

2.5 Die vier Dimensionen des Produkt- und Service-Managements

“ Kurz erklärt

Die vier Dimensionen unterstützen eine ganzheitliche Betrachtung digitaler Produkte und Services.

Sie helfen dabei, nicht ausschließlich auf Technik, Prozesse oder einzelne Teams zu schauen.

Die vier Dimensionen sind:

1. **Organizations and People** – Organisationen und Menschen
2. **Information and Technology** – Informationen und Technologie
3. **Partners and Suppliers** – Partner und Lieferanten
4. **Value Streams and Processes** – Wertströme und Prozesse

Bei Entscheidungen, Änderungen, Störungen und Verbesserungen sollten alle vier Dimensionen berücksichtigt werden.

Warum die vier Dimensionen notwendig sind

Digitale Produkte und Services entstehen durch das Zusammenwirken unterschiedlicher Bestandteile.

Dazu gehören beispielsweise:

- Menschen,
- Rollen,
- Wissen,
- Informationen,
- Anwendungen,
- Infrastruktur,
- Prozesse,
- Wertströme,
- Lieferanten,
- Verträge,
- Sicherheitsanforderungen,
- und organisatorische Entscheidungen.

Eine technische Lösung kann leistungsfähig sein und trotzdem keinen ausreichenden Wert ermöglichen.

Beispiele:

- Eine Anwendung funktioniert, aber niemand ist für ihren Support verantwortlich.
- Ein Monitoring-System erkennt Fehler, aber Warnungen werden nicht bearbeitet.
- Ein Cloud-Service ist verfügbar, aber der Vertrag enthält keine geeignete Ausstiegsregelung.
- Ein Prozess ist ausführlich dokumentiert, wird aber von den Mitarbeitern nicht verstanden.
- Eine neue Plattform besitzt viele Funktionen, lässt sich aber nicht in die vorhandene Umgebung integrieren.
- Ein Service erfüllt technische Messwerte, unterstützt aber das benötigte Outcome nicht.

Die vier Dimensionen helfen dabei, solche Lücken frühzeitig zu erkennen.

“ Merke

Ein Produkt oder Service ist nur so wirksam wie das Zusammenspiel seiner organisatorischen, technischen, menschlichen und externen Bestandteile.

Die vier Dimensionen im Überblick

Dimension	Zentrale Betrachtung
Organizations and People	Rollen, Fähigkeiten, Kapazitäten, Kommunikation, Kultur und Organisationsstruktur
Information and Technology	Informationen, Wissen, Daten, Anwendungen, Infrastruktur, Integration und Automatisierung
Partners and Suppliers	externe Leistungen, Lieferantenbeziehungen, Verträge, Abhängigkeiten und Zusammenarbeit
Value Streams and Processes	Ende-zu-Ende-Arbeitsfluss, Aktivitäten, Übergaben, Kontrollen und Ergebnisse

Die Dimensionen sind keine voneinander getrennten Bereiche.

Eine Entscheidung in einer Dimension beeinflusst häufig auch die anderen drei Dimensionen.

Die Dimensionen sind Betrachtungsperspektiven

Die vier Dimensionen sind:

- keine vier Abteilungen,

- keine vier aufeinanderfolgenden Prozessschritte,
- keine vier Reifegrade,
- und keine voneinander unabhängigen Managementsysteme.

Sie dienen als Perspektiven, mit denen ein Produkt, Service, Wertstrom, Problem oder Vorhaben untersucht werden kann.

Beispiel:

Eine Organisation führt eine neue Plattform für die zentrale Dateiablage ein.

Organizations and People

- Wer verwaltet die Plattform?
- Wer unterstützt die Benutzer?
- Welche Fähigkeiten werden benötigt?
- Wer genehmigt Zugriffe?

Information and Technology

- Welche Daten werden gespeichert?
- Wie werden Berechtigungen technisch umgesetzt?
- Welche Schnittstellen bestehen?
- Wie werden Backup und Wiederherstellung realisiert?

Partners and Suppliers

- Wird ein Cloud-Anbieter verwendet?
- Welche Leistungen werden vertraglich zugesichert?
- Wie werden Störungen eskaliert?
- Wie können Daten bei Vertragsende exportiert werden?

Value Streams and Processes

- Wie werden neue Zugriffe beantragt?
- Wie werden Freigaben erteilt?
- Wie werden Berechtigungen entfernt?
- Wie werden Incidents und Service Requests bearbeitet?

Erst die gemeinsame Betrachtung ergibt ein vollständigeres Bild.

Nicht jede Dimension benötigt immer denselben Aufwand

Alle vier Dimensionen sollten berücksichtigt werden.

Das bedeutet jedoch nicht, dass sie bei jeder Aufgabe gleich ausführlich dokumentiert werden müssen.

Beispiel:

Bei einer einfachen, dokumentierten Standardtätigkeit kann eine kurze Prüfung ausreichen.

Bei der Einführung einer geschäftskritischen Cloud-Plattform kann dagegen eine umfangreiche Betrachtung notwendig sein.

Der erforderliche Umfang hängt unter anderem ab von:

- Bedeutung des betroffenen Produkts oder Service,
- Anzahl der betroffenen Stakeholder,
- Risiko,
- Komplexität,
- gesetzlichen und vertraglichen Anforderungen,
- Sicherheitsanforderungen,
- Neuartigkeit der Lösung,
- Lieferantenabhängigkeit,
- und möglicher Auswirkung eines Fehlers.

“ Grundsatz

Alle vier Dimensionen berücksichtigen, aber den Prüf- und Dokumentationsaufwand an Risiko und Kontext anpassen.

1. Organizations and People

Die Dimension **Organizations and People** betrachtet die organisatorischen und menschlichen Voraussetzungen für wirksames Produkt- und Service-Management.

Dazu gehören unter anderem:

- Organisationsstruktur,
- Rollen,
- Verantwortlichkeiten,
- Entscheidungsbefugnisse,
- Fähigkeiten,
- Kompetenzen,
- Personalkapazität,
- Kommunikation,
- Zusammenarbeit,
- Führung,

- Kultur,
- Motivation,
- und gemeinsame Werte.

Technische Systeme werden von Menschen:

- geplant,
- entwickelt,
- beschafft,
- konfiguriert,
- betrieben,
- unterstützt,
- überwacht,
- verwendet,
- und verbessert.

Eine technisch geeignete Lösung kann deshalb scheitern, wenn die menschlichen und organisatorischen Voraussetzungen fehlen.

Organisationen sind mehr als Organigramme

Ein Organigramm zeigt formale Strukturen.

Es beantwortet jedoch nicht automatisch:

- Wie werden Entscheidungen tatsächlich getroffen?
- Wer besitzt notwendiges Fachwissen?
- Wer übernimmt bei einem Incident die Koordination?
- Wie arbeiten Teams miteinander?
- Welche informellen Abhängigkeiten bestehen?
- Wo entstehen Konflikte oder Verzögerungen?
- Können Mitarbeiter Probleme offen ansprechen?
- Werden Erfahrungen und Fehler für Verbesserungen genutzt?

Für die Bewertung dieser Dimension müssen deshalb sowohl formale als auch tatsächlich gelebte Arbeitsweisen betrachtet werden.

“ Typischer Fehler

Eine Rolle ist im Organigramm eingetragen, besitzt aber weder ausreichende Befugnisse noch Zeit, Informationen oder Ressourcen, um ihre Verantwortung wahrzunehmen.

Rollen und Verantwortlichkeiten

Für wichtige Produkte, Services und Tätigkeiten sollte geklärt sein:

- Wer entscheidet?
- Wer führt die Tätigkeit aus?
- Wer steht für das Ergebnis ein?
- Wer muss fachlich beteiligt werden?
- Wer muss informiert werden?
- Wer darf Risiken akzeptieren?
- Wer koordiniert bei Störungen?
- Wer pflegt Dokumentationen?
- Wer treibt Verbesserungen voran?

Mögliche Rollen sind beispielsweise:

- Product Owner,
- Product Manager,
- Service Owner,
- Service Manager,
- Systemadministrator,
- Netzwerkadministrator,
- Service-Desk-Mitarbeiter,
- Information Owner,
- Supplier Manager,
- Informationssicherheitsverantwortlicher,
- und Change-Verantwortlicher.

ITIL schreibt nicht vor, dass jede Organisation genau diese Rollenbezeichnungen verwenden muss.

Entscheidend ist, dass Verantwortung, Befugnis und erwartetes Ergebnis eindeutig sind.

Fähigkeiten und Kompetenzen

Eine Organisation benötigt nicht nur ausreichend Personal, sondern auch geeignete Fähigkeiten.

Dazu können gehören:

- technisches Fachwissen,
- Produktwissen,
- Serviceverständnis,
- Fehleranalyse,
- Kommunikation,
- Risikobewertung,
- Dokumentation,
- Lieferantensteuerung,

- Informationssicherheit,
- Automatisierung,
- Datenanalyse,
- und Entscheidungsfähigkeit.

Bei einer neuen Technologie sollte deshalb nicht nur geprüft werden:

“ Kann das Produkt beschafft oder installiert werden?

Zusätzlich ist zu prüfen:

- Wer kann es betreiben?
- Wer kann Fehler analysieren?
- Wer kann die Sicherheit bewerten?
- Wer übernimmt Bereitschaft und Support?
- Wie wird Wissen aufgebaut?
- Wie wird Wissen bei Personalwechsel erhalten?
- Welche Fähigkeiten müssen intern vorhanden bleiben?
- Welche Fähigkeiten können extern bezogen werden?

“ **Merke**

Eine Organisation besitzt eine Fähigkeit nicht allein deshalb, weil sie ein Werkzeug gekauft hat.

Kapazität und Arbeitsbelastung

Auch fachlich geeignete Mitarbeiter können ihre Aufgaben nicht wirksam erfüllen, wenn ausreichende Kapazität fehlt.

Anzeichen für Kapazitätsprobleme können sein:

- Tickets bleiben lange unbearbeitet.
- Dokumentationen werden dauerhaft verschoben.
- Wartungsarbeiten finden nicht statt.
- Verbesserungen werden immer wieder abgebrochen.
- Mitarbeiter reagieren nur noch auf akute Störungen.
- Wissen konzentriert sich auf einzelne Personen.
- Vertretungen fehlen.
- Bereitschaftsdienste sind dauerhaft überlastet.
- Sicherheitsmaßnahmen werden aus Zeitmangel nicht umgesetzt.

Kapazität sollte deshalb nicht nur anhand der Anzahl von Mitarbeitern bewertet werden.

Zu berücksichtigen sind außerdem:

- benötigte Fähigkeiten,
- Arbeitsmenge,
- Komplexität,
- Automatisierungsgrad,
- Servicezeiten,
- Bereitschaftsanforderungen,
- Urlaubs- und Krankheitsvertretung,
- und ungeplante Arbeit.

Kommunikation und Zusammenarbeit

Digitale Produkte und Services überschreiten häufig Team- und Organisationsgrenzen.

Eine wirksame Zusammenarbeit benötigt:

- gemeinsame Ziele,
- verständliche Begriffe,
- geeignete Kommunikationswege,
- sichtbare Zuständigkeiten,
- aktuelle Informationen,
- nachvollziehbare Entscheidungen,
- und funktionierende Eskalationswege.

Mögliche Kommunikationsprobleme sind:

- Teams verwenden dieselben Begriffe mit unterschiedlicher Bedeutung.
- Informationen werden nur in privaten Chats weitergegeben.
- technische Änderungen werden dem Service Desk nicht mitgeteilt.
- Lieferanten erhalten unvollständige Fehlerbeschreibungen.
- Benutzer bekommen widersprüchliche Statusmeldungen.
- Entscheidungen werden nicht dokumentiert.
- Wissen wird erst weitergegeben, wenn eine Schlüsselperson ausfällt.

“ Praxistipp

Die Qualität der Zusammenarbeit zeigt sich besonders an Übergaben, Störungen und Änderungen.

Organisationskultur

Kultur beeinflusst, wie Menschen tatsächlich handeln.

Sie zeigt sich beispielsweise darin:

- ob Fehler offen gemeldet werden,
- ob Risiken angesprochen werden dürfen,
- ob Teams Wissen teilen,
- ob Verantwortlichkeiten übernommen werden,
- ob Probleme nur einzelnen Personen zugeschrieben werden,
- ob Benutzerfeedback ernst genommen wird,
- und ob Verbesserungen dauerhaft unterstützt werden.

Eine Organisation kann offiziell Zusammenarbeit fördern und gleichzeitig durch ihre tatsächliche Arbeitsweise Konkurrenz zwischen Teams erzeugen.

Beispiel:

Teams werden ausschließlich nach ihrer eigenen Bearbeitungszeit bewertet.

Dadurch kann jedes Team versuchen, Vorgänge möglichst schnell weiterzugeben.

Die lokale Kennzahl verbessert sich, während sich die gesamte Bearbeitungsdauer für den Benutzer verlängert.

Leitfragen zu Organizations and People

- Sind Rollen und Verantwortlichkeiten eindeutig?
- Besitzen die Rollen ausreichende Befugnisse?
- Sind notwendige Fähigkeiten vorhanden?
- Gibt es ausreichende Kapazität?
- Wie werden Wissen und Erfahrung weitergegeben?
- Funktionieren Vertretungen?
- Sind Kommunikations- und Eskalationswege bekannt?
- Unterstützt die Organisationskultur Zusammenarbeit?
- Werden Mitarbeiter bei Veränderungen angemessen einbezogen?
- Verstehen die Beteiligten das angestrebte Outcome?
- Sind Anreize und Kennzahlen auf den gesamten Wertstrom ausgerichtet?
- Können Probleme und Risiken offen angesprochen werden?

2. Information and Technology

Die Dimension **Information and Technology** betrachtet die Informationen, das Wissen und die Technologien, die für Produkte und Services benötigt werden.

Dazu gehören beispielsweise:

- Daten,
- Dokumentationen,
- Wissen,
- Anwendungen,
- Infrastruktur,
- Netzwerke,
- Cloud-Plattformen,
- Datenbanken,
- Schnittstellen,
- Automatisierung,
- Monitoring,
- Kommunikationssysteme,
- Sicherheitswerkzeuge,
- und künstliche Intelligenz.

Informationen und Technologie unterstützen nahezu jede Tätigkeit im digitalen Produkt- und Service-Management.

Sie müssen jedoch zu den tatsächlichen Anforderungen und Fähigkeiten der Organisation passen.

Informationen als Arbeitsgrundlage

Geeignete Entscheidungen benötigen geeignete Informationen.

Beispiele:

- Ein Incident benötigt Angaben zu Auswirkungen, Symptomen und betroffenen Services.
- Ein Change benötigt Informationen zu Risiken, Abhängigkeiten und Rückfallmöglichkeiten.
- Ein Service Owner benötigt Informationen über Leistung, Erfahrung und Risiken.
- Ein Administrator benötigt aktuelle Konfigurationsinformationen.
- Ein Lieferantenmanager benötigt Informationen über vereinbarte und tatsächlich erbrachte Leistungen.
- Governance benötigt Informationen über Outcomes, Risiken und Regelkonformität.

Informationen sollten möglichst:

- korrekt,
- aktuell,
- vollständig genug,
- verständlich,
- verfügbar,
- geschützt,
- nachvollziehbar,
- und für den jeweiligen Zweck geeignet

sein.



Wichtig

Mehr Daten bedeuten nicht automatisch bessere Informationen.

Entscheidend ist, ob die Daten verständlich, zuverlässig und für eine konkrete Entscheidung nutzbar sind.

Datenqualität

Fehlerhafte oder veraltete Daten können zu falschen Entscheidungen führen.

Beispiele:

- Ein ausgeschiedener Mitarbeiter besitzt weiterhin aktive Berechtigungen.
- Eine CMDB enthält nicht mehr vorhandene Server.
- Ein Servicekatalog nennt einen nicht mehr verantwortlichen Service Owner.
- Ein Monitoring-System verwendet veraltete Schwellenwerte.
- Eine Knowledge-Base beschreibt eine frühere Softwareversion.
- Ein Asset-System enthält doppelte oder unvollständige Geräteinformationen.

Datenqualität sollte deshalb nicht nur bei der Erfassung, sondern über den gesamten Lebenszyklus betrachtet werden.

Zu klären ist:

- Wer erzeugt die Daten?
- Wer verwendet sie?
- Wer ist für ihre Qualität verantwortlich?
- Wann werden sie aktualisiert?
- Wie werden Fehler erkannt?
- Wann werden sie archiviert oder gelöscht?
- Welche Quelle gilt als maßgeblich?

Information und Wissen unterscheiden

Informationen werden erst durch Einordnung und Erfahrung zu anwendbarem Wissen.

Beispiel:

Information

“ Der Dienst wurde innerhalb von drei Monaten zwölfmal neu gestartet.

Wissen

“ Die Neustarts treten regelmäßig nach einem bestimmten Speicheranstieg auf und stellen nur eine vorübergehende Wiederherstellung dar.

Anwendbare Erkenntnis

“ Die Ursache muss untersucht und eine dauerhafte Korrektur geplant werden.

Knowledge Management soll dabei helfen, relevante Informationen:

- zu erfassen,
- zu bewerten,
- zu strukturieren,
- auffindbar zu machen,
- zu verwenden,
- und aktuell zu halten.

Technologieauswahl

Eine Technologie sollte nicht nur anhand ihrer Funktionen bewertet werden.

Zu berücksichtigen sind beispielsweise:

- benötigte Outcomes,
 - Kompatibilität,
 - Integrationen,
 - Skalierbarkeit,
 - Verfügbarkeit,
 - Sicherheit,
 - Datenschutz,
 - Bedienbarkeit,
 - Wartbarkeit,
 - Support,
 - Kosten,
 - Fähigkeiten der Mitarbeiter,
 - Lieferantenabhängigkeit,
 - Datenportabilität,
 - und Ablösung am Lebensende.
-

Typischer Fehler

Eine neue Technologie wird eingeführt, weil sie viele Funktionen besitzt.

Erst später wird festgestellt, dass sie nicht zu vorhandenen Arbeitsweisen, Fähigkeiten oder Schnittstellen passt.

Architektur und Integration

Digitale Produkte und Services bestehen häufig aus mehreren integrierten Systemen.

Zu berücksichtigen sind:

- Datenflüsse,
- APIs,
- Protokolle,
- Identitäten,
- Berechtigungen,
- Abhängigkeiten,
- Schnittstellen,
- Ausfallszenarien,
- und Versionskompatibilität.

Beispiel:

Eine Anwendung kann technisch verfügbar sein, aber nicht nutzbar, wenn:

- der Identitätsanbieter gestört ist,
- DNS-Einträge fehlen,
- ein Zertifikat abgelaufen ist,
- eine API nicht erreichbar ist,
- oder eine benötigte Lizenz nicht zugeordnet wurde.

Eine ganzheitliche Betrachtung erfordert deshalb Informationen über Ende-zu-Ende-Abhängigkeiten.

Informationssicherheit

Informationen und Technologien müssen angemessen geschützt werden.

Zu den grundlegenden Schutzzielen gehören insbesondere:

- Vertraulichkeit,
- Integrität,

- Verfügbarkeit.

Je nach Kontext können außerdem relevant sein:

- Authentizität,
- Nachvollziehbarkeit,
- Datenschutz,
- Beweissicherheit,
- und Widerstandsfähigkeit.

Bei technischen Entscheidungen sollte geprüft werden:

- Welche Informationen werden verarbeitet?
 - Welchen Schutzbedarf besitzen sie?
 - Wer darf darauf zugreifen?
 - Wie werden Zugriffe kontrolliert?
 - Wie werden Daten übertragen und gespeichert?
 - Welche Protokollierung ist notwendig?
 - Wie werden Daten gesichert und wiederhergestellt?
 - Wann müssen Daten gelöscht werden?
 - Welche Sicherheitsvorfälle sind möglich?
-

Automatisierung

Automatisierung kann:

- wiederkehrende Arbeit reduzieren,
- Ergebnisse vereinheitlichen,
- Fehler verringern,
- Geschwindigkeit erhöhen,
- und Skalierbarkeit verbessern.

Sie benötigt jedoch:

- einen verstandenen Ablauf,
- geeignete Eingabedaten,
- klare Regeln,
- Fehlerbehandlung,
- Überwachung,
- Verantwortlichkeit,
- und eine Rückfallmöglichkeit.

Beispiel:

Eine automatisierte Benutzeranlage kann Konten, Lizenzen und Standardgruppen bereitstellen.

Die Automatisierung muss trotzdem klären:

- Liegt eine gültige Anforderung vor?
 - Wurde der Zugriff genehmigt?
 - Sind die Personaldaten vollständig?
 - Existiert bereits ein Konto?
 - Was geschieht bei einem Teilfehler?
 - Wer prüft das Ergebnis?
 - Wie werden Ausnahmen behandelt?
-

Künstliche Intelligenz

KI kann bei digitalen Produkten und Services unter anderem eingesetzt werden für:

- Klassifizierung,
- Zusammenfassung,
- Analyse,
- Suche,
- Mustererkennung,
- Prognosen,
- Vorschläge,
- Automatisierung,
- und Benutzerinteraktion.

Dabei müssen unter anderem betrachtet werden:

- Datenqualität,
- Datenschutz,
- Informationssicherheit,
- mögliche Verzerrungen,
- Nachvollziehbarkeit,
- Fehlerwahrscheinlichkeit,
- menschliche Kontrolle,
- Verantwortlichkeit,
- Anbieterabhängigkeit,
- und Überwachung der Ergebnisse.

“ Sicherheitsrelevant

Eine KI-generierte Antwort oder Entscheidung muss abhängig von ihrer möglichen Auswirkung angemessen geprüft werden.

Die Verantwortung verbleibt bei der Organisation und den zuständigen Rollen.

Technische Schulden

Technische Schulden entstehen, wenn kurzfristige Lösungen später zusätzlichen Aufwand oder Risiken verursachen.

Beispiele:

- nicht unterstützte Softwareversionen,
- manuelle Sonderkonfigurationen,
- fehlende Automatisierung,
- veraltete Schnittstellen,
- unzureichende Tests,
- fehlende Dokumentation,
- oder dauerhaft eingesetzte Zwischenlösungen.

Technische Schulden sind nicht automatisch vollständig vermeidbar.

Sie sollten jedoch:

- sichtbar,
- bewertet,
- priorisiert,
- verantwortet,
- und kontrolliert reduziert

werden.

Leitfragen zu Information and Technology

- Welche Informationen werden benötigt?
- Sind die Informationen korrekt, aktuell und geschützt?
- Wer ist für die Datenqualität verantwortlich?
- Welche Technologien unterstützen das Outcome?
- Passen die Technologien zur vorhandenen Architektur?
- Welche Integrationen und Abhängigkeiten bestehen?
- Sind Sicherheit und Datenschutz berücksichtigt?
- Sind Backup und Wiederherstellung vorbereitet?
- Besitzen Mitarbeiter die notwendigen Fähigkeiten?
- Welche Tätigkeiten können sinnvoll automatisiert werden?
- Wie werden automatisierte oder KI-gestützte Ergebnisse kontrolliert?
- Welche technischen Schulden bestehen?
- Wie werden Systeme am Ende ihres Lebenszyklus abgelöst?

3. Partners and Suppliers

Die Dimension **Partners and Suppliers** betrachtet externe Organisationen und Personen, die an Produkten, Services oder Wertströmen beteiligt sind.

Dazu können gehören:

- Hardwarehersteller,
- Softwareanbieter,
- Cloud-Provider,
- Telekommunikationsanbieter,
- Beratungsunternehmen,
- Managed Service Provider,
- Logistikunternehmen,
- Wartungsdienstleister,
- Schulungsanbieter,
- und Unterauftragnehmer.

Viele Organisationen können digitale Produkte und Services nicht vollständig allein bereitstellen.

Externe Partner können:

- Technologien,
- Fachwissen,
- Kapazitäten,
- Infrastruktur,
- Support,
- Lizenzen,
- oder vollständige Servicebestandteile

bereitstellen.

Partner und Lieferant unterscheiden

Die Begriffe können in Organisationen unterschiedlich verwendet werden.

Vereinfacht kann unterschieden werden:

Begriff	Mögliche Bedeutung
Lieferant	stellt vertraglich vereinbarte Produkte oder Leistungen bereit
Partner	arbeitet enger und möglicherweise längerfristig an gemeinsamen Outcomes mit

Ein Lieferant kann gleichzeitig ein strategischer Partner sein.

Entscheidend ist nicht nur die Bezeichnung, sondern:

- welche Leistung erbracht wird,
 - welche Verantwortung besteht,
 - welche Abhängigkeit entsteht,
 - wie eng zusammengearbeitet wird,
 - und wie die Beziehung gesteuert wird.
-

Sourcing-Entscheidungen

Organisationen müssen entscheiden, welche Fähigkeiten und Leistungen sie:

- intern aufbauen,
- extern beschaffen,
- gemeinsam mit Partnern erbringen,
- oder vollständig als externen Service nutzen.

Mögliche Kriterien sind:

- strategische Bedeutung,
- vorhandene Fähigkeiten,
- Kosten,
- Geschwindigkeit,
- Flexibilität,
- Skalierbarkeit,
- Sicherheitsanforderungen,
- gesetzliche Anforderungen,
- Kontrollbedarf,
- Verfügbarkeit geeigneter Anbieter,
- und Abhängigkeiten.

“ Typischer Fehler

Eine Tätigkeit wird ausschließlich wegen kurzfristig geringerer Kosten ausgelagert.

Langfristige Abhängigkeiten, Datenportabilität, interne Fähigkeiten und Ausstiegskosten werden nicht berücksichtigt.

Verträge und Vereinbarungen

Verträge und Vereinbarungen sollten die benötigten Outcomes unterstützen.

Mögliche Inhalte sind:

- Leistungsumfang,
- Verantwortlichkeiten,
- Servicezeiten,
- Qualitätsziele,
- Sicherheitsanforderungen,
- Datenschutz,
- Eskalationswege,
- Support,
- Meldepflichten,
- Wartungsbedingungen,
- Datenstandort,
- Unterauftragnehmer,
- Auditmöglichkeiten,
- Haftung,
- Vertragsänderungen,
- Kündigung,
- Datenrückgabe,
- und Übergangsunterstützung.

Eine vertraglich zugesicherte technische Verfügbarkeit beantwortet nicht automatisch:

- wie gut der Support funktioniert,
- wie schnell ein kritischer Incident koordiniert wird,
- wie Daten zurückgeführt werden,
- oder ob der Service das benötigte Outcome ermöglicht.

Lieferantenabhängigkeiten

Externe Abhängigkeiten sollten sichtbar und bewertet sein.

Mögliche Risiken sind:

- Ausfall eines einzelnen Anbieters,
- fehlende alternative Anbieter,
- proprietäre Datenformate,
- schwer ersetzbare Schnittstellen,
- Preissteigerungen,
- Vertragsänderungen,
- fehlende interne Kenntnisse,
- eingeschränkte Datenportabilität,
- nicht kontrollierte Unterauftragnehmer,
- und lange Migrationszeiten.

Besonders kritisch kann eine Konzentration entstehen, wenn viele Produkte und Services von demselben Anbieter abhängen.

Beispiel:

Ein einziger Cloud-Anbieter stellt bereit:

- Identitätsdienst,
- E-Mail,
- Dateiablage,
- Kollaborationsplattform,
- Gerätemanagement,
- und Sicherheitsfunktionen.

Ein Ausfall oder Vertragsproblem kann dann mehrere zentrale Services gleichzeitig beeinflussen.

Geteilte Verantwortung

Bei extern bereitgestellten Services bleiben Verantwortlichkeiten häufig zwischen Anbieter und Kunde aufgeteilt.

Beispiel: Cloud-Service

Der Anbieter kann verantwortlich sein für:

- Betrieb der Plattform,
- physische Infrastruktur,
- bestimmte Sicherheitsmaßnahmen,
- und zugesicherte Verfügbarkeit.

Die nutzende Organisation kann weiterhin verantwortlich sein für:

- Benutzerkonten,
- Berechtigungen,
- Konfiguration,
- Datenklassifizierung,
- Endgeräte,
- sichere Nutzung,
- und eigene Backups oder Exporte.

Die genaue Aufteilung hängt vom jeweiligen Produkt, Vertrag und Bereitstellungsmodell ab.

“ Merke

Eine ausgelagerte Tätigkeit bedeutet nicht automatisch, dass alle Risiken und Verantwortlichkeiten auf den Anbieter übergehen.

Lieferanten in Incidents

Bei einem Incident sollte geklärt sein:

- Welcher Lieferant ist betroffen?
- Welche Vertrags- oder Supportnummer wird benötigt?
- Wer darf den Lieferanten kontaktieren?
- Welche Informationen müssen übermittelt werden?
- Welche Prioritätsstufen verwendet der Lieferant?
- Welche Reaktions- und Lösungsziele gelten?
- Wie erfolgt die Eskalation?
- Wer koordiniert intern weiter?
- Wie werden Benutzer informiert?
- Wie werden Beweise und Protokolle gesichert?

Eine Supportanfrage an einen Lieferanten ersetzt nicht die interne Verantwortung für:

- Koordination,
- Kommunikation,
- Risikobewertung,
- und Überprüfung des gesamten Service.

Ausstiegs- und Übergangsplanung

Bereits bei der Auswahl eines Lieferanten sollte betrachtet werden, wie die Beziehung später verändert oder beendet werden kann.

Zu prüfen sind:

- Können Daten vollständig exportiert werden?
- In welchem Format werden Daten bereitgestellt?
- Wie lange dauert eine Migration?
- Welche technische Unterstützung wird angeboten?
- Was geschieht mit Sicherungskopien?
- Wie werden Zugänge entfernt?
- Welche Dokumentationen werden übergeben?
- Welche internen Fähigkeiten müssen erhalten bleiben?
- Welche Kosten entstehen beim Ausstieg?
- Wie wird ein unterbrechungsarmer Übergang ermöglicht?

“ Praxistipp

Eine Exit-Strategie sollte nicht erst entwickelt werden, wenn der Vertrag bereits beendet werden muss.

Leitfragen zu Partners and Suppliers

- Welche externen Partner sind beteiligt?
- Welche Leistungen stellen sie bereit?
- Welche Produkte und Services hängen davon ab?
- Sind Verantwortlichkeiten eindeutig geregelt?
- Passen Verträge zu den benötigten Outcomes?
- Welche Sicherheits- und Datenschutzerfordernungen gelten?
- Werden Unterauftragnehmer eingesetzt?
- Wie wird die Lieferantenleistung überwacht?
- Welche Eskalationswege bestehen?
- Welche Konzentrations- und Ausfallrisiken bestehen?
- Welche internen Fähigkeiten müssen erhalten bleiben?
- Können Daten und Leistungen zu einem anderen Anbieter übertragen werden?
- Gibt es eine geeignete Ausstiegs- und Übergangsplanung?

4. Value Streams and Processes

Die Dimension **Value Streams and Processes** betrachtet, wie Arbeit durch die Organisation fließt und wie Aktivitäten zu Ergebnissen und Wert beitragen.

Dazu gehören:

- Wertströme,
- Prozesse,
- Aktivitäten,
- Eingaben,
- Ergebnisse,
- Rollen,
- Übergaben,
- Entscheidungen,
- Kontrollen,
- Messgrößen,
- und Rückmeldungen.

Einzelne Teams können ihre Aufgaben gut erfüllen und trotzdem einen schlechten Ende-zu-Ende-Arbeitsfluss erzeugen.

Die Dimension richtet den Blick deshalb nicht nur auf einzelne Prozessschritte, sondern auf den gesamten Weg zum benötigten Outcome.

Value Stream

Ein Value Stream beschreibt eine Abfolge von Schritten, durch die Wert für einen Stakeholder ermöglicht wird.

Beispiele:

- neuen Mitarbeiter arbeitsfähig machen,
- einen Incident bearbeiten,
- eine Anwendung bereitstellen,
- einen Zugriff genehmigen,
- eine Schwachstelle beheben,
- einen Service verbessern,
- oder einen Lieferanten ablösen.

Ein Value Stream kann mehrere:

- Teams,
- Practices,
- Technologien,
- Prozesse,
- Lieferanten,
- und organisatorische Bereiche

verbinden.

“ Merke

Ein Wertstrom folgt dem Weg zum Outcome und nicht automatisch der Struktur des Organigramms.

Prozess

Ein Prozess ist eine strukturierte Folge miteinander verbundener Aktivitäten.

Er überführt bestimmte Eingaben in Ergebnisse.

Ein Prozess kann beispielsweise festlegen:

- welche Informationen benötigt werden,
- welche Schritte durchgeführt werden,
- wer beteiligt ist,
- welche Entscheidungen notwendig sind,
- und wie das Ergebnis kontrolliert wird.

Ein Value Stream kann mehrere Prozesse enthalten.

Ein Prozess kann wiederum in mehreren Value Streams verwendet werden.

Beispiel:

Der Prozess zur Benutzerkontoanlage kann Bestandteil sein von:

- Mitarbeiter-Onboarding,
- Bereitstellung eines zusätzlichen Zugriffs,
- Wechsel der Abteilung,
- und Wiederherstellung eines irrtümlich entfernten Kontos.

Ende-zu-Ende-Sicht

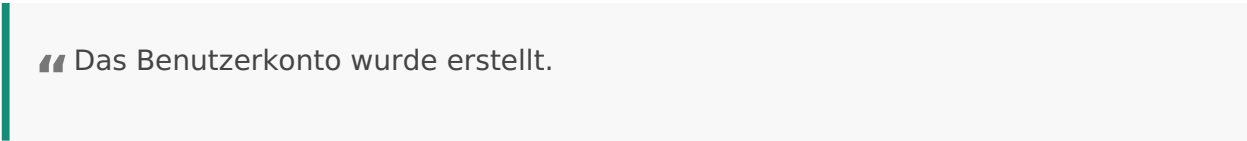
Eine Ende-zu-Ende-Betrachtung prüft den gesamten Weg vom Bedarf bis zum erreichten Outcome.

Beispiel: neuer Mitarbeiter

1. Eintritt wird gemeldet.
2. Aufgaben und benötigte Zugriffe werden bestimmt.
3. Freigaben werden eingeholt.
4. Benutzerkonto wird erstellt.
5. Lizenzen werden zugewiesen.
6. Endgerät wird bereitgestellt.
7. Sicherheitsmaßnahmen werden eingerichtet.
8. Zugriffe werden getestet.
9. Arbeitsplatz wird übergeben.
10. Arbeitsfähigkeit wird bestätigt.

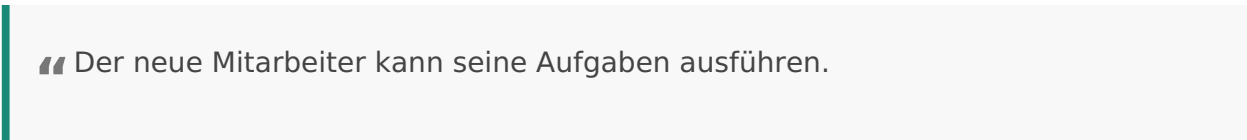
Wird nur die Kontoanlage betrachtet, können andere notwendige Schritte übersehen werden.

Der technische Output:



“ Das Benutzerkonto wurde erstellt.

bedeutet noch nicht automatisch das Outcome:



“ Der neue Mitarbeiter kann seine Aufgaben ausführen.

Übergaben

An Übergaben entstehen häufig:

- Wartezeiten,
- Informationsverluste,
- Missverständnisse,
- doppelte Arbeit,
- und unklare Verantwortlichkeiten.

Beispiele:

- Die Personalabteilung meldet einen Eintritt ohne Funktionsbeschreibung.
- Der Service Desk weist ein Ticket ohne Diagnoseinformationen weiter.
- Ein Change wird umgesetzt, aber das Monitoring-Team wird nicht informiert.
- Ein Lieferant erklärt seine Komponente für funktionsfähig, obwohl der gesamte Service weiterhin gestört ist.
- Eine Lösung wird gefunden, aber nicht in der Wissensdatenbank dokumentiert.

Übergaben sollten deshalb geprüft werden auf:

- benötigte Informationen,
- eindeutige Verantwortung,
- erwartete Ergebnisse,
- Zeitpunkte,
- technische Schnittstellen,
- und Rückmeldungen.

Engpässe und Wartezeiten

Ein Value Stream kann durch Engpässe verlangsamt werden.

Mögliche Ursachen sind:

- fehlende Informationen,
- unklare Freigaben,
- begrenzte Fachkenntnisse,
- unnötige Genehmigungsstufen,
- manuelle Dateneingaben,
- technische Medienbrüche,
- überlastete Teams,
- oder Abhängigkeiten von einzelnen Personen.

Nicht jede lange Gesamtdauer entsteht durch langsame Ausführung.

Häufig besteht ein großer Teil aus Wartezeit.

Beispiel:

Schritt	Bearbeitungszeit	Wartezeit
---------	------------------	-----------

Anforderung prüfen	15 Minuten	1 Tag
Freigabe erteilen	5 Minuten	2 Tage
Konto erstellen	10 Minuten	4 Stunden
Zugriff testen	15 Minuten	1 Tag

Die tatsächliche Bearbeitungszeit beträgt weniger als eine Stunde.

Der gesamte Durchlauf dauert trotzdem mehrere Tage.

Kontrollen im Arbeitsfluss

Kontrollen können notwendig sein für:

- Sicherheit,
- Qualität,
- Risiko,
- Freigabe,
- Nachvollziehbarkeit,
- und gesetzliche Anforderungen.

Sie sollten jedoch einen klaren Zweck besitzen.

Zu prüfen ist:

- Welches Risiko behandelt die Kontrolle?
- Ist sie an der richtigen Stelle?
- Wird sie doppelt durchgeführt?
- Ist eine Automatisierung möglich?
- Passt ihr Umfang zum Risiko?
- Erzeugt sie unnötige Wartezeit?
- Werden Ergebnisse der Kontrolle verwendet?
- Kann sie umgangen werden?

“ Typischer Fehler

Zusätzliche Freigaben werden eingeführt, nachdem ein Fehler aufgetreten ist.

Später wird nicht mehr geprüft, ob sie das Risiko tatsächlich reduzieren oder nur den Arbeitsfluss verlangsamen.

Prozesse dürfen nicht zum Selbstzweck werden

Ein Prozess ist kein Wert an sich.

Er soll ein benötigtes Outcome unterstützen.

Anzeichen für einen ungeeigneten Prozess können sein:

- Mitarbeiter umgehen den offiziellen Ablauf regelmäßig.
 - Informationen werden mehrfach erfasst.
 - Pflichtfelder enthalten bedeutungslose Standardtexte.
 - Genehmigungen erfolgen ohne tatsächliche Prüfung.
 - der Ablauf ist nur wenigen Personen verständlich.
 - Ergebnisse werden nicht gemessen.
 - Ausnahmen werden häufiger als der Standardfall.
 - Benutzer müssen denselben Sachverhalt mehrfach erklären.
 - jeder Vorgang wird gleich behandelt, obwohl die Risiken unterschiedlich sind.
-

Messung von Wertströmen und Prozessen

Mögliche Messgrößen sind:

- Durchlaufzeit,
- Bearbeitungszeit,
- Wartezeit,
- Anzahl der Übergaben,
- Fehlerquote,
- Nacharbeit,
- Erfolgsquote,
- Abbruchquote,
- Benutzererfahrung,
- Kosten,
- und erreichte Outcomes.

Eine einzelne Kennzahl reicht häufig nicht aus.

Beispiel:

Eine kurze Ticketbearbeitungszeit kann positiv sein.

Sie kann aber auch entstehen, weil Tickets:

- voreilig geschlossen,
- an andere Teams weitergegeben,
- oder nur oberflächlich bearbeitet

werden.

Messgrößen sollten deshalb gemeinsam und im Kontext betrachtet werden.

Leitfragen zu Value Streams and Processes

- Welches Outcome soll erreicht werden?
- Wo beginnt und endet der Wertstrom?
- Welche Schritte sind tatsächlich notwendig?
- Welche Teams, Practices und Lieferanten sind beteiligt?
- Wo entstehen Übergaben?
- Welche Informationen werden benötigt?
- Wo entstehen Wartezeiten oder Nacharbeit?
- Welche Kontrollen sind notwendig?
- Welche Schritte erzeugen keinen erkennbaren Nutzen?
- Wo bestehen Engpässe?
- Welche Tätigkeiten können vereinheitlicht oder automatisiert werden?
- Wie wird der Erfolg aus Sicht der Stakeholder geprüft?
- Wie fließt Feedback in Verbesserungen ein?

Zusammenwirken der vier Dimensionen

Die vier Dimensionen beeinflussen sich gegenseitig.

Veränderung	Mögliche Auswirkungen auf andere Dimensionen
neues Ticketsystem	Schulungsbedarf, Rollen, Datenmigration, Lieferantenvertrag und angepasste Prozesse
Outsourcing des Service Desk	neue Schnittstellen, Verantwortlichkeiten, technische Zugänge und Eskalationswege
Automatisierung der Benutzeranlage	Datenqualität, Freigaben, Rollen, Sicherheitskontrollen und Prozessänderungen
Einführung einer Cloud-Plattform	neue Fähigkeiten, Verträge, Integrationen, Datenflüsse und Supportprozesse
Änderung eines Incident-Prozesses	Werkzeugkonfiguration, Schulung, Lieferanteneinbindung und neue Messgrößen
Einsatz von KI	Datenanforderungen, Governance, Kompetenzen, Lieferantenrisiken und Kontrollabläufe

„Merke

Eine Änderung in nur einer Dimension ist in der Praxis selten auf diese eine Dimension begrenzt.

Praxisbeispiel: Einführung eines neuen Ticketsystems

Eine Organisation möchte ihr bisheriges Ticketsystem ersetzen.

Organizations and People

- Welche Teams verwenden das System?
- Welche Rollen und Berechtigungen werden benötigt?
- Welche Schulungen sind notwendig?
- Wer administriert das System?
- Wer verantwortet Kategorien, Vorlagen und Automatisierungen?
- Wie werden Benutzer und Supportmitarbeiter einbezogen?

Information and Technology

- Welche Daten müssen übernommen werden?
- Welche Schnittstellen bestehen?
- Wie werden Identitäten und Berechtigungen integriert?
- Welche Sicherheits- und Datenschutzanforderungen gelten?
- Wie werden Backups, Protokollierung und Monitoring umgesetzt?
- Welche Automatisierungen werden benötigt?

Partners and Suppliers

- Welcher Anbieter stellt die Lösung bereit?
- Welche Support- und Verfügbarkeitsleistungen gelten?
- Wie werden Daten exportiert?
- Welche Unterauftragnehmer sind beteiligt?
- Wie erfolgen Eskalationen?
- Wie kann das System später abgelöst werden?

Value Streams and Processes

- Welche Vorgangsarten werden benötigt?
- Wie laufen Incident, Service Request, Problem und Change durch das System?
- Welche Pflichtinformationen sind sinnvoll?
- Wo bestehen heute unnötige Übergaben?
- Welche Abläufe sollen vereinfacht werden?
- Welche Kennzahlen werden benötigt?

Wird nur die Technologie ausgewählt, können die anderen drei Dimensionen später zu erheblichen Problemen führen.

Praxisbeispiel: wiederkehrender VPN-Ausfall

Mehrere Benutzer verlieren regelmäßig ihre VPN-Verbindung.

Organizations and People

- Wer koordiniert die Untersuchung?
- Besitzen Service Desk und Netzwerkteam ausreichendes Wissen?
- Sind Verantwortlichkeiten zwischen interner IT und Provider klar?

Information and Technology

- Welche Protokolle und Monitoring-Daten liegen vor?
- Welche VPN-Komponenten, Zertifikate und Identitätsdienste sind beteiligt?
- Sind die Daten für eine Ursachenanalyse ausreichend?

Partners and Suppliers

- Ist ein Internet- oder VPN-Provider beteiligt?
- Welche Support- und Eskalationswege gelten?
- Welche Nachweise benötigt der Provider?

Value Streams and Processes

- Werden ähnliche Incidents miteinander verknüpft?
- Wird Problem Management einbezogen?
- Wie werden Benutzer informiert?
- Wie wird eine dauerhafte Korrektur geplant und kontrolliert umgesetzt?

Eine rein technische Einzelbehandlung kann den Service kurzfristig wiederherstellen.

Die ganzheitliche Betrachtung unterstützt zusätzlich eine nachhaltige Verbesserung.

Praxisbeispiel: Backup und Wiederherstellung

Organizations and People

- Wer überwacht Sicherungen?
- Wer darf Wiederherstellungen anfordern?
- Wer führt Tests durch?
- Wer entscheidet bei möglichem Datenverlust?

Information and Technology

- Welche Systeme und Daten werden gesichert?
- Sind Sicherungen verschlüsselt und geschützt?
- Funktionieren Wiederherstellungen?
- Welche RPO- und RTO-Anforderungen bestehen?

Partners and Suppliers

- Wird ein Cloud- oder Backup-Anbieter verwendet?
- Welche Leistungen sind zugesichert?
- Wie können Daten bei Anbieterwechsel zurückgeführt werden?
- Welche Supportwege bestehen?

Value Streams and Processes

- Wie werden neue Systeme in die Sicherung aufgenommen?
- Wie werden Fehler behandelt?
- Wie laufen Wiederherstellungstests ab?
- Wie werden Ergebnisse und Verbesserungen dokumentiert?

“ Merke

Backup ist nicht nur eine Technologie.

Wiederherstellbarkeit entsteht durch das Zusammenspiel aller vier Dimensionen.

Die vier Dimensionen bei einem Incident

Dimension	Beispielhafte Fragen
Organizations and People	Wer koordiniert, entscheidet, analysiert und kommuniziert?
Information and Technology	Welche Systeme, Daten, Protokolle und Abhängigkeiten sind betroffen?
Partners and Suppliers	Welche Anbieter müssen beteiligt oder eskaliert werden?
Value Streams and Processes	Wie erfolgt Erfassung, Priorisierung, Wiederherstellung, Kommunikation und Abschluss?

Die vier Dimensionen bei einem Change

Dimension	Beispielhafte Fragen
Organizations and People	Wer beantragt, bewertet, autorisiert, implementiert und prüft?
Information and Technology	Welche Komponenten, Daten, Schnittstellen und Sicherheitsmaßnahmen sind betroffen?
Partners and Suppliers	Werden Hersteller, Provider oder Wartungspartner benötigt?

Dimension	Beispielhafte Fragen
Value Streams and Processes	Wie erfolgen Bewertung, Test, Autorisierung, Umsetzung, Rückfall und Erfolgskontrolle?

Die vier Dimensionen bei einer Verbesserung

Dimension	Beispielhafte Fragen
Organizations and People	Welche Fähigkeiten, Rollen oder kulturellen Veränderungen werden benötigt?
Information and Technology	Welche Daten belegen das Problem und welche Technologie unterstützt die Verbesserung?
Partners and Suppliers	Welche externen Beiträge oder Vertragsänderungen sind notwendig?
Value Streams and Processes	Welcher Arbeitsfluss wird verbessert und wie wird die Wirkung gemessen?

Typische Fehler

Fehler 1: Nur Technik betrachten

Eine Organisation kauft eine neue Plattform, ohne Rollen, Fähigkeiten, Support und Arbeitsabläufe vorzubereiten.

Fehler 2: Nur Prozesse dokumentieren

Abläufe werden beschrieben, aber notwendige Informationen, Technologien und Kompetenzen fehlen.

Fehler 3: Lieferanten nicht als Teil des Service betrachten

Externe Abhängigkeiten werden erst berücksichtigt, wenn ein Incident eskaliert.

Fehler 4: Menschen als austauschbare Ressourcen behandeln

Benötigte Fähigkeiten, Erfahrungen, Motivation und Zusammenarbeit werden nicht berücksichtigt.

Fehler 5: Jede Dimension getrennt optimieren

Ein Team verbessert seine eigene Kennzahl, verschlechtert aber den gesamten Wertstrom.

Fehler 6: Alle Situationen gleich ausführlich prüfen

Kleine Standardtätigkeiten werden unnötig kompliziert, während kritische Vorhaben nicht risikogerecht vertieft werden.

Fehler 7: Werkzeuge mit Fähigkeiten verwechseln

Eine Organisation besitzt eine Funktion im Ticketsystem, hat aber keine wirksame Arbeitsweise und keine eindeutigen Verantwortlichkeiten dafür.

Fehler 8: Verträge nur beim Einkauf betrachten

Betrieb, Support, Sicherheit, Eskalation und Ausstieg werden nicht ausreichend einbezogen.

Fehler 9: Datenmenge mit Informationsqualität verwechseln

Viele Kennzahlen werden gesammelt, liefern aber keine Grundlage für Entscheidungen oder Verbesserungen.

Fehler 10: Prozesse an Teamgrenzen enden lassen

Jedes Team bearbeitet nur seinen Teil, während niemand das Ende-zu-Ende-Outcome verantwortet.

Bedeutung für Fachinformatiker für Systemintegration

Fachinformatiker arbeiten häufig hauptsächlich in der technischen Dimension.

Ihre Aufgaben beeinflussen jedoch immer wieder alle vier Dimensionen.

Beispiel: neuer Server

Tätigkeit	Betroffene Dimension
Server installieren und konfigurieren	Information and Technology
Zuständigkeit und Betrieb klären	Organizations and People
Hardware-, Software- oder Cloud-Anbieter einbinden	Partners and Suppliers
Bereitstellung, Change, Monitoring und Support einordnen	Value Streams and Processes

Vor einer technischen Maßnahme sind deshalb zusätzliche Fragen sinnvoll:

- Welcher Service hängt von der Komponente ab?
- Wer trägt Verantwortung?
- Wer muss informiert werden?

- Welche Informationen müssen dokumentiert werden?
 - Welche Lieferanten sind beteiligt?
 - Welche Arbeitsabläufe werden verändert?
 - Wie wird der Erfolg aus Benutzersicht geprüft?
 - Welche langfristigen Betriebs- und Supportaufgaben entstehen?
-

30-Sekunden-Prüfung

Bei einer neuen Aufgabe kannst du alle vier Dimensionen mit vier Kurzfragen prüfen:

1. **Menschen:** Wer ist beteiligt, verantwortlich und ausreichend befähigt?
2. **Technologie:** Welche Informationen, Systeme und technischen Abhängigkeiten werden benötigt?
3. **Partner:** Welche externen Anbieter und vertraglichen Abhängigkeiten bestehen?
4. **Arbeitsfluss:** Wie gelangt die Aufgabe vom Bedarf zum überprüften Outcome?

Diese Kurzprüfung ersetzt keine notwendige Detailanalyse.

Sie hilft jedoch dabei, eine Dimension nicht vollständig zu übersehen.

Checkliste zu Organizations and People

- ☐ Sind Rollen und Verantwortlichkeiten eindeutig?
 - ☐ Sind Entscheidungs- und Eskalationswege bekannt?
 - ☐ Sind notwendige Fähigkeiten vorhanden?
 - ☐ Besteht ausreichende Kapazität?
 - ☐ Sind Vertretungen geregelt?
 - ☐ Funktioniert die Zusammenarbeit zwischen Teams?
 - ☐ Werden Wissen und Erfahrungen geteilt?
 - ☐ Unterstützt die Kultur offene Kommunikation und Verbesserung?
 - ☐ Verstehen die Beteiligten das erwartete Outcome?
-

Checkliste zu Information and Technology

- ☐ Sind benötigte Informationen verfügbar und aktuell?
- ☐ Ist die Verantwortung für Datenqualität geklärt?
- ☐ Passen Technologien und Architektur zum Bedarf?
- ☐ Sind Schnittstellen und Abhängigkeiten dokumentiert?
- ☐ Sind Informationssicherheit und Datenschutz berücksichtigt?

- ☐ Sind Backup und Wiederherstellung vorbereitet?
 - ☐ Werden Systeme angemessen überwacht?
 - ☐ Sind Automatisierungen kontrollierbar?
 - ☐ Sind technische Schulden und Lebenszyklusrisiken bekannt?
-

Checkliste zu Partners and Suppliers

- ☐ Sind alle relevanten Lieferanten bekannt?
 - ☐ Sind Leistungsumfang und Verantwortlichkeiten eindeutig?
 - ☐ Passen Verträge zu den benötigten Outcomes?
 - ☐ Sind Sicherheits- und Datenschutzanforderungen geregelt?
 - ☐ Bestehen bekannte Ausfall- oder Konzentrationsrisiken?
 - ☐ Sind Support- und Eskalationswege vorbereitet?
 - ☐ Werden Lieferantenleistungen überwacht?
 - ☐ Bleiben notwendige interne Fähigkeiten erhalten?
 - ☐ Besteht eine Ausstiegs- und Übergangsplanung?
-

Checkliste zu Value Streams and Processes

- ☐ Ist das gewünschte Outcome eindeutig?
 - ☐ Sind Anfang und Ende des Wertstroms bekannt?
 - ☐ Sind notwendige Aktivitäten und Verantwortlichkeiten geklärt?
 - ☐ Sind Übergaben und Informationsflüsse sichtbar?
 - ☐ Werden Wartezeiten und Engpässe erkannt?
 - ☐ Besitzen Kontrollen einen nachvollziehbaren Zweck?
 - ☐ Werden unnötige Schritte vermieden?
 - ☐ Unterstützen Prozesse den gesamten Wertstrom?
 - ☐ Werden Ergebnisse und Stakeholdererfahrung geprüft?
 - ☐ Fließt Feedback in Continual Improvement ein?
-

Gesamtcheck für ein Produkt oder einen Service

- ☐ Wurden alle vier Dimensionen berücksichtigt?
- ☐ Sind die Dimensionen aufeinander abgestimmt?
- ☐ Wurden Outcomes, Kosten und Risiken betrachtet?

- ☐ Wurde die Erfahrung der relevanten Stakeholder berücksichtigt?
- ☐ Sind betriebliche und gesetzliche Vorgaben einbezogen?
- ☐ Sind technische und organisatorische Abhängigkeiten sichtbar?
- ☐ Sind Verantwortung und Entscheidungsbefugnisse eindeutig?
- ☐ Sind Lieferantenbeziehungen und Verträge geeignet?
- ☐ Ist der Ende-zu-Ende-Wertstrom nachvollziehbar?
- ☐ Sind Betrieb, Support, Sicherheit und Verbesserung vorbereitet?
- ☐ Wird der Erfolg anhand des tatsächlichen Outcomes geprüft?

Schnellreferenz

Dimension	Kurzfrage
Organizations and People	Wer wird benötigt und wie arbeiten die Beteiligten zusammen?
Information and Technology	Welche Informationen und Technologien ermöglichen das Outcome?
Partners and Suppliers	Welche externen Leistungen und Abhängigkeiten bestehen?
Value Streams and Processes	Wie fließt die Arbeit vom Bedarf zum Ergebnis?

Zusammenfassende Darstellung

“ Organizations and People

Rollen · Fähigkeiten · Kapazität · Kommunikation · Kultur

Information and Technology

Daten · Wissen · Anwendungen · Infrastruktur · Integration · Automatisierung

Partners and Suppliers

Leistungen · Verträge · Zusammenarbeit · Abhängigkeiten · Ausstieg

Value Streams and Processes

Aktivitäten · Übergaben · Kontrollen · Arbeitsfluss · Outcomes

↓

ganzheitliches digitales Produkt- und Service-Management

↓

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
- 2.6 Der Product and Service Lifecycle
- 2.7 Die ITIL Management Practices
- 2.8 Value Streams und Value Stream Mapping
- 2.9 Continual Improvement
- 2.10 ITIL an den eigenen Kontext anpassen
- Supplier Management
- Information Security Management
- Knowledge Management
- Service Configuration Management
- IT Asset Management

Quellen und Versionsstand

Offizielle Grundlagen

- [PeopleCert: ITIL Foundation – Version 5](#)
- [ITIL: ITIL Foundation – Version 5](#)
- [PeopleCert: ITIL Experience – Version 5](#)
- [PeopleCert: Supporting the ITIL evolution with the new Transition module](#)
- [ITIL: ITIL Capability and Maturity Assessment](#)

Einordnung

ITIL Version 5 verwendet die folgenden vier Dimensionen des Produkt- und Service-Managements:

- Organizations and People
- Information and Technology
- Partners and Suppliers
- Value Streams and Processes

Die offiziellen ITIL-Version-5-Grundlagen beschreiben die vier Dimensionen als Grundlage einer ganzheitlichen Betrachtung digitaler Produkte und Services.

Die ausführlichen Leitfragen, Beispiele, Checklisten und technischen Einordnungen auf dieser Seite sind zusätzliche herstellerneutrale Erläuterungen dieses unabhängigen Nachschlagewerks.

Sie stellen keine wörtlichen offiziellen ITIL-Definitionen und keine für jede Organisation verbindlichen Arbeitsabläufe dar.

Konkrete Rollen, Technologien, Lieferantenmodelle, Prozesse und Kontrollen müssen an den jeweiligen Kontext angepasst werden.

Behandelter Framework-Stand: ITIL Version 5

Zusätzlich berücksichtigt: ITIL 4

Fachlicher Stand: August 2026
