5.2 Change-Typen und Risikobewertung

> **Kurz erklärt**
>
> Nicht jede Änderung besitzt dasselbe Risiko.
>
> Change Enablement unterscheidet deshalb verschiedene Change-Typen und bewertet Änderungen nach Risiko, Auswirkung, Dringlichkeit und Standardisierbarkeit.
>
> Ziel ist, einfache und risikoarme Änderungen schnell durchführen zu können, während kritische Änderungen sorgfältig geplant und kontrolliert werden.

Warum Change-Typen wichtig sind

Eine kleine Standardänderung sollte nicht denselben Aufwand verursachen wie eine kritische Produktionsumstellung.

Beispiele:

- Passwort eines Testkontos zurücksetzen,
- Standardsoftware installieren,
- Firewall-Regel in Produktion ändern,
- Datenbankmigration durchführen,
- Sicherheitsupdate wegen aktiver Schwachstelle einspielen,
- zentrale Authentifizierung umstellen.

Diese Änderungen unterscheiden sich stark in:

- Risiko,
- Auswirkung,
- Dringlichkeit,
- Wiederholbarkeit,
- Genehmigungsbedarf,
- Testaufwand,
- Kommunikationsbedarf,
- Rollback-Möglichkeit.

Change-Typen helfen dabei, den passenden Umgang mit einer Änderung festzulegen.

Grundidee der Change-Klassifizierung

Eine Organisation sollte festlegen:

- welche Change-Typen verwendet werden,
- welche Kriterien dafür gelten,
- wer entscheiden darf,
- welche Genehmigung notwendig ist,
- welche Dokumentation erwartet wird,
- welche Tests erforderlich sind,
- wann Kommunikation notwendig ist,
- und wie der Erfolg geprüft wird.

ITIL schreibt keine für alle Organisationen identische Change-Matrix vor.

Die Einteilung muss zur Organisation, zu den Services und zu den Risiken passen.

Typische Change-Typen

Viele Organisationen unterscheiden mindestens:

Change-Typ	Kurzbeschreibung
Standard Change	vorab bewertete, wiederholbare und risikoarme Änderung
Normal Change	Änderung mit individueller Bewertung, Planung und Genehmigung
Emergency Change	dringende Änderung zur Abwehr akuter Schäden oder zur schnellen Wiederherstellung
Major Change	besonders umfangreiche, geschäftskritische oder risikoreiche Änderung
Minor Change	kleine Änderung mit begrenzter Auswirkung
Routine Change	regelmäßig vorkommende Änderung nach definiertem Ablauf

Nicht jede Organisation verwendet alle Begriffe.

Wichtig ist, dass die Begriffe intern eindeutig definiert sind.

Standard Change

Ein Standard Change ist eine Änderung, die bereits vorab geprüft und genehmigt wurde.

Typische Merkmale:

- wiederholt sich häufig,
- besitzt geringes Risiko,

- Ablauf ist dokumentiert,
- Auswirkungen sind bekannt,
- Umsetzung ist standardisiert,
- Genehmigung ist bereits grundsätzlich erteilt,
- Rollen und Schritte sind klar,
- Erfolg ist leicht prüfbar.

Beispiele:

- Standardsoftware aus genehmigtem Katalog installieren,
- Benutzer in eine genehmigte Standardgruppe aufnehmen,
- Standardarbeitsplatz bereitstellen,
- neues Standard-Monitoring für einen Server aktivieren,
- Zertifikat nach geprüftem Runbook erneuern,
- Standarddrucker einrichten.

Ein Standard Change ist nicht ungeprüft.

Er wurde nur bereits vorab bewertet.

Normal Change

Ein Normal Change wird individuell bewertet, geplant und genehmigt.

Typische Merkmale:

- nicht vollständig standardisiert,
- Risiko muss bewertet werden,
- Auswirkungen müssen geprüft werden,
- Genehmigung ist erforderlich,
- Umsetzung muss geplant werden,
- Tests und Rollback müssen betrachtet werden.

Beispiele:

- Update einer produktiven Anwendung,
- Änderung einer Firewall-Regel,
- Datenbankänderung,
- Umstellung eines Servers,
- Anpassung einer Schnittstelle,
- Änderung an einem produktiven Netzwerksegment,
- Einführung eines neuen Tools.

Normal Changes benötigen je nach Risiko unterschiedlich viel Prüfung.

Emergency Change

Ein Emergency Change ist eine dringende Änderung, die wegen eines akuten Risikos oder Schadens schnell durchgeführt werden muss.

Typische Auslöser:

- kritischer Service ist ausgefallen,
- Sicherheitslücke wird aktiv ausgenutzt,
- Datenverlust droht,
- Major Incident benötigt sofortige technische Maßnahme,
- kein sicherer Workaround ist verfügbar,
- dringende Wiederherstellung ist notwendig.

Beispiele:

- kritischen Patch kurzfristig einspielen,
- fehlerhafte Konfiguration sofort zurückrollen,
- abgelaufenes Zertifikat bei Produktionsausfall erneuern,
- kompromittierten Zugang sperren,
- DNS oder Routing kurzfristig korrigieren.

Emergency Changes dürfen nicht als Abkürzung für schlechte Planung genutzt werden.

Auch unter Zeitdruck müssen Maßnahmen nachvollziehbar dokumentiert und nachträglich überprüft werden.

Major Change

Ein Major Change ist eine Änderung mit besonders hoher Auswirkung oder hohem Risiko.

Beispiele:

- neues Rechenzentrum anbinden,
- zentrales Identity-System migrieren,
- ERP-System aktualisieren,
- Netzwerkarchitektur grundlegend ändern,
- neue Cloud-Plattform einführen,
- mehrere Standorte gleichzeitig umstellen,
- kritische Datenbank migrieren.

Typische Merkmale:

- viele Stakeholder betroffen,
- hoher Planungsaufwand,
- mehrere Teams beteiligt,

- umfangreiche Tests notwendig,
- Kommunikationsplan erforderlich,
- Rollback komplex oder nur eingeschränkt möglich,
- Management-Entscheidung notwendig.

Ein Major Change ist nicht automatisch ein Emergency Change.

Er kann lange geplant sein und trotzdem sehr risikoreich sein.

Minor Change

Ein Minor Change ist eine kleinere Änderung mit begrenzter Auswirkung.

Beispiele:

- kleine Konfigurationsanpassung an einem nicht kritischen System,
- Ergänzung einer Monitoringbeschreibung,
- Anpassung eines Formularfelds,
- Änderung eines nicht produktiven Testsystems,
- kleinere Dokumentationsänderung.

Auch kleine Changes können Risiken besitzen.

Beispiel:

Eine scheinbar kleine Firewall-Regel kann große Auswirkungen haben, wenn sie einen kritischen Service betrifft.

Change-Typen im Vergleich

Kriterium	Standard Change	Normal Change	Emergency Change
Risiko	gering und vorab bewertet	individuell zu bewerten	häufig hoch oder zeitkritisch
Dringlichkeit	planbar	planbar	akut
Genehmigung	vorab genehmigt	je nach Risiko erforderlich	beschleunigt oder nachträglich ergänzt
Ablauf	standardisiert	individuell geplant	schnell, aber kontrolliert
Dokumentation	standardisiert	vollständig nach Bedarf	mindestens entscheidungsrelevant
Beispiele	Standardsoftware	produktives Update	kritischer Sicherheitspatch

---

Risikobewertung

Risikobewertung bedeutet, mögliche negative Folgen eines Changes vor der Umsetzung zu betrachten.

Typische Fragen:

- Was kann schiefgehen?
- Welche Services wären betroffen?
- Welche Benutzer oder Kunden wären betroffen?
- Wie wahrscheinlich ist ein Fehler?
- Wie schwer wären die Auswirkungen?
- Wie gut ist der Change getestet?
- Gibt es einen Rollback?
- Gibt es ein Wartungsfenster?
- Gibt es Abhängigkeiten?
- Gibt es Sicherheits- oder Datenschutzrisiken?
- Wer muss informiert werden?

Risiko entsteht aus Wahrscheinlichkeit und Auswirkung.

Auswirkung bewerten

Die Auswirkung beschreibt, wie stark Benutzer, Services oder Geschäftsprozesse betroffen wären.

Zu prüfen ist:

- Ist ein geschäftskritischer Service betroffen?
- Sind interne Benutzer betroffen?
- Sind externe Kunden betroffen?
- Sind mehrere Standorte betroffen?
- Gibt es Auswirkungen auf Produktion, Verkauf, Abrechnung oder Support?
- Können Daten verloren gehen?
- Können Sicherheitsanforderungen verletzt werden?
- Sind gesetzliche oder vertragliche Anforderungen betroffen?
- Gibt es Abhängigkeiten zu anderen Services?

Je größer die mögliche Auswirkung, desto sorgfältiger muss der Change gesteuert werden.

Wahrscheinlichkeit bewerten

Die Wahrscheinlichkeit beschreibt, wie wahrscheinlich ein Fehler bei der Änderung ist.

Einflussfaktoren:

- Komplexität der Änderung,
- Erfahrung des Teams,

- Qualität der Tests,
- Reife des Runbooks,
- Anzahl beteiligter Systeme,
- Anzahl manueller Schritte,
- bekannte Fehler,
- Stabilität der Umgebung,
- Lieferantenabhängigkeit,
- Neuartigkeit der Änderung.

Eine Änderung mit geringer Auswirkung, aber hoher Fehlerwahrscheinlichkeit kann trotzdem relevant sein.

Dringlichkeit bewerten

Nicht jede dringende Änderung ist automatisch ein Emergency Change.

Zu prüfen ist:

- Warum ist die Änderung dringend?
- Gibt es einen akuten Schaden?
- Droht ein Sicherheitsvorfall?
- Läuft eine Frist ab?
- Gibt es einen Workaround?
- Kann die Änderung bis zum nächsten Wartungsfenster warten?
- Wird die Dringlichkeit durch schlechte Planung verursacht?
- Welche Risiken entstehen durch sofortige Umsetzung?

Dringlichkeit darf nicht dazu führen, dass grundlegende Sicherheits- und Dokumentationspflichten ignoriert werden.

Nutzen bewerten

Neben Risiko und Dringlichkeit muss der Nutzen betrachtet werden.

Möglicher Nutzen:

- Incident dauerhaft beheben,
- Sicherheitsrisiko reduzieren,
- Performance verbessern,
- Kosten senken,
- Benutzererfahrung verbessern,
- gesetzliche Anforderungen erfüllen,
- technische Schulden reduzieren,
- Stabilität erhöhen,
- Automatisierung ermöglichen,

- Betrieb vereinfachen.

Ein Change kann sinnvoll sein, obwohl er Risiko besitzt.

Entscheidend ist, ob Nutzen und Risiko bewusst bewertet wurden.

Typische Risikokriterien

Kriterium	Beispiele
Servicekritikalität	produktiv, geschäftskritisch, Testsystem
Benutzerimpact	einzelne Person, Team, Standort, Kunden
Technische Komplexität	einfache Konfiguration, Migration, Architekturänderung
Rollback-Fähigkeit	einfach, schwierig, nicht möglich
Testabdeckung	vollständig getestet, teilweise getestet, nicht getestet
Sicherheitsbezug	Berechtigungen, Firewall, Daten, Logging
Zeitpunkt	Geschäftszeit, Wartungsfenster, Monatsabschluss
Abhängigkeiten	Datenbank, Netzwerk, Identität, Lieferant
Erfahrung	häufig durchgeführt, neu, einmalig
Kommunikationsbedarf	keine Benutzerinfo, interne Info, Kundenkommunikation

---

Einfache Risikomatrix

Eine einfache Matrix kann helfen.

Auswirkung	Wahrscheinlichkeit niedrig	Wahrscheinlichkeit mittel	Wahrscheinlichkeit hoch
hoch	mittel	hoch	sehr hoch
mittel	niedrig	mittel	hoch
niedrig	niedrig	niedrig	mittel

Diese Matrix ist nur ein Beispiel.

Die Organisation muss eigene Bewertungsstufen festlegen.

Beispiel für Change-Risikostufen

Risikostufe	Bedeutung
Niedrig	begrenzte Auswirkung, gut getestet, einfacher Rollback

Risikostufe	Bedeutung
Mittel	mehrere Benutzer oder wichtiger Service betroffen, Rollback möglich
Hoch	kritischer Service, viele Benutzer, komplexe Änderung
Sehr hoch	geschäftskritisch, schwieriger Rollback, erhebliche Sicherheits- oder Datenrisiken

Die Risikostufe beeinflusst:

- Genehmigung,
- Testtiefe,
- Kommunikationsbedarf,
- Wartungsfenster,
- Dokumentationsumfang,
- Beteiligung von Spezialisten,
- Nachprüfung.

Change Authority passend wählen

Die Genehmigungsinstanz sollte zum Risiko passen.

Beispiele:

Change	mögliche Change Authority
Standardsoftware installieren	vorab genehmigter Standardprozess
kleine Konfigurationsänderung	Team Lead oder Service Owner
produktives Anwendungsupdate	Change Manager oder Change Advisory Board
sicherheitskritische Firewall-Regel	Informationssicherheit und Service Owner
Emergency Security Patch	Emergency Change Authority
große Plattformmigration	Management, Service Owner, Change Board

Nicht jede Änderung benötigt ein großes Gremium.

Aber risikoreiche Änderungen brauchen ausreichend Perspektiven.

Wann ein Change Advisory Board sinnvoll ist

Ein Change Advisory Board kann sinnvoll sein, wenn:

- mehrere Services betroffen sind,
- mehrere Teams beteiligt sind,

- hohes Risiko besteht,
- der Rollback schwierig ist,
- Benutzer oder Kunden informiert werden müssen,
- Sicherheitsfragen bestehen,
- Lieferanten beteiligt sind,
- mehrere Changes zeitlich kollidieren,
- oder Managemententscheidungen notwendig sind.

Ein CAB sollte beraten und Risiken sichtbar machen.

Es sollte nicht jede Routineänderung unnötig verzögern.

Emergency Change Authority

Für Emergency Changes kann eine kleinere, schnell erreichbare Entscheidungsgruppe sinnvoll sein.

Mögliche Beteiligte:

- Incident Manager,
- Change Manager,
- Service Owner,
- Informationssicherheit,
- verantwortliches Fachteam,
- Management bei hohem Geschäftsrisiko.

Wichtig ist:

- Entscheidung dokumentieren,
- Risiko akzeptieren oder begründen,
- Umsetzung kontrollieren,
- Ergebnis prüfen,
- nachträgliches Review durchführen.

Standard Change richtig definieren

Ein Standard Change sollte nicht leichtfertig als Standard eingestuft werden.

Vorab zu klären:

- Ist der Ablauf wiederholbar?
- Ist das Risiko niedrig?
- Sind Auswirkungen bekannt?
- Gibt es ein geprüftes Runbook?
- Sind Berechtigungen klar?
- Gibt es definierte Erfolgskriterien?

- Gibt es Abbruchkriterien?
- Wird die Ausführung protokolliert?
- Wird der Standard regelmäßig überprüft?

Wenn ein Standard Change häufig fehlschlägt, muss er neu bewertet werden.

Emergency Change Missbrauch vermeiden

Emergency Changes sollten nicht genutzt werden, nur weil:

- ein Request zu spät gestellt wurde,
- Planung vergessen wurde,
- Genehmigung umgangen werden soll,
- ein Team schneller arbeiten möchte,
- normale Change-Zeiten als störend empfunden werden.

Ungeeignet:

> „Wir machen daraus einen Emergency Change, damit wir keine Freigabe brauchen.

Besser:

> „Es liegt kein akuter Schaden vor. Der Change wird als Normal Change mit beschleunigter Planung behandelt.

Risiko durch Nicht-Handeln

Nicht nur Durchführung kann riskant sein.

Auch Nicht-Handeln kann Risiko erzeugen.

Beispiele:

- Sicherheitslücke bleibt offen,
- Zertifikat läuft bald ab,
- Speicher läuft voll,
- instabile Version bleibt produktiv,
- gesetzliche Frist wird verpasst,
- Workaround belastet Betrieb dauerhaft,
- bekannte Fehler erzeugen weitere Incidents.

Eine gute Bewertung betrachtet deshalb:

- Risiko des Changes,
- Risiko des Nicht-Handelns,
- Risiko einer Verzögerung,
- Risiko des Workarounds.

Rollback und Backout in der Risikobewertung

Ein Change ist weniger riskant, wenn ein zuverlässiger Rollback möglich ist.

Zu prüfen ist:

- Kann die Änderung vollständig zurückgenommen werden?
- Wie lange dauert der Rollback?
- Sind Backups vorhanden?
- Wurden Konfigurationen gesichert?
- Werden Daten verändert?
- Gibt es Abhängigkeiten?
- Wer entscheidet über Abbruch?
- Wann ist der späteste sichere Abbruchzeitpunkt?

Wenn kein Rollback möglich ist, muss besonders sorgfältig getestet und kommuniziert werden.

Testumfang nach Risiko

Der Testumfang sollte zur Risikostufe passen.

Risiko	möglicher Testumfang
niedrig	Standardprüfung, kurzer Funktionstest
mittel	Testsystem, Review, definierter Smoke Test
hoch	ausführlicher Testplan, Abhängigkeitstest, Rollback-Test
sehr hoch	Pilot, Lasttest, Sicherheitsprüfung, Managementfreigabe

Tests sollten nicht nur prüfen, ob die Änderung technisch durchgeführt wurde.

Sie sollten prüfen, ob der Service danach wie erwartet nutzbar ist.

Kommunikationsbedarf nach Risiko

Je höher Risiko und Auswirkung, desto wichtiger wird Kommunikation.

Zu informieren sind je nach Change:

- betroffene Benutzer,
- Service Desk,
- Fachbereiche,
- Management,
- Lieferanten,
- Informationssicherheit,
- Kunden,
- Bereitschaftsdienst.

Inhalt der Kommunikation:

- Was wird geändert?
- Wann wird geändert?
- Welche Auswirkungen sind möglich?
- Gibt es eine Unterbrechung?
- Was müssen Benutzer tun?
- Wo gibt es Statusinformationen?
- Wann gilt der Change als abgeschlossen?

Wartungsfenster bewerten

Ein Wartungsfenster sollte passend gewählt werden.

Zu berücksichtigen sind:

- Servicezeiten,
- Geschäftsprozesse,
- internationale Zeitzonen,
- Monats- oder Jahresabschluss,
- Produktionszeiten,
- Kundenverkehr,
- Backupfenster,
- Lieferantenverfügbarkeit,
- Bereitschaft,
- Rollbackdauer.

Ein technisch bequemes Wartungsfenster ist nicht automatisch geschäftlich sinnvoll.

Abhängigkeiten und Change-Kollisionen

Mehrere Changes können sich gegenseitig beeinflussen.

Beispiele:

- Netzwerkteam ändert Routing, während Anwendungsteam ein Deployment durchführt.

- Datenbankwartung fällt mit Reporting-Lauf zusammen.
- Cloud-Team ändert Identitätsdienst, während VPN-Client aktualisiert wird.
- Backupfenster überschneidet sich mit Datenbankmigration.

Change Enablement sollte prüfen:

- Welche Changes laufen gleichzeitig?
- Betreffen sie gleiche Services oder CIs?
- Können sie sich gegenseitig beeinflussen?
- Gibt es ein Change Freeze?
- Muss eine Reihenfolge festgelegt werden?

Change Freeze

Ein Change Freeze ist ein Zeitraum, in dem Änderungen eingeschränkt werden.

Beispiele:

- Jahresabschluss,
- kritische Verkaufsphase,
- Produktionshochlauf,
- Prüfung oder Audit,
- große Migration,
- Feiertagsgeschäft.

Ein Change Freeze verhindert nicht zwingend jede Änderung.

Emergency Changes oder wichtige Sicherheitsmaßnahmen können trotzdem notwendig sein.

Dann muss besonders bewusst entschieden werden.

Sicherheitsrisiken bewerten

Besonders sorgfältig zu bewerten sind Changes an:

- Firewall-Regeln,
- Identitätsdiensten,
- Administratorrechten,
- MFA,
- Logging,
- Verschlüsselung,
- Zertifikaten,
- externen Schnittstellen,
- Cloud-Berechtigungen,
- Datenfreigaben,

- Sicherheitssoftware.

Fragen:

- Werden neue Zugriffe eröffnet?
- Werden Rechte erweitert?
- Werden Schutzmaßnahmen deaktiviert?
- Werden Logs reduziert?
- Werden sensible Daten berührt?
- Gibt es ein Prüf- oder Rezertifizierungsverfahren?

Datenschutz und Compliance

Manche Changes betreffen Datenschutz oder Compliance.

Beispiele:

- neue Datenverarbeitung,
- neue Schnittstelle,
- neue Cloud-Ablage,
- geänderte Aufbewahrung,
- geänderte Protokollierung,
- Zugriff auf personenbezogene Daten,
- Standortwechsel von Daten,
- Einführung eines neuen Tools.

Dann können zusätzliche Prüfungen erforderlich sein.

Beispielsweise durch Datenschutz, Informationssicherheit, Compliance oder Rechtsabteilung.

Lieferantenrisiken

Bei Changes mit Lieferantenbezug zu prüfen:

- Ist der Lieferant verfügbar?
- Gibt es Support während des Wartungsfensters?
- Gibt es Herstellerhinweise?
- Ist die Version unterstützt?
- Gibt es bekannte Fehler?
- Wer führt welche Aufgabe aus?
- Welche Eskalationswege gelten?
- Welche SLA oder Verträge sind betroffen?
- Wie wird das Ergebnis abgenommen?

Auch externe Changes müssen intern nachvollziehbar gesteuert werden.

Change-Erfolgskriterien

Vor der Umsetzung sollte klar sein, wann ein Change erfolgreich ist.

Beispiele:

- Anwendung startet ohne Fehler,
- Benutzer können sich anmelden,
- Schnittstelle überträgt Daten korrekt,
- Monitoring ist grün,
- keine neuen Fehler in Logs,
- Performance bleibt im Zielbereich,
- Sicherheitsprüfung erfolgreich,
- Service Desk erhält keine Störungswelle,
- Fachbereich bestätigt Funktion.

Ohne Erfolgskriterien ist die Nachprüfung unklar.

Failed Change und Lessons Learned

Ein Change kann fehlschlagen.

Wichtig ist dann:

- Auswirkungen begrenzen,
- Rollback durchführen, falls erforderlich,
- Benutzer informieren,
- Incident oder Problem verknüpfen,
- Ursache des Fehlschlags untersuchen,
- Change-Modell verbessern,
- Tests anpassen,
- Dokumentation korrigieren.

Ziel ist Lernen, nicht Schuldzuweisung.

Praxisbeispiel: Standard Change

Änderung

Standardsoftware aus genehmigtem Katalog wird installiert.

Bewertung

- Ablauf ist bekannt,
- Software ist geprüft,
- Zielgruppe ist definiert,

- Risiko ist niedrig,
- Installation ist automatisiert,
- Rollback ist möglich.

Umgang

Der Change kann als Standard Change über das Serviceportal ausgeführt werden.

Praxisbeispiel: Normal Change

Änderung

Eine produktive Fachanwendung erhält ein Versionsupdate.

Bewertung

- mehrere Fachbereiche betroffen,
- Testsystem vorhanden,
- Wartungsfenster notwendig,
- Rollback möglich, aber zeitaufwendig,
- Benutzerkommunikation erforderlich.

Umgang

Der Change wird geplant, getestet, genehmigt und nach Umsetzung geprüft.

Praxisbeispiel: Emergency Change

Änderung

Eine aktiv ausgenutzte Sicherheitslücke muss kurzfristig geschlossen werden.

Bewertung

- Risiko des Nicht-Handelns sehr hoch,
- Testzeit begrenzt,
- Produktionssystem betroffen,
- Management und Informationssicherheit müssen eingebunden werden.

Umgang

Emergency Change wird kontrolliert durchgeführt, dokumentiert und nachträglich reviewed.

Praxisbeispiel: Falsch eingestufter Change

Situation

Eine Firewall-Regel wird als kleine Routineänderung behandelt.

Problem

Die Regel betrifft eine zentrale Schnittstelle zur Warenwirtschaft.

Nach Umsetzung kann der Versand keine Aufträge mehr übertragen.

Lerneffekt

Der Change war technisch klein, aber geschäftlich kritisch.

Künftig werden Firewall-Changes nach betroffenen Services und Geschäftsprozessen bewertet, nicht nur nach technischem Aufwand.

Typische Fehler

Fehler 1

Jede Änderung wird gleich behandelt.

Fehler 2

Ein riskanter Change wird fälschlich als Standard Change eingestuft.

Fehler 3

Emergency Change wird als Abkürzung genutzt.

Fehler 4

Nur technische Risiken werden bewertet.

Fehler 5

Risiko des Nicht-Handelns wird ignoriert.

Fehler 6

Rollback wird erst während der Störung überlegt.

Fehler 7

Tests passen nicht zum Risiko.

Fehler 8

Benutzer und Service Desk werden nicht informiert.

Fehler 9

Abhängigkeiten und parallele Changes werden nicht geprüft.

Fehler 10

Sicherheits- und Datenschutzrisiken werden zu spät erkannt.

Fehler 11

Change-Erfolgskriterien fehlen.

Fehler 12

Failed Changes werden nicht ausgewertet.

Checkliste Change-Typ bestimmen

- [ ] Ist die Änderung wiederholbar?
- [ ] Ist der Ablauf dokumentiert?
- [ ] Ist das Risiko vorab bewertet?
- [ ] Ist die Änderung bereits vorab genehmigt?
- [ ] Gibt es akuten Zeitdruck?
- [ ] Droht Schaden bei Verzögerung?
- [ ] Ist ein produktiver Service betroffen?
- [ ] Sind mehrere Teams beteiligt?
- [ ] Ist ein Rollback möglich?
- [ ] Gibt es Sicherheits- oder Datenschutzbezug?
- [ ] Muss ein Service Owner entscheiden?
- [ ] Passt Standard, Normal oder Emergency Change?

Checkliste Risikobewertung

- [ ] betroffener Service bekannt
- [ ] betroffene CIs bekannt
- [ ] Benutzer- oder Kundenimpact bewertet
- [ ] geschäftliche Auswirkungen bewertet
- [ ] technische Komplexität bewertet
- [ ] Sicherheitsrisiken geprüft
- [ ] Datenschutz oder Compliance geprüft
- [ ] Abhängigkeiten geprüft
- [ ] parallele Changes geprüft
- [ ] Testumfang festgelegt
- [ ] Rollback oder Backout geprüft
- [ ] Kommunikationsbedarf bewertet
- [ ] Risiko des Nicht-Handelns bewertet

Checkliste Emergency Change

- [ ] akuter Schaden oder hohes Risiko liegt vor
- [ ] Grund für Dringlichkeit dokumentiert
- [ ] Entscheidungsträger eingebunden
- [ ] Risiko bewertet
- [ ] Mindesttest durchgeführt, soweit möglich
- [ ] Rollback geprüft
- [ ] Umsetzung dokumentiert
- [ ] Service Desk informiert
- [ ] Benutzer oder Stakeholder informiert, falls notwendig
- [ ] Ergebnis geprüft
- [ ] nachträgliches Review geplant
- [ ] Folgeproblem oder Improvement erstellt, falls nötig

Bedeutung für Fachinformatiker für Systemintegration

Fachinformatiker müssen Change-Typen und Risiken praktisch einschätzen können.

Im Arbeitsalltag bedeutet das:

- nicht jede Änderung sofort produktiv durchführen,
- technische und geschäftliche Auswirkungen bedenken,
- betroffene Services und Abhängigkeiten prüfen,
- Rollback vor der Umsetzung planen,
- Tests passend zum Risiko durchführen,
- Service Desk und Benutzer informieren,
- Changes sauber dokumentieren,
- und aus fehlgeschlagenen Changes lernen.

Gerade kleine technische Änderungen können große Auswirkungen haben, wenn sie einen kritischen Service betreffen.

Zusammenfassung

> Änderung erkennen
> ↓
> Change-Typ bestimmen
> ↓
> Auswirkung und Wahrscheinlichkeit bewerten
> ↓
> Risiko des Changes und Risiko des Nicht-Handelns vergleichen
> ↓
> Test, Rollback und Kommunikation planen
> ↓
> passende Change Authority einbinden
> ↓
> Änderung kontrolliert durchführen
> ↓
> Erfolg prüfen
> ↓
> Lessons Learned übernehmen

Merksätze

> Nicht jede Änderung benötigt denselben Prozessaufwand.

> Ein Standard Change ist vorab bewertet, nicht ungeprüft.

>

> Ein Emergency Change ist kein Ersatz für schlechte Planung.

> Technisch klein bedeutet nicht automatisch risikoarm.

> Risiko entsteht aus Auswirkung, Wahrscheinlichkeit und Kontext.

> Auch Nicht-Handeln kann riskant sein.

> Der Change-Typ muss zur tatsächlichen Auswirkung passen.

Verwandte Seiten

- 5.1 Change Enablement – Ziele, Begriffe und Abgrenzung
- 5.3 Genehmigung, Planung und Umsetzung von Changes
- 5.4 Release Management und Deployment Management
- 5.5 Change-Erfolg messen und Continual Improvement
- Incident Management
- Problem Management
- Service Configuration Management
- Information Security Management

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: Information Security Management
- PeopleCert – ITIL Practice Guide: Service Configuration Management
- ITIL Foundation – Version 5

Einordnung

Die dargestellten:

- Change-Typen,
- Risikokriterien,
- Matrizen,
- Checklisten,
- Praxisbeispiele,
- und Bewertungsfragen

sind herstellerneutrale Praxisempfehlungen.

ITIL schreibt keine universelle:

- Change-Typen-Matrix,
- Risikoskala,
- Genehmigungsmatrix,
- CAB-Pflicht,
- Testvorgabe,
- oder Emergency-Change-Struktur

für alle Organisationen vor.

Die konkrete Umsetzung muss an:

- Services,
- Risiken,
- Organisation,
- Service Levels,
- Sicherheitsanforderungen,
- Change-Modell,
- Lieferanten,
- Datenqualität,
- und verfügbare Fähigkeiten

angepasst werden.

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