellen,
- Rollback vorbereiten,
- Pilotbetrieb,
- Redundanzen verwenden,
- Benutzer informieren.

Ziel ist nicht,

jedes Risiko vollständig auszuschließen,

sondern es auf ein akzeptables Maß zu reduzieren.

Rest-Risiko

Auch nach sorgfältiger Planung bleibt häufig ein Restrisiko bestehen.

Beispiel:

Ein Betriebssystem-Update wurde erfolgreich getestet.

Trotzdem kann es in der Produktivumgebung zu unerwarteten Problemen kommen.

Deshalb gehören Rollback und Monitoring zu jeder kritischen Änderung.

Praxisbeispiel

Ein Unternehmen plant ein Firmware-Update für zentrale Switches.

Die Bewertung ergibt:

- hoher Business Impact,
- mittlere Eintrittswahrscheinlichkeit,
- vorhandene Redundanz,
- getesteter Rollback.

Der Change wird als Normal Change durchgeführt.

Das Wartungsfenster wird nachts geplant,

Monitoring überwacht die Umsetzung

und bei Problemen steht ein Rollback bereit.

Typische Fehler

Fehler 1

Alle Änderungen werden gleich behandelt.

Fehler 2

Risiken werden nicht dokumentiert.

Fehler 3

Business Impact wird unterschätzt.

Fehler 4

Emergency Changes werden nicht nachbereitet.

Fehler 5

Standard Changes werden nie überprüft.

Fehler 6

Es existiert kein Rollback.

Fehler 7

Tests fehlen.

Fehler 8

Benutzer werden nicht informiert.

Fehler 9

Monitoring überwacht den Change nicht.

Fehler 10

Risikobewertung erfolgt nur technisch,

nicht geschäftlich.

Checkliste Risikobewertung

- [ ] Change-Typ bestimmt
- [ ] Auswirkungen bewertet
- [ ] Business Impact geprüft
- [ ] Risiken dokumentiert
- [ ] Tests durchgeführt
- [ ] Rollback vorbereitet
- [ ] Wartungsfenster geplant

- [ ] Monitoring berücksichtigt

Checkliste Change-Typen

- [ ] Standard Change geeignet?
- [ ] Normal Change erforderlich?
- [ ] Emergency Change begründet?
- [ ] Genehmigung vorhanden
- [ ] Dokumentation aktuell
- [ ] Verantwortlichkeiten bekannt
- [ ] Nachbereitung geplant

Bedeutung für Fachinformatiker für Systemintegration

Fachinformatiker bewerten und begleiten regelmäßig Änderungen.

Typische Aufgaben:

- Risiken einschätzen,
- Auswirkungen analysieren,
- Tests durchführen,
- Rollback vorbereiten,
- Monitoring überwachen,
- Dokumentationen aktualisieren.

Eine realistische Risikobewertung gehört zu den wichtigsten Voraussetzungen erfolgreicher Changes.

Zusammenfassung

> Änderungsbedarf erkennen
>
> ↓
>
> Change-Typ bestimmen
>
> ↓
>
> Risiken bewerten

> ↓
>
> Business Impact analysieren
>
> ↓
>
> Maßnahmen planen
>
> ↓
>
> Genehmigung vorbereiten

Merksätze

> Nicht jede Änderung benötigt denselben Aufwand.

> Standard Changes sind vorab genehmigt und risikoarm.

> Normal Changes werden individuell bewertet.

> Emergency Changes beschleunigen den Prozess – sie ersetzen ihn nicht.

> Jede Risikobewertung sollte technische und geschäftliche Auswirkungen berücksichtigen.

Verwandte Seiten

- 13.1 Ziele und Grundlagen des Change Enablement
- 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

Quellen und Versionsstand

Offizielle Grundlagen

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

Einordnung

Die dargestellten Change-Typen und Verfahren zur Risikobewertung entsprechen den Empfehlungen der ITIL Practice „Change Enablement“. ITIL schreibt keine feste Risikomatrix oder konkrete Bewertungsmethode vor. Organisationen definieren diese entsprechend ihrer Geschäftsanforderungen und ihrer Risikobereitschaft.

Behandelter Framework-Stand: ITIL Version 5
Zusätzlich berücksichtigt: aktuelle ITIL-4-Practice-Guidance
Fachlicher Stand: August 2026
