

2.7 Die ITIL Management Practices

“ Kurz erklärt

ITIL Management Practices bündeln organisatorische Ressourcen und Fähigkeiten, die für einen bestimmten Zweck eingesetzt werden.

Eine Practice umfasst deshalb nicht nur einen Prozess.

Sie umfassen auch Fähigkeiten und Rollen,

- Fähigkeiten und Wissen,
- Informationen und Daten,
- Wertströme und Prozesse,
- Technologien und Werkzeuge,
- Partner und Lieferanten,
- Regeln und Kontrollen,
- Messgrößen,
- sowie Verbesserungsmaßnahmen.

ITIL Version 5 führt weiterhin **34 Management Practices**. Sie wurden gegenüber ITIL 4 nicht vollständig ersetzt, sondern weitgehend fortgeführt und an den neuen Produkt- und Servicekontext angepasst.

Warum Management Practices notwendig sind

Digitale Produkte und Services benötigen unterschiedliche organisatorische Fähigkeiten.

Beispiele:

- Incidents müssen erkannt und bearbeitet werden.
- Benutzer benötigen einen eindeutigen Kontaktweg.
- Änderungen müssen hinsichtlich Nutzen und Risiken bewertet werden.
- technische Komponenten und Abhängigkeiten müssen bekannt sein.
- Wissen muss verfügbar und aktuell sein.
- Lieferanten müssen gesteuert werden.
- Sicherheitsanforderungen müssen berücksichtigt werden.
- wiederkehrende Fehler müssen nachhaltig untersucht werden.
- Serviceleistung und Erfahrungen müssen ausgewertet werden.
- Verbesserungen müssen geplant und umgesetzt werden.

Eine einzelne Abteilung oder ein einzelner Prozess kann diese Aufgaben normalerweise nicht vollständig erfüllen.

Management Practices stellen deshalb strukturierte Fähigkeiten bereit, die in unterschiedlichen Wertströmen miteinander kombiniert werden können.

“ Merke

Eine Practice beschreibt eine organisatorische Fähigkeit.

Ein konkreter Wertstrom verwendet die benötigten Practices, um ein bestimmtes Outcome zu erreichen.

Practice, Prozess, Team und Werkzeug unterscheiden

Diese Begriffe dürfen nicht gleichgesetzt werden.

Begriff	Bedeutung
Management Practice	organisatorische Ressourcen und Fähigkeiten für einen bestimmten Zweck
Prozess	strukturierte Folge von Aktivitäten, die Eingaben in Ergebnisse überführt
Value Stream	Ende-zu-Ende-Abfolge von Schritten zur Ermöglichung eines bestimmten Outcomes
Team	Gruppe von Personen, die bestimmte Aufgaben oder Verantwortlichkeiten übernimmt
Rolle	definierte Verantwortung, Befugnis oder Tätigkeit
Werkzeug	technische Unterstützung für Informationen, Kommunikation, Automatisierung oder Kontrolle
Arbeitsanweisung	konkrete Beschreibung, wie eine bestimmte Tätigkeit ausgeführt wird

Beispiel: Incident Management

Die Practice kann enthalten:

- Rollen und Verantwortlichkeiten,
- Priorisierungskriterien,
- Eskalationswege,
- Kommunikationsregeln,
- Wissen,
- Ticketsystem,

- Monitoring-Informationen,
- Lieferantenkontakte,
- Messgrößen,
- und Verbesserungsaktivitäten.

Ein Prozess kann beschreiben:

1. Incident erfassen
2. Auswirkungen und Dringlichkeit bewerten
3. kategorisieren
4. zuständige Bearbeitung zuweisen
5. untersuchen und diagnostizieren
6. Service wiederherstellen
7. Ergebnis prüfen
8. dokumentieren und abschließen

Ein Team kann sein:

- Service Desk,
- Netzwerkteam,
- Anwendungsteam,
- Infrastrukturteam,
- externer Provider,
- oder eine bereichsübergreifende Incident-Gruppe.

Ein Werkzeug kann sein:

- Ticketsystem,
- Monitoring-Plattform,
- Kommunikationsplattform,
- Wissensdatenbank,
- oder Automatisierungslösung.

“ Typischer Fehler

Eine Practice wird eingeführt, indem lediglich ein entsprechendes Modul im Ticketsystem aktiviert wird.

Ein Werkzeug kann eine Practice unterstützen, aber fehlende Verantwortung, Fähigkeiten, Informationen und Zusammenarbeit nicht ersetzen.

Die vier Dimensionen innerhalb einer Practice

Jede Practice sollte ganzheitlich über die vier Dimensionen betrachtet werden.

Dimension	Beispielhafte Inhalte einer Practice
Organizations and People	Rollen, Fähigkeiten, Kapazität, Kommunikation und Verantwortung
Information and Technology	Daten, Wissen, Ticketsysteme, Monitoring und Automatisierung
Partners and Suppliers	externe Supportpartner, Hersteller, Provider und Verträge
Value Streams and Processes	Aktivitäten, Übergaben, Kontrollen und Arbeitsergebnisse

Beispiel: Monitoring and Event Management

Organizations and People

- Wer überwacht die Meldungen?
- Wer entscheidet über die notwendige Reaktion?
- Besteht ausreichende Bereitschaft und Fachkenntnis?

Information and Technology

- Welche Systeme werden überwacht?
- Sind Messwerte und Schwellenwerte zuverlässig?
- Wie werden Events korreliert und gespeichert?

Partners and Suppliers

- Welche Provider liefern eigene Meldungen?
- Wie werden Störungen externer Services eskaliert?

Value Streams and Processes

- Wie wird aus einem relevanten Event eine Handlung?
- Wann wird ein Incident erfasst?
- Wie werden Fehlalarme verbessert?

Management Practices sind keine isolierten Silos

Eine Practice arbeitet normalerweise nicht allein.

Bei einer realen Situation können mehrere Practices zusammenwirken.

Beispiel: Eine Unternehmensanwendung fällt nach einem Update aus.

1. **Monitoring and Event Management** erkennt eine Zustandsänderung.
2. **Incident Management** koordiniert die Wiederherstellung.
3. **Service Desk** dient als Kontakt- und Kommunikationspunkt.
4. **Service Configuration Management** liefert Informationen über Abhängigkeiten.

5. **Knowledge Management** stellt bekannte Diagnose- und Wiederherstellungsschritte bereit.
6. **Supplier Management** bindet gegebenenfalls den Hersteller ein.
7. **Problem Management** untersucht die zugrunde liegende Ursache.
8. **Change Enablement** unterstützt die kontrollierte dauerhafte Korrektur.
9. **Release Management** plant die Bereitstellung einer korrigierten Version.
10. **Deployment Management** überträgt die korrigierten Komponenten in die Zielumgebung.
11. **Service Validation and Testing** prüft die neue oder geänderte Lösung.
12. **Continual Improvement** leitet Verbesserungen für Tests, Monitoring und Arbeitsweisen ab.

“ Merke

Ein Vorgang gehört nicht immer nur zu einer Practice.

Die benötigten Practices werden entsprechend dem tatsächlichen Wertstrom miteinander verbunden.

Änderungen gegenüber ITIL 4

ITIL Version 5 führt die 34 Management Practices weitgehend fort.

Sie werden im aktuellen Framework in zwei übergeordneten Gruppen organisiert:

1. **Product and Service Management Practices**
2. **General Management Practices**

Die frühere ITIL-4-Einteilung in:

- General Management Practices,
- Service Management Practices,
- und Technical Management Practices

soll deshalb nicht ungeprüft als aktuelle ITIL-Version-5-Struktur übernommen werden.

Die öffentlich zugänglichen offiziellen Übersichtsseiten bestätigen die neue Einteilung in zwei Gruppen, veröffentlichen dort jedoch keine vollständige frei zugängliche Zuordnung aller 34 Practices zu diesen beiden Gruppen.

Die detaillierten aktuellen Practice Guides werden über PeopleCert Plus bereitgestellt.

Wichtig

Diese Seite führt die 34 Practices deshalb alphabetisch auf.

Sie behauptet keine nicht ausreichend öffentlich belegte Einzelzuordnung zu den beiden neuen Gruppen.

Hinweis zur Bezeichnung Change Enablement

Die aktuelle offizielle ITIL-Version-5-Übersicht zum Practice-Manager-Pfad verwendet weiterhin die Bezeichnung **Change Enablement**.

In anderen offiziellen Überblickstexten wird teilweise allgemein von **change management** gesprochen.

Solange die konkrete aktuelle Practice Guidance keine eindeutig abweichende offizielle Practice-Bezeichnung vorgibt, verwendet dieses Buch deshalb:

“ Change Enablement

Change Management kann weiterhin als allgemeiner organisatorischer Oberbegriff oder als betriebliche Bezeichnung vorkommen.

“ Versionsabhängig

Eine betriebliche Organisation kann weiterhin eigene Begriffe wie Change Management, Änderungsmanagement oder Change-Prozess verwenden.

Entscheidend ist, dass Zweck, Verantwortlichkeiten und Arbeitsweise eindeutig sind.

Die 34 ITIL Management Practices im Überblick

Die folgenden Kurzbeschreibungen sind praxisnahe Zusammenfassungen in eigenen Worten.

Sie ersetzen nicht die vollständigen offiziellen Practice Guides.

Nr.	Management Practice	Praxisnahe Kurzbeschreibung
-----	---------------------	-----------------------------

1	Architecture Management	aktuelle und zukünftige Strukturen, Beziehungen und Architekturentscheidungen nachvollziehbar gestalten
2	Availability Management	sicherstellen, dass Produkte und Services die benötigte und vereinbarte Verfügbarkeit unterstützen
3	Business Analysis	Bedürfnisse, Probleme und Anforderungen untersuchen und geeignete Lösungsoptionen unterstützen
4	Capacity and Performance Management	ausreichende Kapazität und Leistung für aktuelle und zukünftige Anforderungen sicherstellen
5	Change Enablement	erfolgreiche Änderungen durch angemessene Bewertung, Autorisierung und Steuerung unterstützen
6	Continual Improvement	Produkte, Services, Practices und Arbeitsweisen fortlaufend an veränderte Bedürfnisse anpassen
7	Deployment Management	neue oder geänderte Komponenten kontrolliert in Zielumgebungen übertragen
8	Incident Management	negative Auswirkungen von Incidents verringern und den normalen Servicebetrieb angemessen schnell wiederherstellen
9	Information Security Management	Informationen und unterstützende Systeme entsprechend den Sicherheitsanforderungen schützen
10	Infrastructure and Platform Management	Infrastruktur- und Plattformressourcen über ihren Lebenszyklus planen, betreiben und verbessern
11	IT Asset Management	IT-Assets über ihren Lebenszyklus steuern, um Wert, Kosten, Risiken und Entscheidungen zu unterstützen
12	Knowledge Management	benötigtes Wissen und Informationen wirksam erfassen, pflegen, teilen und verwenden
13	Measurement and Reporting	verlässliche Messungen und Berichte für Entscheidungen, Steuerung und Verbesserung bereitstellen

14	Monitoring and Event Management	Produkte, Services und Komponenten systematisch beobachten und relevante Zustandsänderungen behandeln
15	Organizational Change Management	menschliche und organisatorische Veränderungen so unterstützen, dass neue Arbeitsweisen angenommen und dauerhaft genutzt werden
16	Portfolio Management	Investitionen, Produkte, Services, Programme und Projekte auf Strategie, Wert und verfügbare Ressourcen ausrichten
17	Problem Management	Ursachen und Wahrscheinlichkeiten von Incidents reduzieren sowie bekannte Fehler und Workarounds verwalten
18	Project Management	zeitlich begrenzte Vorhaben strukturiert planen, steuern und abschließen
19	Relationship Management	Beziehungen zu Stakeholdern aufbauen, pflegen und für gemeinsame Outcomes nutzen
20	Release Management	neue oder geänderte Produkte, Services und Funktionen für die vorgesehene Nutzung verfügbar machen
21	Risk Management	Risiken identifizieren, bewerten, behandeln, überwachen und angemessen kommunizieren
22	Service Catalogue Management	verlässliche und verständliche Informationen über Services und Serviceangebote bereitstellen
23	Service Configuration Management	zuverlässige Informationen über Services, Configuration Items und deren Beziehungen verfügbar machen
24	Service Continuity Management	ausreichende Servicefähigkeit nach schwerwiegenden Störungen oder Katastrophen vorbereiten und erhalten
25	Service Design	Produkte und Services ganzheitlich so gestalten, dass sie zweckmäßig, nutzbar und nachhaltig betreibbar sind
26	Service Desk	zentralen Kontakt, Kommunikation sowie Unterstützung für Benutzer und Kunden ermöglichen

27	Service Financial Management	finanzielle Informationen, Planung und Kontrolle für Produkte, Services und Entscheidungen unterstützen
28	Service Level Management	verständliche, geschäftsbezogene Serviceziele vereinbaren und deren Erfüllung steuern
29	Service Request Management	vereinbarte und häufig standardisierte Benutzeranfragen wirksam bearbeiten
30	Service Validation and Testing	prüfen, ob neue oder geänderte Produkte und Services definierte Anforderungen und Nutzungsbedürfnisse erfüllen
31	Software Development and Management	Software so entwickeln und verwalten, dass sie Anforderungen, Qualität, Wartbarkeit und Compliance unterstützt
32	Strategy Management	Ziele, Ausrichtung und geeignete Handlungsoptionen für die Organisation entwickeln
33	Supplier Management	Lieferanten, Verträge, Leistungen und Beziehungen angemessen steuern
34	Workforce and Talent Management	sicherstellen, dass ausreichend geeignete Menschen, Fähigkeiten und Entwicklungsmöglichkeiten vorhanden sind

Nicht jede Practice muss gleich stark ausgeprägt sein

Eine Organisation muss nicht jede Practice:

- als eigene Abteilung,
- mit einem eigenen Practice Owner,
- mit einem umfangreichen Prozess,
- oder mit einem separaten Werkzeugmodul

aufbauen.

Der benötigte Umfang hängt unter anderem ab von:

- Größe der Organisation,
- Produkten und Services,
- Risiken,
- gesetzlichen Anforderungen,
- Anzahl der Benutzer,
- Lieferantenabhängigkeiten,

- vorhandenen Fähigkeiten,
- technischer Komplexität,
- und strategischer Bedeutung.

Beispiel:

Ein kleines Unternehmen kann Supplier Management durch:

- klar dokumentierte Verträge,
- eindeutige Ansprechpartner,
- regelmäßige Leistungsprüfungen,
- und vorbereitete Eskalationswege

umsetzen.

Eine große Organisation benötigt möglicherweise zusätzlich:

- mehrere Supplier Manager,
- formalisierte Lieferantenbewertungen,
- Risikokategorien,
- regelmäßige Reviews,
- Vertragsdatenbanken,
- Auditverfahren,
- und strategische Lieferantenprogramme.

“ Grundsatz

Eine Practice muss wirksam und angemessen sein.

Sie muss nicht möglichst groß oder kompliziert sein.

Foundation-Wissen und vollständige Practice Guidance unterscheiden

Die ITIL Foundation vermittelt:

- grundlegende Begriffe,
- zentrale Zwecke,
- wichtige Zusammenhänge,
- und ausgewählte Practice-Terminologie.

Die vollständige Practice Guidance kann darüber hinaus behandeln:

- Erfolgsfaktoren,
- Practice-Prozesse,

- Aktivitäten,
- Rollen,
- Informationen,
- Technologien,
- Partner,
- Messgrößen,
- Wertströme,
- Reife und Fähigkeiten,
- Automatisierung,
- und Verbesserung.

“ Wichtig

Eine kurze Foundation-Definition reicht nicht aus, um eine vollständige betriebliche Practice zu gestalten.

Für eine praktische Einführung werden zusätzlich benötigt:

- Analyse des aktuellen Zustands,
- Ziele und Outcomes,
- betriebliche Anforderungen,
- Rollen und Befugnisse,
- konkrete Wertströme,
- Werkzeuge,
- Daten,
- Schulungen,
- Messgrößen,
- und ein Verbesserungsplan.

Zertifizierungsbezogene Practice-Bündel

Die aktuelle offizielle Practice-Manager-Struktur verwendet drei Bündel mit jeweils fünf Practices.

Diese Bündel sind für die Zertifizierungsstruktur relevant.

Sie sind nicht mit den zwei übergeordneten Practice-Gruppen von ITIL Version 5 gleichzusetzen.

Monitor, Support and Fulfil

Enthaltene Practices:

- Service Desk
- Incident Management

- Problem Management
- Service Request Management
- Monitoring and Event Management

Gemeinsamer praktischer Schwerpunkt:

- Zustände erkennen,
 - Benutzerkontakte ermöglichen,
 - Störungen bearbeiten,
 - Anfragen erfüllen,
 - wiederkehrende Ursachen reduzieren,
 - und Erkenntnisse aus dem laufenden Betrieb verwenden.
-

Plan, Implement and Control

Enthaltene Practices:

- Change Enablement
- Deployment Management
- Release Management
- Service Configuration Management
- IT Asset Management

Gemeinsamer praktischer Schwerpunkt:

- Veränderungen vorbereiten,
 - Risiken und Abhängigkeiten verstehen,
 - Komponenten kontrolliert bereitstellen,
 - Releases verfügbar machen,
 - und Informationen über Assets sowie Konfigurationen pflegen.
-

Collaborate, Assure and Improve

Enthaltene Practices:

- Relationship Management
- Supplier Management
- Service Level Management
- Continual Improvement
- Information Security Management

Gemeinsamer praktischer Schwerpunkt:

- Beziehungen und Erwartungen gestalten,
- Lieferanten steuern,

- Serviceziele vereinbaren,
- Informationssicherheit unterstützen,
- und Verbesserungen fortlaufend umsetzen.

“ Hinweis

Die übrigen Practices bleiben weiterhin Bestandteil der insgesamt 34 ITIL Management Practices, auch wenn sie nicht in diesen drei Practice-Manager-Bündeln enthalten sind.

Wichtige Practices für Fachinformatiker für Systemintegration

Für Fachinformatiker für Systemintegration sind abhängig vom Arbeitsplatz besonders häufig folgende Practices relevant:

Practice	Typischer Bezug zum Arbeitsalltag
Service Desk	Benutzerkontakt, Erfassung, Kommunikation und Weiterleitung
Incident Management	Störungen analysieren und Servicebetrieb wiederherstellen
Service Request Management	Benutzerkonten, Zugriffe, Software und Standardleistungen bereitstellen
Problem Management	wiederkehrende Fehler und zugrunde liegende Ursachen untersuchen
Change Enablement	technische Änderungen bewerten und kontrolliert durchführen
Deployment Management	Software, Konfigurationen oder Infrastrukturkomponenten bereitstellen
Release Management	neue oder geänderte Funktionen für die Nutzung verfügbar machen
Monitoring and Event Management	technische Zustände und relevante Abweichungen erkennen
Service Configuration Management	Abhängigkeiten und Configuration Items nachvollziehen
IT Asset Management	Hardware, Software, Lizenzen und Cloud-Ressourcen verwalten
Knowledge Management	Lösungen, Arbeitsanweisungen und Erkenntnisse verfügbar machen
Information Security Management	Schutzanforderungen bei Betrieb und Änderungen berücksichtigen
Supplier Management	Hersteller, Provider und Supportpartner einbinden

Practice	Typischer Bezug zum Arbeitsalltag
Service Continuity Management	Wiederherstellung und Fortführung kritischer Services unterstützen
Capacity and Performance Management	Leistung, Kapazität und zukünftigen Bedarf bewerten
Availability Management	benötigte Verfügbarkeit technischer und servicebezogener Fähigkeiten unterstützen
Continual Improvement	wiederkehrende Probleme und Arbeitsweisen nachhaltig verbessern

Nicht jeder Fachinformatiker ist für die vollständige Steuerung dieser Practices verantwortlich.

Er kann jedoch durch technische Arbeit, Dokumentation, Eskalation und Rückmeldungen zu ihrer Wirksamkeit beitragen.

Service Desk und Incident Management unterscheiden

Diese beiden Practices werden häufig gleichgesetzt.

Service Desk	Incident Management
stellt einen zentralen Kontakt- und Kommunikationspunkt bereit	koordiniert die Behandlung von Incidents
bearbeitet Kontakte, Fragen, Anfragen und Meldungen	konzentriert sich auf negative Serviceauswirkungen und Wiederherstellung
unterstützt Benutzerkommunikation	organisiert Priorisierung, Diagnose, Eskalation und Wiederherstellung
kann Incidents und Service Requests erfassen	kann mehrere Teams und Lieferanten einbeziehen
ist eine Practice und kann organisatorisch als Team umgesetzt sein	ist eine Practice, die nicht auf ein einzelnes Team begrenzt ist

Ein Service Desk kann Incident Management wesentlich unterstützen.

Er ist jedoch nicht mit der gesamten Incident-Management-Practice identisch.

Incident Management und Problem Management unterscheiden

Incident Management	Problem Management
konzentriert sich auf die aktuelle negative Auswirkung	konzentriert sich auf Ursachen und zukünftige Auswirkungen
priorisiert Wiederherstellung	priorisiert Untersuchung und nachhaltige Risikoreduzierung
kann eine Zwischenlösung verwenden	verwaltet Ursachen, bekannte Fehler und Workarounds

Incident Management	Problem Management
arbeitet häufig unter höherem Zeitdruck	kann nach der Wiederherstellung vertieft arbeiten
Erfolg: Service ist wieder nutzbar	Erfolg: Wahrscheinlichkeit oder Auswirkung weiterer Incidents wird reduziert

Beispiel:

Ein Dienst wird nach einem Speicherfehler neu gestartet.

- Der Neustart kann den Incident lösen.
- Die Ursache des steigenden Speicherverbrauchs bleibt ein mögliches Problem.
- Eine dauerhafte Korrektur kann anschließend einen Change, Release und Deployment benötigen.

“ Merke

Ein Incident muss nicht vollständig ursächlich verstanden sein, bevor der Service wiederhergestellt wird.

Eine Wiederherstellung beseitigt jedoch nicht automatisch die zugrunde liegende Ursache.

Event, Incident und Problem unterscheiden

Begriff	Bedeutung
Event	erkannte Zustandsänderung, die für das Management eines Produkts oder Service relevant sein kann
Incident	ungeplante Unterbrechung, Qualitätsminderung oder andere negative Serviceauswirkung
Problem	Ursache oder mögliche Ursache eines oder mehrerer Incidents

Beispiel:

- Monitoring meldet eine hohe Speicherauslastung: **Event**
- Anwendung reagiert nicht mehr: **Incident**
- fehlerhafte Speicherverwaltung der Anwendung: **Problem**

Nicht jedes Event wird zu einem Incident.

Nicht jeder Incident benötigt einen eigenen Problem Record.

Die konkrete Einordnung hängt von Auswirkungen, Wiederholung, Risiko und betrieblicher Arbeitsweise ab.

Service Request und Incident unterscheiden

Service Request	Incident
vorgesehene Benutzeranfrage	ungeplante negative Serviceauswirkung
häufig standardisierbar	benötigt Untersuchung oder Wiederherstellung
Beispiel: neue Software anfordern	Beispiel: vorhandene Software startet nicht
Beispiel: Zugriff beantragen	Beispiel: genehmigter Zugriff funktioniert nicht
Beispiel: Auskunft anfordern	Beispiel: Service ist nicht erreichbar

Die Formulierung eines Benutzers entscheidet nicht automatisch über die Einordnung.

Ein Benutzer kann beispielsweise sagen:

“ Ich brauche ein neues Kennwort.

Dahinter können unterschiedliche Situationen stehen:

- planmäßige Kennwortänderung,
- vergessenes Kennwort,
- gesperrtes Konto,
- möglicher Sicherheitsvorfall,
- oder fehlerhafter Identitätsdienst.

Change Enablement, Release und Deployment unterscheiden

Practice	Zentrale Betrachtung
Change Enablement	Nutzen, Risiko, Bewertung, Autorisierung und Steuerung einer Änderung
Release Management	neue oder geänderte Funktionen und Servicebestandteile für die Nutzung verfügbar machen
Deployment Management	Komponenten in eine Zielumgebung übertragen

Beispiel: neue Anwendungsversion

Change Enablement

- Auswirkungen und Risiken bewerten

- notwendige Autorisierung sicherstellen
- Zeitpunkt und Abhängigkeiten koordinieren
- Rückfall- oder Wiederherstellungsplanung berücksichtigen

Release Management

- festlegen, welche Funktionen und Änderungen gemeinsam verfügbar gemacht werden
- Releaseinformationen bereitstellen
- Erwartungen und Zeitplanung abstimmen

Deployment Management

- Softwarepaket technisch übertragen
- Konfiguration anwenden
- Installation oder Aktivierung durchführen
- technisches Ergebnis prüfen

Diese Tätigkeiten können miteinander verbunden sein, besitzen aber unterschiedliche Zwecke.

IT Asset und Configuration Item unterscheiden

Ein **IT Asset** wird hinsichtlich seines finanziellen, vertraglichen, risikobezogenen und lebenszyklusbezogenen Werts verwaltet.

Ein **Configuration Item** wird verwaltet, weil Informationen über seinen Zustand und seine Beziehungen für das Management eines Produktes oder Service benötigt werden.

Ein Gegenstand kann:

- nur IT Asset,
- nur Configuration Item,
- beides,
- oder keines von beidem

sein.

Beispiele:

Gegenstand	Mögliche Einordnung
physischer Server	IT Asset und Configuration Item
Softwarelizenz	IT Asset, möglicherweise auch Configuration Item
virtueller Cluster	Configuration Item, abhängig vom Modell möglicherweise Asset-Bezug
Netzwerkkabel	je nach Bedeutung weder einzeln verwaltetes Asset noch CI

Gegenstand	Mögliche Einordnung
Cloud-Abonnement	IT Asset und möglicherweise Configuration Item
Service-Dokumentation	möglicherweise Configuration Item, aber normalerweise kein IT Asset

“ Wichtig

Nicht jede technische Komponente muss automatisch als einzelnes Configuration Item erfasst werden.

Der benötigte Detaillierungsgrad muss einen erkennbaren Nutzen besitzen.

Practice Owner, Process Owner und ausführende Rolle

Organisationen können unterschiedliche Verantwortlichkeiten verwenden.

Rolle	Möglicher Schwerpunkt
Practice Owner	Wirksamkeit und Weiterentwicklung der gesamten Practice
Process Owner	Gestaltung und Pflege eines konkreten Prozesses
Process Manager	laufende Steuerung eines Prozesses
Service Owner	Ende-zu-Ende-Verantwortung für einen Service
Product Owner oder Product Manager	Prioritäten und Entwicklung eines Produkts
ausführende Rolle	konkrete Bearbeitung einer Aufgabe
Tool Owner	Betrieb und Weiterentwicklung des unterstützenden Werkzeugs

ITIL schreibt nicht vor, dass jede Organisation genau diese Rollen einsetzen muss.

Entscheidend ist, dass geklärt ist:

- wer entscheidet,
- wer ausführt,
- wer für Ergebnisse einsteht,
- wer Verbesserungen steuert,
- und wer die benötigten Informationen und Ressourcen bereitstellt.

Eine Practice einführen oder verbessern

Eine Practice sollte nicht mit der Auswahl eines Werkzeugs beginnen.

Eine sinnvolle Vorgehensweise ist:

1. Problem oder Bedarf verstehen
2. gewünschte Outcomes bestimmen
3. aktuellen Zustand untersuchen
4. relevante Stakeholder einbeziehen
5. betroffene Wertströme bestimmen
6. vorhandene Fähigkeiten und Daten bewerten
7. Rollen und Verantwortung klären
8. angemessene Prozesse und Kontrollen gestalten
9. benötigte Informationen und Werkzeuge festlegen
10. Lieferanten und Abhängigkeiten berücksichtigen
11. Messgrößen und Erfolgskriterien definieren
12. schrittweise einführen
13. Feedback auswerten
14. fortlaufend verbessern

“ Typischer Fehler

Eine vollständige theoretische Practice wird auf einmal entworfen und anschließend der Organisation aufgezwungen.

Dadurch entstehen umfangreiche Dokumentationen, die nicht zur tatsächlichen Arbeitsweise passen.

Eine Practice an Wertströmen ausrichten

Practices sollten nicht ausschließlich intern optimiert werden.

Beispiel:

Incident Management erreicht eine kurze interne Bearbeitungszeit, indem Tickets schnell an andere Teams weitergegeben werden.

Dadurch können jedoch entstehen:

- mehr Übergaben,
- Informationsverluste,
- längere Gesamtdauer,
- wiederholte Rückfragen,
- und schlechte Benutzererfahrung.

Deshalb sollte geprüft werden:

- Welchen Value Stream unterstützt die Practice?
- Welches Outcome soll erreicht werden?
- Welche anderen Practices sind beteiligt?
- Wo entstehen Übergaben?
- Welche Informationen müssen fließen?
- Welche lokalen Kennzahlen schaden möglicherweise dem Gesamtergebnis?

“ **Merke**

Eine leistungsfähige Practice unterstützt den gesamten Wertstrom und nicht nur ihre eigene interne Kennzahl.

Messung einer Practice

Messgrößen sollten den Zweck und die Outcomes einer Practice unterstützen.

Nicht ausreichend ist es, nur leicht verfügbare Aktivitäten zu zählen.

Beispiel: Incident Management

Mögliche Aktivitätszahlen:

- Anzahl geöffneter Tickets
- Anzahl geschlossener Tickets
- durchschnittliche Bearbeitungszeit

Zusätzliche Ergebnisinformationen:

- tatsächliche Wiederherstellungszeit
- Auswirkung auf Benutzer
- wiederholte Incidents
- Erfolgsquote von Wiederherstellungen
- Qualität der Kommunikation
- erneute Kontaktaufnahme
- Anzahl falsch geschlossener Vorgänge
- Serviceerfahrung
- nachhaltige Verbesserungen

Beispiel: Knowledge Management

Unzureichende Einzelkennzahl:



Ergänzende Fragen:

- Werden die Artikel gefunden?
- Sind sie aktuell?
- Helfen sie bei der Lösung?
- Werden sie von Benutzern und Mitarbeitern verstanden?
- Reduzieren sie wiederholte Analyse?
- Werden falsche oder veraltete Inhalte entfernt?

Kennzahlen dürfen nicht das Verhalten verschlechtern

Eine ungeeignete Kennzahl kann unerwünschtes Verhalten fördern.

Kennzahl	Mögliche Fehlwirkung
möglichst viele geschlossene Tickets	Vorgänge werden voreilig abgeschlossen
möglichst kurze Gesprächsdauer	Benutzerproblem wird nicht vollständig verstanden
möglichst wenige Changes	notwendige Verbesserungen und Sicherheitsupdates werden vermieden
möglichst wenige Incidents	Incidents werden nicht erfasst oder falsch eingeordnet
möglichst viele Wissensartikel	Qualität und Aktualität sinken
möglichst hohe technische Verfügbarkeit	tatsächliche Nutzbarkeit und Erfahrung werden übersehen

Messgrößen sollten deshalb gemeinsam betrachtet und regelmäßig überprüft werden.

Practice Capability und Maturity

Eine Practice kann unterschiedlich stark entwickelt sein.

Zu bewerten sind beispielsweise:

- Klarheit von Zweck und Outcomes,
- Rollen und Verantwortlichkeiten,
- Fähigkeiten,
- Informationen,
- Prozesse,
- Werkzeuge,
- Lieferanten,
- Messung,
- Integration in Wertströme,

- und Continual Improvement.

Eine umfangreiche Dokumentation bedeutet nicht automatisch hohe Fähigkeit oder Reife.

Eine Practice kann formal beschrieben sein und trotzdem unwirksam bleiben, wenn:

- Mitarbeiter den Ablauf umgehen,
- Informationen unzuverlässig sind,
- Befugnisse fehlen,
- Werkzeuge nicht passen,
- Schnittstellen nicht funktionieren,
- oder Ergebnisse nicht verbessert werden.

“ Merke

Practice Capability zeigt sich in der wirksamen Erreichung des Zwecks und nicht in der Menge der Dokumente.

Automatisierung innerhalb von Practices

Automatisierung kann Practices unterstützen.

Beispiele:

Practice	Mögliche Automatisierung
Incident Management	automatische Erfassung aus relevantem Monitoring-Event
Service Request Management	standardisierte Bereitstellung genehmigter Software
Change Enablement	risikobasierte Weiterleitung und Terminprüfung
IT Asset Management	automatische Inventarisierung
Service Configuration Management	technische Discovery und Beziehungsaktualisierung
Knowledge Management	Vorschläge passender Wissensartikel
Monitoring and Event Management	Korrelation und Unterdrückung redundanter Events
Measurement and Reporting	automatische Datensammlung und Berichtserstellung
Deployment Management	automatisierte Bereitstellung und technische Prüfung
Information Security Management	automatische Richtlinien- und Konfigurationskontrolle

Vor der Automatisierung muss geprüft werden:

- Ist der Zweck verstanden?
- Ist die Arbeitsweise geeignet?

- Sind Eingabedaten zuverlässig?
- Sind Ausnahmen bekannt?
- Wie werden Fehler erkannt?
- Wer trägt Verantwortung?
- Wie wird die Automatisierung überwacht?
- Gibt es eine Rückfallmöglichkeit?
- Entsteht ein tatsächlicher Nutzen?

“ Grundsatz

Erst verstehen und optimieren, dann automatisieren.

Künstliche Intelligenz innerhalb von Practices

KI kann unter anderem unterstützen bei:

- Klassifizierung von Tickets,
- Zusammenfassung von Vorgängen,
- Suche nach Wissensartikeln,
- Erkennung von Mustern,
- Priorisierungsvorschlägen,
- Analyse von Monitoring-Daten,
- Berichtserstellung,
- Übersetzung,
- und Formulierung von Benutzerkommunikation.

Dabei müssen berücksichtigt werden:

- Datenqualität,
- Datenschutz,
- Informationssicherheit,
- Nachvollziehbarkeit,
- mögliche Verzerrungen,
- Fehlerwahrscheinlichkeit,
- menschliche Kontrolle,
- und Verantwortung.

Beispiel:

Eine KI schlägt eine hohe Incident-Priorität vor.

Die zuständige Arbeitsweise muss weiterhin klären:

- Welche Auswirkungen bestehen tatsächlich?

- Wie dringend ist die Situation?
- Welche Kriterien verwendet die Organisation?
- Sind die Eingangsdaten vollständig?
- Wer bestätigt oder ändert die Priorität?
- Wie wird die Entscheidung dokumentiert?

“ Sicherheitsrelevant

Eine KI-Empfehlung überträgt die Entscheidungs- und Ergebnisverantwortung nicht auf das technische System.

Practice und betriebliche Organisation

Organisationen können Practices unterschiedlich benennen oder zusammenfassen.

Beispiele:

- Incident Management kann intern als Störungsmanagement bezeichnet werden.
- Service Request Management kann im Bestell- oder Benutzerportal integriert sein.
- Change Enablement kann als Change Management bezeichnet werden.
- Monitoring and Event Management kann organisatorisch im Network Operations Center liegen.
- IT Asset Management kann teilweise durch Einkauf oder Finanzabteilung unterstützt werden.
- Information Security Management kann eng mit einem Informationssicherheitsmanagementsystem verbunden sein.

Die interne Bezeichnung ist weniger wichtig als eine eindeutige Arbeitsweise.

Zu klären ist:

- Welcher Zweck wird verfolgt?
- Welche Outcomes werden erwartet?
- Wer trägt Verantwortung?
- Welche Informationen werden benötigt?
- Welche Schnittstellen bestehen?
- Wie wird die Wirksamkeit geprüft?
- Wie werden Verbesserungen umgesetzt?

Praxisbeispiel: wiederkehrender VPN-Ausfall

Mehrere Benutzer verlieren regelmäßig die VPN-Verbindung.

Monitoring and Event Management

- Verbindungsabbrüche und technische Zustände erkennen
- relevante Messwerte und Ereignisse bereitstellen

Service Desk

- Benutzerkontakte und Rückmeldungen erfassen
- verständliche Statusinformationen bereitstellen

Incident Management

- Auswirkungen und Dringlichkeit bewerten
- Wiederherstellung koordinieren
- zuständige Teams und Provider einbinden

Service Configuration Management

- Abhängigkeiten zwischen VPN-Gateway, Identitätsdienst, Zertifikaten, Netzwerk und Provider darstellen

Supplier Management

- externe Anbieter anhand geeigneter Informationen einbinden und eskalieren

Knowledge Management

- Diagnose- und Zwischenlösungen verfügbar machen

Problem Management

- wiederkehrende Muster und zugrunde liegende Ursache untersuchen

Change Enablement

- dauerhafte Korrektur hinsichtlich Risiko, Autorisierung und Zeitpunkt steuern

Deployment Management

- geänderte Konfiguration oder Software kontrolliert bereitstellen

Service Validation and Testing

- Stabilität, Kompatibilität und erwartete Nutzung prüfen

Continual Improvement

- Monitoring, Dokumentation, Eskalation und technische Lösung verbessern

Praxisbeispiel: neuer Mitarbeiter

Das gewünschte Outcome lautet:

“ Der neue Mitarbeiter kann am ersten Arbeitstag sicher und vollständig arbeiten.

Mögliche beteiligte Practices:

Practice	Beitrag
Service Request Management	Onboarding-Anfrage erfassen und koordinieren
Service Catalogue Management	verfügbare Arbeitsplatz- und Zugangsangebote beschreiben
IT Asset Management	Endgerät und Lizenzen bereitstellen und verwalten
Service Configuration Management	relevante Beziehungen und Konfigurationen dokumentieren
Information Security Management	Zugriff und Sicherheitsanforderungen berücksichtigen
Supplier Management	externe Lieferung oder Lizenzbereitstellung steuern
Knowledge Management	Anleitungen und Übergabeinformationen bereitstellen
Service Desk	Fragen und Probleme beim Einstieg unterstützen
Continual Improvement	Verzögerungen und wiederkehrende Fehler im Onboarding reduzieren

Der Value Stream endet nicht bereits mit der Erstellung des Benutzerkontos.

Er endet mit dem überprüften Outcome der Arbeitsfähigkeit.

Praxisbeispiel: abgelaufenes Zertifikat

Ein Zertifikat läuft ab und verursacht einen Serviceausfall.

Incident Management

- Service wiederherstellen

Monitoring and Event Management

- prüfen, warum keine ausreichende Warnung erfolgte

Service Configuration Management

- betroffene Zertifikate, Systeme und Services nachvollziehen

Problem Management

- systemische Ursache untersuchen

Knowledge Management

- Erneuerungs- und Wiederherstellungsverfahren dokumentieren

Change Enablement

- dauerhafte technische oder organisatorische Korrektur steuern

Information Security Management

- sichere Zertifikatsverwaltung berücksichtigen

Continual Improvement

- zentrale Erfassung, Verantwortlichkeit und Alarmierung verbessern

“ Merke

Die unmittelbare technische Reparatur kann einen Incident lösen.

Mehrere weitere Practices können notwendig sein, um eine Wiederholung zu verhindern.

Typische Fehler bei der Anwendung von Practices

Fehler 1: Practice mit Prozess gleichsetzen

Die Organisation dokumentiert einen Ablauf, berücksichtigt aber Rollen, Wissen, Werkzeuge und Partner nicht ausreichend.

Fehler 2: Practice mit Team gleichsetzen

Incident Management wird ausschließlich als Aufgabe des Service Desk betrachtet, obwohl technische Teams, Service Owner und Lieferanten beteiligt sein können.

Fehler 3: Tool als Ausgangspunkt verwenden

Das Ticketsystem bestimmt Kategorien und Arbeitsweisen, obwohl der tatsächliche Bedarf nicht untersucht wurde.

Fehler 4: Practices isoliert optimieren

Jede Practice verbessert ihre eigenen Kennzahlen, während Übergaben und Gesamtdauer schlechter werden.

Fehler 5: jede Practice maximal formalisieren

Auch einfache und risikoarme Tätigkeiten erhalten unnötig umfangreiche Prozesse und Freigaben.

Fehler 6: nur den Normalfall gestalten

Ausnahmen, Eskalationen, Sicherheitsvorfälle und Lieferantenausfälle werden nicht berücksichtigt.

Fehler 7: Verantwortung nicht eindeutig festlegen

Viele Teams sind beteiligt, aber niemand koordiniert das Ende-zu-Ende-Ergebnis.

Fehler 8: Messung nur auf Aktivität ausrichten

Gezählt werden Tickets, Changes oder Wissensartikel, aber nicht deren Nutzen und Qualität.

Fehler 9: Practice nach Einführung nicht weiterentwickeln

Arbeitsweisen, Werkzeuge und Anforderungen verändern sich, während die Practice unverändert bleibt.

Fehler 10: ältere Begriffe ungeprüft übernehmen

ITIL-4-Kategorien oder betriebliche Begriffe werden ohne Versionshinweis als aktuelle ITIL-Version-5-Struktur dargestellt.

30-Sekunden-Prüfung einer Practice

Bei der Bewertung einer Practice kannst du folgende Fragen stellen:

1. Welchen Zweck erfüllt die Practice?
2. Welches Outcome soll sie unterstützen?
3. In welchen Wertströmen wird sie verwendet?

4. Wer trägt Verantwortung?
 5. Welche Fähigkeiten werden benötigt?
 6. Welche Informationen und Werkzeuge sind notwendig?
 7. Welche anderen Practices sind beteiligt?
 8. Welche Partner oder Lieferanten werden benötigt?
 9. Wie wird die Wirksamkeit gemessen?
 10. Wie wird die Practice verbessert?
-

Checkliste für den Aufbau einer Practice

- ☐ Ist der konkrete Bedarf bekannt?
 - ☐ Sind Zweck und gewünschte Outcomes eindeutig?
 - ☐ Wurde der aktuelle Zustand untersucht?
 - ☐ Sind relevante Stakeholder beteiligt?
 - ☐ Sind die betroffenen Wertströme bekannt?
 - ☐ Sind Rollen, Verantwortung und Befugnisse geklärt?
 - ☐ Sind benötigte Fähigkeiten und Kapazitäten vorhanden?
 - ☐ Sind Informationen und Daten ausreichend zuverlässig?
 - ☐ Sind Prozesse und Kontrollen angemessen?
 - ☐ Unterstützen Werkzeuge die Arbeitsweise?
 - ☐ Sind Partner und Lieferanten berücksichtigt?
 - ☐ Sind Schnittstellen zu anderen Practices geklärt?
 - ☐ Sind Messgrößen und Erfolgskriterien definiert?
 - ☐ Wird schrittweise mit Feedback eingeführt?
 - ☐ Ist Continual Improvement integriert?
-

Checkliste für die Bewertung einer bestehenden Practice

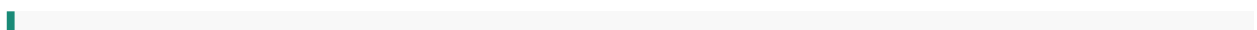
- ☐ Erfüllt die Practice ihren tatsächlichen Zweck?
- ☐ Unterstützt sie benötigte Outcomes und Wertströme?
- ☐ Sind Verantwortung und Eskalationswege bekannt?
- ☐ Werden Arbeitsweisen tatsächlich angewendet?
- ☐ Sind Daten und Dokumentationen aktuell?
- ☐ Sind Werkzeuge zweckmäßig konfiguriert?
- ☐ Funktionieren Übergaben zu anderen Practices?
- ☐ Werden Benutzer- und Stakeholdererfahrungen berücksichtigt?
- ☐ Entstehen unnötige Wartezeiten oder Freigaben?

- ☐ Werden Risiken angemessen behandelt?
- ☐ Sind Lieferanten wirksam eingebunden?
- ☐ Messen Kennzahlen Ergebnisse statt nur Aktivitäten?
- ☐ Werden Automatisierungen überwacht?
- ☐ Werden bekannte Schwächen priorisiert verbessert?
- ☐ Passt die Practice weiterhin zur Organisation?

Schnellreferenz für häufige Arbeitssituationen

Situation	Häufig beteiligte Practices
Service ist ausgefallen	Incident Management, Service Desk, Monitoring and Event Management
Fehler tritt wiederholt auf	Problem Management, Knowledge Management, Continual Improvement
Benutzer benötigt Standardsoftware	Service Request Management, IT Asset Management, Service Desk
System soll aktualisiert werden	Change Enablement, Release Management, Deployment Management
Abhängigkeiten sind unklar	Service Configuration Management, Architecture Management
Hardware oder Lizenz muss verwaltet werden	IT Asset Management, Supplier Management, Service Financial Management
Sicherheitsrisiko wurde erkannt	Information Security Management, Risk Management, Change Enablement
Anbieterleistung ist unzureichend	Supplier Management, Service Level Management, Relationship Management
neue Anwendung wird eingeführt	Service Design, Business Analysis, Architecture Management, Project Management
Service muss nach Katastrophe wiederhergestellt werden	Service Continuity Management, Incident Management, Availability Management
Leistung reicht nicht aus	Capacity and Performance Management, Availability Management
Benutzer verstehen den Service nicht	Service Catalogue Management, Knowledge Management, Relationship Management
Arbeitsweise soll verbessert werden	Continual Improvement, Measurement and Reporting
neues Team oder neue Arbeitsweise wird eingeführt	Organizational Change Management, Workforce and Talent Management

Zusammenfassende Darstellung



Bedarf oder Chance



gewünschtes Outcome und Value Stream bestimmen



benötigte Management Practices auswählen



Menschen · Informationen · Prozesse · Technologie · Partner verbinden



Arbeit durchführen und Ergebnisse messen



Feedback und Erkenntnisse auswerten



Practices und Wertströme kontinuierlich verbessern

Verwandte Seiten

- 2.1 Was ist ITIL und wie ist das Framework aufgebaut?
- 2.2 Das ITIL Value System
- 2.3 Die sieben Guiding Principles
- 2.4 Governance und Verantwortlichkeit
- 2.5 Die vier Dimensionen des Produkt- und Service-Managements
- 2.6 Der Product and Service Lifecycle
- 2.8 Value Streams und Value Stream Mapping
- 2.9 Continual Improvement
- 2.10 ITIL an den eigenen Kontext anpassen
- Service Desk
- Incident Management
- Service Request Management
- Problem Management
- Change Enablement
- Monitoring and Event Management
- Knowledge Management
- Service Configuration Management
- IT Asset Management

Quellen und Versionsstand

Offizielle Grundlagen

- [PeopleCert: ITIL Foundation – Version 5](#)
- [ITIL: ITIL Foundation – Version 5](#)
- [ITIL: New ITIL Explained for Certified Professionals](#)

- [PeopleCert: Frequently Asked Questions about ITIL](#)
- [ITIL: ITIL Foundation Version 5 – What’s New?](#)
- [PeopleCert: ITIL 4 Management Practices 2023](#)
- [PeopleCert: ITIL Practice Guides – A Hidden Gem](#)
- [ITIL: PeopleCert Plus](#)

Offiziell bestätigter Stand

Die offiziellen aktuellen ITIL-Version-5-Informationen bestätigen:

- ITIL Version 5 führt weiterhin 34 Management Practices.
- Die Practices bleiben gegenüber ITIL 4 weitgehend erhalten.
- Anpassungen erfolgen zur Ausrichtung auf die neuen ITIL-Version-5-Inhalte.
- Die 34 Practices werden in zwei Gruppen organisiert:
 - Product and Service Management Practices
 - General Management Practices
- Die vollständigen Practice Guides werden über PeopleCert Plus bereitgestellt.
- Die Practice-Manager-Bündel enthalten jeweils fünf ausgewählte Practices.

Hinweis zur Practice-Bezeichnung

Die aktuelle offizielle Beschreibung des Practice-Manager-Moduls **Plan, Implement and Control** verwendet weiterhin die Bezeichnung **Change Enablement**.

Deshalb wird diese Practice auf dieser Seite nicht ohne eindeutigen offiziellen Nachweis in **Change Management** umbenannt.

Einordnung

Die alphabetische Übersicht, deutschen Kurzbeschreibungen, Vergleiche, Praxisbeispiele, Checklisten und Arbeitssituationen sind eigene herstellerneutrale Erläuterungen dieses unabhängigen Nachschlagewerks.

Sie stellen keine wörtlichen offiziellen ITIL-Definitionen und keine für jede Organisation vorgeschriebenen Prozesse dar.

Die konkrete Gestaltung, Priorisierung und Ausprägung einer Practice muss an Ziele, Risiken, Fähigkeiten und Wertströme der jeweiligen Organisation angepasst werden.

Behandelter Framework-Stand: ITIL Version 5

Zusätzlich berücksichtigt: ITIL 4

Fachlicher Stand: August 2026
