2.4 Governance und Verantwortlichkeit

> **Kurz erklärt**
>
> Governance beschreibt, wie eine Organisation gelenkt und kontrolliert wird.
>
> Sie sorgt dafür, dass:
>
> - Ziele und Prioritäten festgelegt werden,
> - Entscheidungen innerhalb klarer Rahmenbedingungen getroffen werden,
> - Verantwortlichkeiten eindeutig sind,
> - Risiken angemessen behandelt werden,
> - verbindliche Vorgaben eingehalten werden,
> - und die tatsächlichen Ergebnisse überwacht werden.
>
> Im ITIL Value System wird Governance durch drei grundlegende Aktivitäten verwirklicht:
>
> 1. **Evaluate** – bewerten
> 2. **Direct** – Richtung vorgeben
> 3. **Monitor** – überwachen

Warum Governance notwendig ist

Digitale Produkte und Services beeinflussen heute häufig:

- Geschäftsprozesse,
- Kommunikation,
- Kundenerfahrung,
- Informationssicherheit,
- Datenschutz,
- Finanzen,
- Produktion,
- Lieferketten,
- und die Arbeitsfähigkeit von Mitarbeitern.

Technische Entscheidungen können deshalb weitreichende organisatorische Folgen besitzen.

Beispiele:

- Eine Firewall-Regel beeinflusst die Sicherheit und Erreichbarkeit eines Service.
- Eine neue Cloud-Anwendung kann personenbezogene Daten verarbeiten.

- Eine Änderung am Verzeichnisdienst kann viele Benutzer und Anwendungen betreffen.
- Eine nicht getestete Wiederherstellung kann im Notfall zu langen Ausfallzeiten führen.
- Eine KI-gestützte Entscheidung kann falsche oder nicht nachvollziehbare Ergebnisse erzeugen.
- Ein externer Dienstleister kann eine kritische Abhängigkeit für mehrere Services darstellen.

Ohne klare Governance können unter anderem folgende Probleme entstehen:

- Entscheidungen werden ohne ausreichende Befugnis getroffen.
- Verantwortlichkeiten sind unklar.
- Risiken werden uneinheitlich bewertet.
- Teams verfolgen widersprüchliche Ziele.
- verbindliche Vorgaben werden übersehen.
- technische Maßnahmen unterstützen nicht die Ziele der Organisation.
- Leistung wird gemessen, aber nicht wirksam bewertet.
- bekannte Probleme bleiben ohne Konsequenz.
- externe Dienstleister werden nicht ausreichend kontrolliert.
- niemand trägt erkennbar Verantwortung für das Gesamtergebnis.

> **Merke**
>
> Governance soll nicht jede technische Einzelentscheidung zentralisieren.
>
> Sie schafft den Rahmen, innerhalb dessen angemessene Entscheidungen getroffen und kontrolliert werden können.

Governance im ITIL Value System

Governance ist einer der fünf Bestandteile des ITIL Value Systems.

Das Value System verbindet:

- Guiding Principles,
- Governance,
- Value Chain Activities,
- Management Practices,
- und Continual Improvement.

Governance stellt dabei sicher, dass die Tätigkeiten der Organisation:

- an ihren Zielen ausgerichtet sind,
- innerhalb akzeptierter Grenzen stattfinden,
- nachvollziehbar entschieden werden,

- und hinsichtlich Leistung, Risiken und Regelkonformität überwacht werden.

Governance wirkt damit auf:

- digitale Produkte,
- Services,
- Practices,
- Wertströme,
- Projekte,
- technische Änderungen,
- Lieferantenbeziehungen,
- Investitionen,
- Informationssicherheit,
- und Verbesserungsinitiativen.

> **Wichtig**
>
> Governance ist kein einzelner Prozess und keine einzelne Management Practice.
>
> Sie ist ein übergreifender Bestandteil des gesamten ITIL Value Systems.

Die drei Governance-Aktivitäten

Governance wird durch drei grundlegende Aktivitäten verwirklicht:

Aktivität	Bedeutung	Zentrale Frage
Evaluate	Bedürfnisse, Optionen, Leistung, Risiken und Rahmenbedingungen bewerten	Was ist notwendig und welche Entscheidung ist angemessen?
Direct	Richtung, Prioritäten, Grundsätze und Entscheidungsrahmen vorgeben	Was soll erreicht werden und innerhalb welcher Grenzen?
Monitor	Leistung, Ergebnisse, Risiken und Einhaltung überwachen	Erreichen wir die Ziele und werden die Vorgaben eingehalten?

Diese Aktivitäten sind miteinander verbunden.

Die Ergebnisse des Monitorings können eine erneute Bewertung auslösen.

Aus einer neuen Bewertung können wiederum geänderte Vorgaben oder Prioritäten entstehen.

> **Vereinfachter Kreislauf**

> Evaluate
> ↓
> Direct
> ↓
> Monitor
> ↓
> neue Erkenntnisse
> ↓
> erneut Evaluate

Evaluate – bewerten

Bei **Evaluate** werden die aktuelle Situation, Bedürfnisse, Möglichkeiten und Risiken untersucht.

Mögliche Bewertungsgegenstände sind:

- Anforderungen von Kunden und Benutzern,
- Ziele der Organisation,
- gesetzliche Verpflichtungen,
- vertragliche Anforderungen,
- technische Möglichkeiten,
- bestehende Fähigkeiten,
- Kosten,
- Risiken,
- Sicherheitsanforderungen,
- Nachhaltigkeitsaspekte,
- Erfahrungen der Stakeholder,
- und erwartete Outcomes.

Beispiel:

Eine Organisation prüft, ob eine zentrale Cloud-Plattform eingeführt werden soll.

Bei der Bewertung können unter anderem folgende Fragen relevant sein:

- Welches Problem soll gelöst werden?
- Welche Outcomes werden erwartet?
- Welche Daten werden verarbeitet?
- Welche Sicherheits- und Datenschutzanforderungen gelten?
- Welche Kosten entstehen?
- Welche Lieferantenabhängigkeiten entstehen?
- Welche vorhandenen Systeme müssen integriert werden?
- Welche Risiken entstehen bei einem Ausfall?
- Welche Fähigkeiten werden intern benötigt?

- Welche Alternativen bestehen?
- Wie kann die Lösung später wieder abgelöst werden?

> **Typischer Fehler**
>
> Eine Entscheidung wird ausschließlich anhand des Anschaffungspreises oder einzelner technischer Funktionen bewertet.
>
> Betrieb, Support, Integration, Sicherheit, Abhängigkeiten und spätere Ablösung werden nicht berücksichtigt.

Evaluate bedeutet nicht nur einmalig prüfen

Bewertung findet nicht ausschließlich vor einer Einführung statt.

Eine erneute Bewertung kann notwendig sein, wenn:

- sich Geschäftsziele ändern,
- neue gesetzliche Anforderungen entstehen,
- ein Sicherheitsvorfall auftritt,
- ein Lieferant seine Leistung verändert,
- neue Technologien verfügbar werden,
- Benutzerfeedback auf Probleme hinweist,
- Kosten deutlich steigen,
- Risiken anders eingeschätzt werden,
- oder ein Service seine Ziele nicht mehr erreicht.

Beispiel:

Eine Anwendung wurde ursprünglich nur für eine kleine interne Abteilung eingeführt.

Später wird sie für einen unternehmenskritischen Prozess eingesetzt.

Dadurch können sich ändern:

- Verfügbarkeitsanforderungen,
- Sicherheitsanforderungen,
- Supportzeiten,
- Wiederherstellungsziele,
- Überwachung,
- Dokumentation,
- und notwendige Lieferantenvereinbarungen.

Die ursprüngliche Bewertung reicht dann möglicherweise nicht mehr aus.

Direct – Richtung vorgeben

Bei **Direct** werden Richtung, Prioritäten und Rahmenbedingungen vorgegeben.

Dies kann beispielsweise erfolgen durch:

- Strategien,
- Grundsätze,
- Richtlinien,
- Ziele,
- Prioritäten,
- Entscheidungsbefugnisse,
- Risikogrenzen,
- Rollen,
- Vorgaben für Kontrollen,
- und zu erreichende Ergebnisse.

Beispiele:

- Administrative Zugriffe müssen durch Multi-Faktor-Authentifizierung geschützt werden.
- Kritische Services müssen dokumentierte Wiederherstellungsverfahren besitzen.
- Produktive Änderungen benötigen eine dem Risiko angemessene Autorisierung.
- Personenbezogene Daten dürfen nur in freigegebenen Systemen verarbeitet werden.
- Für kritische Lieferanten müssen Ausweich- oder Beendigungsstrategien betrachtet werden.
- Sicherheitsrelevante Ereignisse müssen nach dem festgelegten Verfahren gemeldet werden.
- Wiederherstellungsverfahren müssen in festgelegten Abständen getestet werden.

Governance gibt dabei normalerweise nicht jeden technischen Einzelschritt vor.

Beispiel:

Governance kann festlegen:

> Administrative Zugriffe müssen mit einer starken Mehrfaktor-Authentifizierung geschützt werden.

Das zuständige Management und die Fachteams bestimmen anschließend:

- welche technische Lösung verwendet wird,
- wie sie eingeführt wird,
- welche Ausnahmen zulässig sind,
- wie Benutzer unterstützt werden,

- und wie die Wirksamkeit kontrolliert wird.

Richtung und Grenzen

Eine gute Governance-Vorgabe beantwortet möglichst:

- Welches Ziel wird verfolgt?
- Für welchen Bereich gilt die Vorgabe?
- Wer trägt Verantwortung?
- Welche Grenzen müssen eingehalten werden?
- Welche Ausnahmen sind möglich?
- Wer darf Ausnahmen genehmigen?
- Wie wird die Einhaltung geprüft?
- Was geschieht bei Abweichungen?
- Wann wird die Vorgabe erneut bewertet?

Unklare Vorgabe:

> Systeme müssen sicher sein.

Präzisere Vorgabe:

> Kritische Systeme müssen entsprechend der festgelegten Schutzbedarfs- und Risikobewertung abgesichert, überwacht und regelmäßig auf die Wirksamkeit ihrer Kontrollen geprüft werden.

Die konkrete technische Umsetzung wird anschließend durch zuständige Fachkräfte und Management Practices gestaltet.

Monitor – überwachen

Bei **Monitor** wird geprüft, ob:

- die vorgegebene Richtung eingehalten wird,
- Ziele erreicht werden,
- Risiken innerhalb akzeptierter Grenzen bleiben,
- Kontrollen wirksam sind,
- Verantwortlichkeiten wahrgenommen werden,
- und Produkte sowie Services die erwarteten Outcomes unterstützen.

Monitoring im Governance-Kontext bedeutet mehr als technische Überwachung.

Es kann unter anderem umfassen:

- Serviceleistung,
- Benutzer- und Kundenerfahrung,
- Sicherheitsrisiken,
- Einhaltung von Richtlinien,
- Kostenentwicklung,
- Lieferantenleistung,
- Fortschritt strategischer Vorhaben,
- Ergebnisse von Audits,
- Status kritischer Verbesserungen,
- Wiederherstellbarkeit,
- und Wirksamkeit organisatorischer Kontrollen.

Beispiel:

Eine Organisation verlangt regelmäßige Wiederherstellungstests.

Governance-Monitoring prüft nicht nur, ob ein Testtermin im Kalender stand.

Es prüft beispielsweise:

- Wurde der Test tatsächlich durchgeführt?
- Welche Systeme wurden getestet?
- War die Wiederherstellung erfolgreich?
- Wurden die vereinbarten Wiederherstellungsziele erreicht?
- Welche Probleme wurden erkannt?
- Wurden notwendige Verbesserungen umgesetzt?
- Bestehen weiterhin nicht akzeptierte Risiken?

> **Merke**
>
> Aktivität ist nicht automatisch Wirksamkeit.
>
> Ein ausgefülltes Kontrollformular beweist noch nicht, dass das gewünschte Ergebnis erreicht wurde.

Governance und Management unterscheiden

Governance und Management sind eng miteinander verbunden, aber nicht identisch.

Governance	Management

bewertet Bedürfnisse, Erwartungen und Rahmenbedingungen	plant und organisiert die praktische Umsetzung
gibt Richtung und Grenzen vor	weist Ressourcen und Aufgaben zu
legt Verantwortlichkeit und Entscheidungsbefugnisse fest	koordiniert Teams, Practices und Arbeitsabläufe
überwacht Outcomes, Risiken und Regelkonformität	überwacht die laufende Ausführung
entscheidet über grundlegende Prioritäten	trifft operative und taktische Entscheidungen innerhalb des Rahmens
stellt Rechenschaftspflicht sicher	liefert Ergebnisse und berichtet darüber

Vereinfacht:

> **Governance**
>
> Bestimmt, was erreicht und kontrolliert werden muss.
>
> **Management**
>
> Organisiert, wie dies innerhalb des vorgegebenen Rahmens umgesetzt wird.

Diese Trennung bedeutet nicht, dass Governance nur die Unternehmensleitung betrifft.

Auch nachgelagerte Gremien oder Rollen können delegierte Governance-Aufgaben wahrnehmen.

Die grundlegende Rechenschaftspflicht muss jedoch eindeutig bleiben.

Beispiel: Einführung von Multi-Faktor-Authentifizierung

Governance

- bewertet Sicherheitsrisiken und rechtliche Anforderungen
- gibt das Ziel einer starken Authentifizierung vor
- legt Geltungsbereich und zulässige Ausnahmen fest
- bestimmt Verantwortlichkeit
- fordert Wirksamkeitsnachweise
- überwacht Risiken und Einhaltung

Management

- plant die Einführung
- wählt geeignete Produkte und Verfahren
- organisiert Ressourcen
- legt Zeitplan und Pilotgruppen fest

- koordiniert Kommunikation und Support
- behandelt technische Probleme
- berichtet über Fortschritt und Ergebnisse

Technische Umsetzung

- Identitätsanbieter konfigurieren
- Authentifizierungsmethoden einrichten
- Richtlinien anwenden
- Benutzer registrieren
- Protokollierung aktivieren
- Notfallzugänge absichern
- Funktion und Rückfallmöglichkeiten testen

Alle drei Ebenen sind notwendig.

Eine technisch erfolgreiche Konfiguration allein beweist noch nicht, dass:

- der vollständige Geltungsbereich geschützt ist,
- Ausnahmen kontrolliert werden,
- Benutzer unterstützt werden,
- oder die Sicherheitsziele tatsächlich erreicht werden.

Verantwortung und Verantwortlichkeit

Im Deutschen wird der Begriff **Verantwortung** häufig für unterschiedliche Sachverhalte verwendet.

Für eine klare Rollenverteilung ist die Unterscheidung hilfreich zwischen:

Begriff	Bedeutung
Ausführungsverantwortung	eine Person oder Rolle führt eine Aufgabe aus
Entscheidungsverantwortung	eine Person oder Rolle besitzt die Befugnis, eine Entscheidung zu treffen
Ergebnisverantwortung	eine Person oder Rolle steht für das erreichte Ergebnis ein
Rechenschaftspflicht	eine Person oder ein Gremium muss Entscheidungen und Ergebnisse erklären und vertreten
Beratung	Fachwissen wird eingebracht, ohne selbst die endgültige Entscheidung zu treffen
Informationsbedarf	eine Person oder Rolle muss über Entscheidung oder Ergebnis informiert werden

Eine Person kann eine Aufgabe ausführen, ohne die endgültige Entscheidungs- oder Ergebnisverantwortung zu besitzen.

Beispiel:

Ein Systemadministrator setzt eine freigegebene Firewall-Regel um.

- Der Administrator ist für die korrekte technische Ausführung verantwortlich.
- Eine andere Rolle kann für die fachliche Anforderung verantwortlich sein.
- Eine Sicherheitsrolle kann die Risikobewertung durchführen.
- Eine autorisierte Rolle kann die Änderung genehmigen.
- Ein Service Owner kann für die Auswirkungen auf den Service rechenschaftspflichtig sein.

> **Typischer Fehler**
>
> Die Person, die eine technische Änderung ausführt, wird automatisch für sämtliche geschäftlichen, rechtlichen und organisatorischen Entscheidungen verantwortlich gemacht.

Verantwortung muss eindeutig sein

Bei wichtigen Produkten, Services und Entscheidungen sollte erkennbar sein:

- Wer besitzt die Entscheidungsbefugnis?
- Wer führt die Aufgabe aus?
- Wer prüft das Ergebnis?
- Wer akzeptiert verbleibende Risiken?
- Wer kommuniziert mit betroffenen Stakeholdern?
- Wer aktualisiert die Dokumentation?
- Wer überwacht die langfristige Wirksamkeit?
- Wer eskaliert bei Abweichungen?

Unklare Verantwortung kann zu folgenden Situationen führen:

- Jeder geht davon aus, dass ein anderer handelt.
- Entscheidungen werden mehrfach oder widersprüchlich getroffen.
- Risiken werden ohne erkennbare Autorisierung akzeptiert.
- Probleme werden zwischen Teams weitergereicht.
- Dokumentationen bleiben veraltet.
- notwendige Eskalationen erfolgen zu spät.
- niemand überprüft das Ende-zu-Ende-Ergebnis.

> **Praxistipp**

> Kann bei einer kritischen Aufgabe niemand eindeutig benennen, wer entscheidet und wer für das Ergebnis einsteht, besteht ein Governance- und Verantwortlichkeitsproblem.

Delegation und Rechenschaftspflicht

Aufgaben und Entscheidungsbefugnisse können delegiert werden.

Eine sinnvolle Delegation benötigt:

- einen klaren Umfang,
- bekannte Grenzen,
- ausreichende Fachkenntnisse,
- benötigte Ressourcen,
- Zugang zu relevanten Informationen,
- definierte Eskalationswege,
- und eine geeignete Kontrolle.

Beispiel:

Ein Betriebsteam darf bestimmte dokumentierte Standardänderungen selbstständig durchführen.

Die Delegation kann festlegen:

- welche Änderungen umfasst sind,
- welche Voraussetzungen gelten,
- wann keine zusätzliche Genehmigung notwendig ist,
- welche Dokumentation erforderlich ist,
- wann eskaliert werden muss,
- und wie die Ergebnisse überwacht werden.

> **Wichtig**
>
> Delegation bedeutet nicht, dass keine Kontrolle mehr erforderlich ist.
>
> Sie soll Entscheidungen dort ermöglichen, wo ausreichendes Wissen vorhanden ist und das Risiko angemessen beherrscht werden kann.

Entscheidungsbefugnisse

Entscheidungsbefugnisse sollten zum Risiko und zur Bedeutung einer Entscheidung passen.

Mögliche Entscheidungsbereiche sind:

- Investitionen,
- Produkt- und Serviceprioritäten,
- Sicherheitsausnahmen,
- Change-Autorisierung,
- Risikoakzeptanz,
- Lieferantenauswahl,
- Datenverarbeitung,
- Notfallmaßnahmen,
- und Außerbetriebnahme von Systemen.

Eine Entscheidungsbefugnis sollte möglichst beantworten:

- Wer darf entscheiden?
- Für welchen Umfang?
- Bis zu welcher Risikogrenze?
- Welche Informationen werden benötigt?
- Welche Beratung ist erforderlich?
- Welche Entscheidung muss dokumentiert werden?
- Wann ist eine höhere Instanz einzubeziehen?

Beispiel:

Ein Administrator darf einen abgestürzten Dienst nach einer dokumentierten Arbeitsanweisung neu starten.

Er darf möglicherweise nicht ohne zusätzliche Autorisierung:

- die gesamte Serverplattform neu konfigurieren,
- Sicherheitskontrollen deaktivieren,
- Daten löschen,
- oder einen nicht getesteten Change an einem kritischen Produktivsystem durchführen.

Autorisierung nach Risiko und Kontext

Nicht jede Entscheidung benötigt denselben Freigabeumfang.

Situation	Mögliche Behandlung
häufige, dokumentierte und risikoarme Standardtätigkeit	delegierte oder vorab autorisierte Ausführung
normale Änderung mit überschaubarem Risiko	Bewertung und Autorisierung durch zuständige Rolle
komplexe Änderung an kritischem Service	erweiterte fachliche, technische und geschäftliche Bewertung

Situation	Mögliche Behandlung
dringende Sicherheitsmaßnahme	beschleunigtes Verfahren mit klarer Befugnis und nachträglicher Kontrolle
grundlegende strategische Änderung	Entscheidung durch entsprechend befugtes Governance-Gremium

Die konkrete Organisation legt fest:

- welche Entscheidungsmodelle verwendet werden,
- welche Risikokriterien gelten,
- wer autorisieren darf,
- und welche Nachweise erforderlich sind.

> **Typischer Fehler**
>
> Jede Änderung muss dieselben umfangreichen Genehmigungsstufen durchlaufen.
>
> Dadurch werden risikoarme Tätigkeiten unnötig verzögert, während kritische Entscheidungen möglicherweise trotzdem nicht ausreichend fachlich bewertet werden.

Governance ist mehr als Genehmigung

Governance wird häufig fälschlich auf Freigaben reduziert.

Eine Freigabe beantwortet lediglich eine begrenzte Frage:

> Darf diese konkrete Handlung innerhalb des festgelegten Rahmens durchgeführt werden?

Governance umfasst zusätzlich:

- Ziele,
- Strategien,
- Verantwortung,
- Risikogrenzen,
- Leistung,
- Regelkonformität,
- Erfahrung,
- Nachhaltigkeit,

- und fortlaufende Kontrolle.

Ein Change kann formal genehmigt sein und dennoch schlecht gesteuert werden, wenn:

- das Ziel unklar ist,
- Auswirkungen nicht verstanden wurden,
- das Ergebnis nicht geprüft wird,
- Verantwortlichkeiten fehlen,
- oder wiederholt dieselben Probleme entstehen.

Richtlinien, Standards und Arbeitsanweisungen unterscheiden

Governance-Vorgaben können auf unterschiedlichen Ebenen konkretisiert werden.

Dokumentenart	Zweck	Beispiel
Grundsatz oder Policy	legt Ziel, Richtung und verbindliche Erwartungen fest	administrative Zugriffe müssen angemessen geschützt werden
Standard	legt verbindliche einheitliche Anforderungen fest	zugelassene MFA-Verfahren und Mindestanforderungen
Prozess oder Ablauf	beschreibt zusammenhängende Aktivitäten und Verantwortlichkeiten	Beantragung und Freigabe eines administrativen Zugriffs
Verfahren	beschreibt eine festgelegte Vorgehensweise	Registrierung eines neuen MFA-Geräts
Arbeitsanweisung	beschreibt konkrete Ausführungsschritte	Menü- und Konfigurationsschritte im Identitätssystem
Checkliste	unterstützt die Kontrolle wichtiger Punkte	Prüfung eines neuen administrativen Kontos

Nicht jede Organisation verwendet exakt diese Bezeichnungen.

Entscheidend ist, dass:

- Geltungsbereich,
- Verbindlichkeit,
- Verantwortlichkeit,
- und erforderliche Handlung

eindeutig sind.

Beispiel: Backup-Governance

Governance-Vorgabe

> Geschäftskritische Daten und Systeme müssen entsprechend ihrer Kritikalität gesichert und innerhalb definierter Ziele wiederhergestellt werden können.

Mögliche Standards

- zulässige Sicherungsziele
- Verschlüsselungsanforderungen
- Aufbewahrungszeiten
- Trennung von Produktiv- und Sicherungszugängen
- Anforderungen an unveränderbare Sicherungen
- Häufigkeit von Wiederherstellungstests

Management

- plant Backup-Infrastruktur
- weist Verantwortlichkeiten zu
- organisiert Lizenzen und Speicher
- koordiniert Tests
- bewertet Kapazität und Kosten
- berichtet über Abweichungen

Technische Umsetzung

- Backup-Jobs konfigurieren
- Zugangsdaten absichern
- Zeitpläne einrichten
- Warnungen konfigurieren
- Wiederherstellungen testen
- Ergebnisse dokumentieren

Governance-Monitoring

- Sind alle kritischen Systeme erfasst?
- Sind Wiederherstellungen erfolgreich?
- Werden Zielzeiten erreicht?
- Werden Fehler zeitnah behandelt?
- Sind verbleibende Risiken akzeptiert?
- Werden Verbesserungen umgesetzt?

Risikobereitschaft und Risikotoleranz

Governance legt fest, welche Risiken:

- akzeptiert,
- reduziert,

- übertragen,
- vermieden,
- oder weiter beobachtet

werden.

Die Organisation kann dafür Risikogrenzen definieren.

Beispiele:

- maximal tolerierbare Ausfallzeit
- maximal akzeptabler Datenverlust
- zulässige Lieferantenabhängigkeit
- notwendiger Freigabeumfang
- erforderliche Sicherheitskontrollen
- maximale finanzielle Auswirkung
- zulässige Restunsicherheit bei einer Einführung

Ein technisches Team sollte verbleibende erhebliche Risiken nicht ohne entsprechende Befugnis selbst akzeptieren.

Beispiel:

Ein Administrator stellt fest, dass ein veraltetes System keine Sicherheitsupdates mehr erhält.

Er kann:

- die technische Situation dokumentieren,
- mögliche Maßnahmen vorschlagen,
- Auswirkungen bewerten,
- kurzfristige Schutzmaßnahmen umsetzen,
- und das Risiko eskalieren.

Die Entscheidung, ein erhebliches Restrisiko langfristig zu akzeptieren, benötigt eine entsprechend befugte Rolle.

> **Merke**
>
> Risikoanalyse kann durch Fachkräfte erfolgen.
>
> Risikoakzeptanz muss durch eine dafür autorisierte Stelle erfolgen.

Kontrollen

Eine Kontrolle soll ein Risiko reduzieren, eine Vorgabe sicherstellen oder eine Abweichung erkennbar machen.

Kontrollen können sein:

- vorbeugend,
- erkennend,
- korrigierend,
- manuell,
- technisch automatisiert,
- organisatorisch,
- oder eine Kombination daraus.

Kontrollart	Beispiel
Vorbeugend	MFA verhindert Anmeldung nur mit Kennwort
Erkennend	Monitoring erkennt abgelaufenes Zertifikat
Korrigierend	dokumentiertes Wiederherstellungsverfahren
Manuell	Vier-Augen-Prüfung einer kritischen Änderung
Automatisiert	Richtlinie blockiert unsichere Konfiguration
Organisatorisch	Funktionstrennung zwischen Beantragung und Genehmigung

Eine Kontrolle sollte hinsichtlich ihrer Wirksamkeit bewertet werden.

Fragen dazu:

- Welches Risiko behandelt die Kontrolle?
- Ist sie vollständig umgesetzt?
- Kann sie umgangen werden?
- Erzeugt sie neue Risiken?
- Wird ihre Funktion regelmäßig geprüft?
- Ist der Aufwand angemessen?
- Gibt es Ausnahmen?
- Werden Abweichungen verfolgt?

Messgrößen und Governance

Governance benötigt Informationen, um Leistung und Risiken bewerten zu können.

Kennzahlen sollten jedoch nicht isoliert betrachtet werden.

Beispiel:

> 98 Prozent aller Tickets wurden innerhalb der Zielzeit geschlossen.

Diese Zahl beantwortet nicht automatisch:

- Waren die Lösungen nachhaltig?
- Wurden Tickets voreilig geschlossen?
- Mussten Benutzer erneut Kontakt aufnehmen?
- Wurden wichtige Incidents angemessen priorisiert?
- Wurde das erwartete Outcome erreicht?
- Sind die Zielzeiten selbst sinnvoll?

Geeignete Governance-Informationen können umfassen:

- erreichte Outcomes,
- Serviceleistung,
- Benutzer- und Kundenerfahrung,
- Risiken und Abweichungen,
- Sicherheitsvorfälle,
- wiederkehrende Incidents,
- Wirksamkeit von Verbesserungen,
- Kostenentwicklung,
- Lieferantenleistung,
- Wiederherstellungstests,
- und Einhaltung verbindlicher Anforderungen.

> **Typischer Fehler**
>
> Eine einzelne leicht messbare Kennzahl wird zum alleinigen Steuerungsziel.
>
> Mitarbeiter optimieren anschließend die Kennzahl, ohne den tatsächlichen Wert zu verbessern.

Verantwortlichkeit für Produkte und Services

Für wichtige Produkte und Services sollten Verantwortlichkeiten geklärt sein.

Mögliche Rollen können sein:

- Product Owner,
- Product Manager,
- Service Owner,
- Service Manager,

- technische Systemverantwortliche,
- Information Owner,
- Process Owner,
- Practice Owner,
- Supplier Manager,
- Risk Owner,
- und Informationssicherheitsverantwortliche.

ITIL schreibt nicht für jede Organisation dieselben Rollenbezeichnungen oder Organisationsstrukturen vor.

Entscheidend ist, dass folgende Fragen beantwortet werden:

- Wer verantwortet das Produkt?
- Wer verantwortet den Service?
- Wer entscheidet über Prioritäten?
- Wer verantwortet technische Komponenten?
- Wer akzeptiert Risiken?
- Wer verantwortet Daten?
- Wer steuert Lieferanten?
- Wer überwacht die Leistung?
- Wer treibt Verbesserungen voran?

> **Wichtig**
>
> Eine Rollenbezeichnung allein schafft noch keine wirksame Verantwortung.
>
> Die Rolle benötigt Befugnisse, Informationen, Fähigkeiten und Ressourcen.

Service Owner und technische Verantwortung unterscheiden

Ein Service Owner betrachtet den Service normalerweise aus einer Ende-zu-Ende-Perspektive.

Technische Verantwortliche betreuen dagegen möglicherweise einzelne Bestandteile.

Beispiel: E-Mail-Service

Verantwortungsbereich	Mögliche Zuständigkeit
gesamter E-Mail-Service	Service Owner
Identitätsplattform	Identity-Team
DNS	Netzwerk- oder Infrastrukturteam
Mailplattform	Messaging-Team oder Cloud-Provider

Verantwortungsbereich	Mögliche Zuständigkeit
Endgeräte und Client	Workplace-Team
Sicherheitsanforderungen	Informationssicherheit
Lieferantenvertrag	Supplier Management oder Einkauf
Benutzerunterstützung	Service Desk

Der Service Owner muss nicht jede technische Tätigkeit selbst ausführen.

Er benötigt jedoch ausreichende Informationen, um:

- Serviceleistung zu bewerten,
- Abhängigkeiten zu verstehen,
- Risiken zu eskalieren,
- Prioritäten abzustimmen,
- und Verbesserungen zu unterstützen.

RACI als mögliches Hilfsmittel

Eine RACI-Matrix kann helfen, Rollen bei einer Tätigkeit zu klären.

Kürzel	Bedeutung
R – Responsible	führt die Aufgabe aus
A – Accountable	steht für das Ergebnis ein und besitzt die übergeordnete Verantwortlichkeit
C – Consulted	wird vor oder während der Entscheidung fachlich einbezogen
I – Informed	wird über Entscheidung oder Ergebnis informiert

Beispiel: produktive Firewall-Änderung

Rolle	Zuordnung
Netzwerkadministrator	Responsible
autorisierte Change- oder Service-Rolle	Accountable
Informationssicherheit und Anwendungsverantwortlicher	Consulted
Service Desk und betroffene Benutzergruppen	Informed

Eine RACI-Matrix ist ein mögliches Organisationswerkzeug und keine zwingend vorgeschriebene ITIL-Darstellung.

Bei der Verwendung sollte vermieden werden:

- mehrere unklare Accountable-Zuordnungen,
- fehlende ausführende Verantwortung,
- Beteiligung zu vieler Personen,
- veraltete Rollenzuordnungen,
- und eine Matrix ohne praktische Anwendung.

Eskalation

Eskalation ist notwendig, wenn:

- eine Entscheidung außerhalb der eigenen Befugnis liegt,
- ein Risiko die eigene Entscheidungsgrenze überschreitet,
- vereinbarte Ziele gefährdet sind,
- benötigte Ressourcen fehlen,
- Verantwortlichkeiten unklar bleiben,
- ein Konflikt nicht gelöst werden kann,
- eine Sicherheits- oder Datenschutzverletzung möglich ist,
- oder eine verbindliche Vorgabe nicht eingehalten werden kann.

Eskalation bedeutet nicht automatisch persönliches Versagen.

Sie ist ein vorgesehener Mechanismus, um Entscheidungen an die geeignete Verantwortungs- und Befugnisebene zu übergeben.

> **Praxistipp**
>
> Eine gute Eskalation enthält:
>
> - konkrete Situation,
> - bekannte Auswirkungen,
> - bisherige Maßnahmen,
> - bestehendes Risiko,
> - benötigte Entscheidung,
> - mögliche Optionen,
> - und den spätesten sinnvollen Entscheidungszeitpunkt.

Ungeeignete Eskalation:

> Das System funktioniert nicht. Bitte entscheiden.

Besser:

> Der zentrale Dateiservice ist seit 09:10 Uhr für zwei Standorte nicht erreichbar. Die lokale Wiederherstellung war erfolglos. Eine Umschaltung auf das Ersatzsystem ist möglich, kann aber Datenänderungen der letzten 15 Minuten verlieren. Benötigt wird die Entscheidung, ob die Umschaltung durchgeführt und der mögliche Datenverlust akzeptiert wird.

Governance bei Incidents

Governance bestimmt unter anderem den Rahmen für:

- Priorisierung,
- Eskalation,
- Major-Incident-Kriterien,
- Kommunikation,
- Entscheidungsbefugnisse,
- Sicherheitsmeldungen,
- und Risikoakzeptanz.

Bei einem kritischen Incident sollte geklärt sein:

- Wer darf ein Major-Incident-Verfahren aktivieren?
- Wer übernimmt die Koordination?
- Wer darf Notfallmaßnahmen autorisieren?
- Wer informiert Führungskräfte, Kunden oder Behörden?
- Welche Risiken dürfen kurzfristig akzeptiert werden?
- Wer entscheidet über eine Wiederherstellung mit möglichen Nebenwirkungen?
- Welche Dokumentation ist zwingend erforderlich?
- Wann muss eine nachgelagerte Überprüfung stattfinden?

Governance soll die Wiederherstellung nicht unnötig verzögern.

Entscheidungsrechte und Notfallverfahren sollten deshalb vor einem Incident vorbereitet werden.

Governance bei Changes

Governance legt den Rahmen fest, innerhalb dessen Changes bewertet und autorisiert werden.

Dazu können gehören:

- Change-Modelle,
- Risikokriterien,
- Entscheidungsbefugnisse,
- Funktionstrennung,
- notwendige Tests,

- Rückfallplanung,
- Dokumentation,
- und nachgelagerte Überprüfung.

Nicht jeder Change benötigt dieselben Beteiligten oder dasselbe Gremium.

Die Autorisierung sollte sich richten nach:

- Risiko,
- Auswirkungen,
- Komplexität,
- Unsicherheit,
- betroffenen Services,
- und betrieblichen Vorgaben.

> **Typischer Fehler**
>
> Ein Change Advisory Board wird als zentrale Freigabestelle für jede kleine Änderung verwendet.
>
> Dadurch können unnötige Verzögerungen entstehen, ohne dass kritische Changes automatisch besser bewertet werden.

Governance bei Lieferanten

Externe Lieferanten können einen wesentlichen Teil eines Produkts oder Service bereitstellen.

Governance sollte unter anderem klären:

- Welche Leistung wird erwartet?
- Welche Risiken entstehen durch die Abhängigkeit?
- Welche Daten verarbeitet der Lieferant?
- Welche Sicherheitsanforderungen gelten?
- Welche Unterauftragnehmer werden eingesetzt?
- Wie wird die Leistung gemessen?
- Welche Eskalationswege bestehen?
- Welche Rechte bestehen bei Leistungsabweichungen?
- Wie können Daten und Services zurückgeführt werden?
- Was geschieht bei Vertragsende oder Ausfall des Lieferanten?

> **Merke**

> Die Auslagerung einer Tätigkeit überträgt nicht automatisch die gesamte Verantwortung für das Ergebnis oder die Risiken an den Lieferanten.

Governance bei künstlicher Intelligenz

ITIL Version 5 berücksichtigt ausdrücklich AI-gestützte Produkte, Services und Arbeitsweisen.

Governance für KI kann unter anderem behandeln:

- zulässige Anwendungsfälle,
- Verantwortlichkeit,
- verwendete Daten,
- Datenschutz,
- Informationssicherheit,
- Transparenz,
- Nachvollziehbarkeit,
- Verzerrungen,
- menschliche Kontrolle,
- Qualität der Ergebnisse,
- Überwachung,
- und gesetzliche Anforderungen.

Vor dem Einsatz einer KI-Lösung sollte unter anderem geprüft werden:

- Welches Outcome soll unterstützt werden?
- Welche Entscheidungen darf die KI beeinflussen?
- Welche Daten werden eingegeben oder gespeichert?
- Können vertrauliche Informationen offengelegt werden?
- Wie werden falsche Ergebnisse erkannt?
- Wer prüft kritische Entscheidungen?
- Wie werden Modelle oder Anbieteränderungen überwacht?
- Kann die Funktion bei Problemen deaktiviert werden?
- Wer trägt die Ergebnisverantwortung?

> **Sicherheitsrelevant**
>
> Die Verwendung einer KI-Lösung überträgt die Verantwortung für Entscheidungen und Folgen nicht automatisch auf das technische System oder den Anbieter.

Governance und Continual Improvement

Governance und Continual Improvement unterstützen sich gegenseitig.

Governance gibt unter anderem vor:

- welche Ziele wichtig sind,
- welche Risiken behandelt werden müssen,
- welche Ergebnisse überwacht werden,
- und welche Abweichungen nicht akzeptabel sind.

Continual Improvement nutzt unter anderem:

- Leistungsdaten,
- Feedback,
- Auditergebnisse,
- Incident-Erkenntnisse,
- Risikobewertungen,
- und Governance-Entscheidungen,

um Verbesserungen zu identifizieren und umzusetzen.

Beispiel:

Das Monitoring zeigt wiederholt, dass kritische Zertifikate erst kurz vor Ablauf erneuert werden.

Governance kann festlegen:

- kritische Zertifikate müssen zentral erfasst werden,
- Verantwortlichkeiten müssen eindeutig sein,
- Warnfristen müssen definiert werden,
- und die Einhaltung muss überwacht werden.

Continual Improvement entwickelt und verbessert anschließend:

- Erfassung,
- Alarmierung,
- Arbeitsabläufe,
- Automatisierung,
- und Erfolgskontrolle.

Praxisbeispiel: Ausfall eines zentralen Speichersystems

Ein zentrales Speichersystem zeigt kritische Fehler.

Technische Situation

- mehrere Hosts verwenden das Storage

- erste Datenträger zeigen Fehler
- ein Ersatzsystem ist vorhanden
- eine Umschaltung kann kurzzeitige Unterbrechungen verursachen
- der Datenstand des Ersatzsystems muss geprüft werden

Evaluate

- Welche Services sind betroffen?
- Wie hoch ist das Ausfallrisiko?
- Welche Daten könnten verloren gehen?
- Welche Alternativen bestehen?
- Welche Auswirkungen besitzt eine sofortige Umschaltung?
- Wie lange kann weiterbetrieben werden?

Direct

- Welche Services müssen zuerst geschützt werden?
- Wer darf die Umschaltung autorisieren?
- Welche Unterbrechung wird akzeptiert?
- Welche Stakeholder müssen informiert werden?
- Welche Datenverlustrisiken dürfen nicht überschritten werden?

Monitor

- Bleibt das Primärsystem stabil?
- Ist die Replikation aktuell?
- Funktioniert das Ersatzsystem?
- Werden die Services nach der Umschaltung wiederhergestellt?
- Werden alle offenen Risiken nachverfolgt?

Mögliche Verantwortlichkeiten

- Storage-Administrator: technische Analyse und Umsetzung
- Service Owner: Bewertung der Serviceauswirkungen
- Informationssicherheit oder Datenverantwortlicher: Bewertung des Datenrisikos
- Incident-Koordination: Koordination und Kommunikation
- autorisierte Entscheidungsrolle: Freigabe der risikobehafteten Umschaltung

Dieses Beispiel zeigt, dass technische Kompetenz, Management und Governance zusammenwirken müssen.

Typische Governance-Fehler

Fehler 1: Verantwortung ohne Befugnis

Eine Person soll für ein Ergebnis einstehen, besitzt aber keine Möglichkeit:

- Entscheidungen zu treffen,
- Ressourcen zu erhalten,
- Informationen einzufordern,
- oder Risiken zu eskalieren.

Fehler 2: Befugnis ohne Kontrolle

Eine Rolle darf weitreichende Entscheidungen treffen, ohne:

- Ergebnisse dokumentieren,
- Risiken begründen,
- oder über Auswirkungen berichten

zu müssen.

Fehler 3: Governance nur als Genehmigung verstehen

Viele Freigaben werden eingeführt, aber Ziele, Verantwortlichkeiten und Erfolgskriterien bleiben unklar.

Fehler 4: Jede Entscheidung zentralisieren

Auch risikoarme Tätigkeiten benötigen hochrangige Genehmigungen.

Dadurch entstehen:

- Verzögerungen,
- Überlastung,
- Umgehungslösungen,
- und unklare operative Verantwortung.

Fehler 5: Risiken ohne Befugnis akzeptieren

Ein technisches Team dokumentiert ein erhebliches Risiko, entscheidet aber eigenständig, es dauerhaft zu akzeptieren.

Fehler 6: Nur technische Leistung überwachen

Server und Anwendungen sind verfügbar, aber:

- Benutzer können ihre Aufgaben nicht ausführen,
- Lieferanten erfüllen Vereinbarungen nicht,
- oder Sicherheitsrisiken bleiben unbehandelt.

Fehler 7: Dokumentation mit Wirksamkeit verwechseln

Eine Richtlinie existiert, wird aber:

- nicht verstanden,
- nicht umgesetzt,
- nicht kontrolliert,
- oder durch Ausnahmen vollständig umgangen.

Fehler 8: Verantwortung bleibt an Teamgrenzen hängen

Jedes Team erfüllt seine Komponentenaufgabe, aber niemand verantwortet das Ende-zu-Ende-Ergebnis des Service.

Fehler 9: Governance nicht an Veränderungen anpassen

Entscheidungsmodelle und Kontrollen bleiben unverändert, obwohl sich:

- Technologie,
- Risiken,
- Organisationsstruktur,
- oder gesetzliche Anforderungen

verändert haben.

Fragen für eine neue Organisation

Beim Einstieg in eine neue IT-Organisation solltest du klären:

- Welche Governance-Gremien existieren?
- Wer bestimmt strategische IT-Ziele?
- Wer verantwortet wichtige Produkte und Services?
- Wer darf Risiken akzeptieren?
- Wer darf produktive Changes autorisieren?
- Welche Tätigkeiten sind delegiert oder vorab autorisiert?
- Welche Sicherheitsrichtlinien gelten?
- Welche Eskalationswege bestehen?
- Wie werden kritische Entscheidungen dokumentiert?
- Welche Kennzahlen werden überwacht?
- Wie werden Lieferanten gesteuert?
- Wie werden Ausnahmen behandelt?
- Wie werden Verbesserungen priorisiert?
- Wie werden Major Incidents gesteuert?
- Welche Notfallbefugnisse bestehen?

Entscheidungshilfe: Ist eine Governance-Entscheidung notwendig?

Eine Governance- oder übergeordnete Entscheidung kann erforderlich sein, wenn:

- mehrere Produkte oder Services betroffen sind,
- eine Entscheidung strategische Auswirkungen besitzt,
- erhebliche finanzielle Mittel benötigt werden,
- ein wesentliches Risiko akzeptiert werden soll,
- gesetzliche oder vertragliche Anforderungen betroffen sind,
- mehrere Verantwortungsbereiche im Konflikt stehen,
- eine grundlegende Richtlinie geändert werden soll,
- kritische Lieferantenabhängigkeiten entstehen,
- oder eine Entscheidung außerhalb bestehender Befugnisse liegt.

Eine operative Entscheidung kann dagegen innerhalb delegierter Befugnisse getroffen werden, wenn:

- Ziel und Rahmen eindeutig sind,
- das Risiko innerhalb festgelegter Grenzen liegt,
- ausreichende Fachkenntnisse vorhanden sind,
- und die notwendige Dokumentation und Kontrolle sichergestellt sind.

Checkliste für klare Verantwortlichkeiten

- ☐ Ist das gewünschte Ergebnis eindeutig?
- ☐ Ist bekannt, wer für das Ergebnis einsteht?
- ☐ Ist bekannt, wer die Aufgabe ausführt?
- ☐ Ist die Entscheidungsbefugnis eindeutig?
- ☐ Sind Fachberater und notwendige Beteiligte bekannt?
- ☐ Ist festgelegt, wer informiert werden muss?
- ☐ Besitzen die Rollen notwendige Informationen und Ressourcen?
- ☐ Sind Grenzen der delegierten Befugnisse bekannt?
- ☐ Besteht ein klarer Eskalationsweg?
- ☐ Ist geregelt, wer verbleibende Risiken akzeptieren darf?
- ☐ Wird das Ergebnis kontrolliert?
- ☐ Werden Entscheidungen nachvollziehbar dokumentiert?

Checkliste für wirksame Governance

- ☐ Sind Ziele und Prioritäten eindeutig?

- [ ] Sind Produkte, Services und kritische Outcomes bekannt?
- [ ] Werden Bedürfnisse und Risiken regelmäßig bewertet?
- [ ] Sind Richtlinien und Entscheidungsgrenzen verständlich?
- [ ] Sind Verantwortung und Rechenschaftspflicht eindeutig?
- [ ] Sind notwendige Befugnisse sinnvoll delegiert?
- [ ] Passen Kontrollen zum tatsächlichen Risiko?
- [ ] Werden relevante Ergebnisse und nicht nur Aktivitäten gemessen?
- [ ] Werden Sicherheits-, Datenschutz- und Vertragsanforderungen berücksichtigt?
- [ ] Werden Lieferanten und externe Abhängigkeiten überwacht?
- [ ] Werden Abweichungen eskaliert und behandelt?
- [ ] Werden Risiken nur durch befugte Rollen akzeptiert?
- [ ] Werden Governance-Vorgaben regelmäßig überprüft?
- [ ] Fließen Erkenntnisse in Continual Improvement ein?
- [ ] Wird unnötige Bürokratie vermieden?

Schnellreferenz

Frage	Governance-Bezug
Was wird benötigt?	Evaluate
Welche Optionen und Risiken bestehen?	Evaluate
Welches Ziel und welche Grenzen gelten?	Direct
Wer darf entscheiden?	Direct
Wer trägt die Ergebnisverantwortung?	Direct
Werden Vorgaben eingehalten?	Monitor
Werden Outcomes erreicht?	Monitor
Bleiben Risiken innerhalb akzeptierter Grenzen?	Monitor
Müssen Richtung oder Vorgaben angepasst werden?	erneutes Evaluate und Direct

---

Zusammenfassende Darstellung

> Bedürfnisse, Ziele, Risiken und Rahmenbedingungen
> ↓
> **Evaluate**
> Situation und Optionen bewerten

> ↓
> **Direct**
> Richtung, Verantwortung und Grenzen vorgeben
> ↓
> Management und technische Umsetzung
> ↓
> **Monitor**
> Ergebnisse, Risiken und Einhaltung überwachen
> ↓
> Feedback, Abweichungen und neue Anforderungen
> ↓
> erneute Bewertung und Anpassung

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
- 2.5 Die vier Dimensionen des Produkt- und Service-Managements
- 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
- Change Management
- Information Security Management
- Risk Management
- Supplier Management
- Service Level Management

Quellen und Versionsstand

Offizielle Grundlagen

- PeopleCert: ITIL Foundation – Version 5
- ITIL: New ITIL Explained for Certified Professionals
- PeopleCert: Introduction to the ITIL Maturity Model
- PeopleCert: ITIL Transformation – Version 5
- PeopleCert: ITIL FAQ

Einordnung

Die Aussagen zur Einbindung von Governance in das ITIL Value System sowie zu den Governance-Aktivitäten **Evaluate**, **Direct** und **Monitor** wurden anhand offizieller PeopleCert- und ITIL-Unterlagen geprüft.

Die Ausführungen zu:

- Entscheidungsbefugnissen,
- Verantwortung,
- RACI,
- Richtlinien,
- Kontrollen,
- Eskalation,
- Lieferanten,
- Backup-Governance,
- und den dargestellten Praxisfällen

sind zusätzliche herstellerneutrale Erläuterungen und Praxisempfehlungen dieses unabhängigen Nachschlagewerks.

Eine RACI-Matrix ist ein mögliches Hilfsmittel zur Rollenklärung, aber keine zwingend vorgeschriebene ITIL-Struktur.

Konkrete Governance-Gremien, Rollenbezeichnungen, Freigabestufen und Risikogrenzen müssen von der jeweiligen Organisation festgelegt werden.

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