
WHITEPAPER · PROJEKTSTEUERUNG & COMPLIANCE

IT Service Management, Governance und Compliance

HERAUSGEBER

Manuel Fernandez

VERÖFFENTLICHT

15. Oktober 2026

01 Executive Summary

Viele IT-Organisationen haben ein Ticketsystem, Prozessbeschreibungen und ein Sicherheitskonzept – und können dennoch nicht ohne Weiteres beantworten: „Wer entscheidet hier, nach welcher Regel, und wo ist das belegt?“

Die Kernthese dieses Papiers: Compliance entsteht nicht durch Dokumente neben dem Betrieb, sondern durch einen Betrieb, in dessen Abläufen Vorgaben, Verantwortlichkeiten und Nachweise bereits enthalten sind. Ausgangspunkt ist ein Servicekatalog, der festlegt, was die IT liefert und wer dafür verantwortlich ist. Daran setzen ITIL-orientierte Practices an – und an diesen die Kontrollen, die Regelwerke wie ISO/IEC 27001 oder die NIS2-Richtlinie verlangen.

Für CIO, Head of IT Operations und Informationssicherheitsbeauftragte (ISB) liefert das Papier eine Einordnung der gängigen Bezugsrahmen, ein Vorgehen in sechs Phasen, die erwarteten Artefakte, Erfolgsfaktoren und Risiken sowie eine Checkliste zur Standortbestimmung.

02 Problemstellung

Fachbereiche erwarten verlässliche, schnell bereitgestellte Services; gleichzeitig wächst die Regulierung – übergreifend etwa durch NIS2, im Finanzsektor durch DORA, dazu Datenschutz, Kundenverträge und interne Richtlinien. Beides trifft auf dieselben Teams, Werkzeuge und Abläufe. Typische Symptome:

- **Historisch gewachsene statt definierter Services:** Es fehlt eine gemeinsame Sicht, welcher Service welchen Geschäftsprozess unterstützt und wer ihn verantwortet.
- **Prozesse nur auf dem Papier:** Der dokumentierte Sollzustand ist im Werkzeug nicht abgebildet; Abweichungen fallen erst im Audit auf.
- **Unklare Verantwortung:** Besonders an Schnittstellen zu Informationssicherheit, Einkauf und Dienstleistern fühlen sich mehrere oder keine Stellen zuständig.
- **Compliance als Projekt:** Vor dem Audit werden Nachweise zusammengetragen, danach fällt die Organisation in den alten Zustand zurück.
- **Kontrollen ohne Betriebsbezug:** Unklar bleibt, in welcher Practice, durch welche Rolle und mit welchem Nachweis eine Kontrolle ausgeübt wird.

Die Folge ist doppelter Aufwand: Der Betrieb folgt eigenen Routinen, die Compliance-Funktion pflegt eine parallele Dokumentenwelt – ohne dass die Organisation besser steuerbar wird.

ABGRENZUNG ZU „VULNERABILITY AND PATCH MANAGEMENT“

Das DIP-Whitepaper „Vulnerability and Patch Management“ vertieft einen einzelnen sicherheitskritischen Ablauf: Schwachstellen erkennen, bewerten und über ein geregeltes Change Management beheben. Das vorliegende Papier beschreibt den Rahmen darüber – Servicekatalog, Practices, Rollen, Kontrollen und Steuerung –, in den sich Schwachstellen- und Patchmanagement als eine Practice unter mehreren einfügt. Beide Papiere ergänzen sich.

03 Bezugsrahmen: Governance, Management und Betrieb

ITIL, ISO/IEC 20000-1, ISO/IEC 27001 und COBIT sind keine konkurrierenden Alternativen; sie beantworten unterschiedliche Fragen und lassen sich kombinieren.

- **ITIL 4** beschreibt bewährte Praktiken des Service Managements (Service-Wertsystem, Wertschöpfungskette, Practices wie Incident Management oder Change Enablement). Es ist keine prüfbare Norm, sondern an das eigene Umfeld anzupassen.
- **ISO/IEC 20000-1** formuliert prüfbare Anforderungen an ein Service-Management-System; ITIL-orientierte Prozesse können dafür eine Grundlage sein.
- **ISO/IEC 27001:2022** regelt das Informationssicherheits-Managementsystem. Viele Maßnahmen aus Anhang A werden im IT-Betrieb ausgeübt – etwa im Änderungs-, Konfigurations-, Zugriffs- und Lieferantenmanagement.
- **COBIT 2019** (ISACA) trennt Governance (bewerten, vorgeben, überwachen) von Management und verknüpft IT-Ziele mit Unternehmenszielen.
- **BSI IT-Grundschutz** bietet eine konkrete, mit ISO/IEC 27001 kombinierbare Methodik für Sicherheitsmanagement und Schutzbedarfsfeststellung.

Für das Betriebsmodell ist die Trennung der Ebenen entscheidend: Die Governance legt Ziele, Risikoappetit, Richtlinien und Entscheidungsrechte fest; das Management übersetzt sie in Services, Practices und Kontrollen; der Betrieb erbringt die Services und erzeugt dabei die Daten, die als Nachweis und Steuerungsgrundlage zurückfließen. Welche Kombination der Bezugsrahmen sinnvoll ist, hängt von Regulierung, Kundenanforderungen und dem Ziel ab – interne Steuerbarkeit oder eine angestrebte formale Zertifizierung.

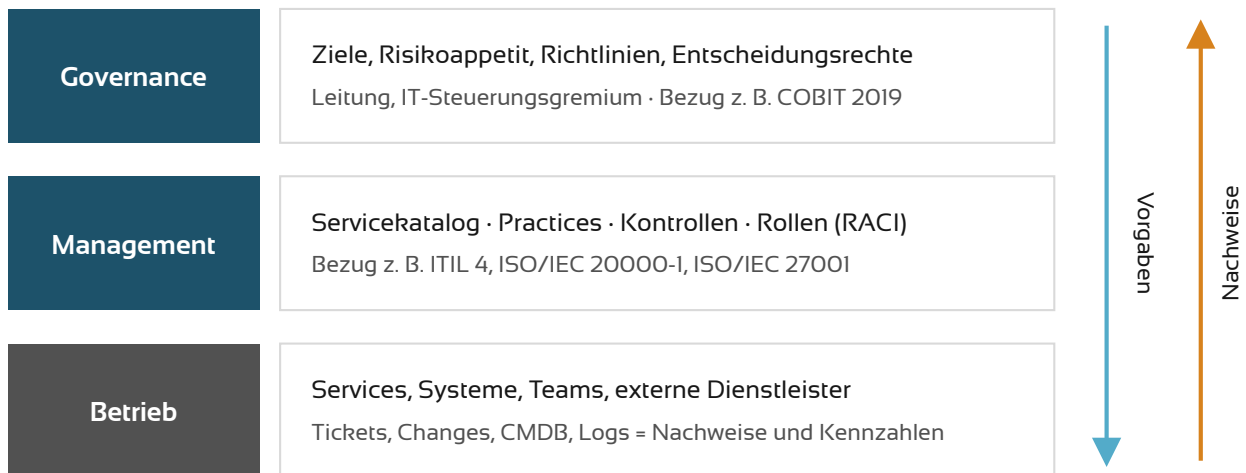


Abb. 1: Ebenenmodell eines integrierten ITSM-Betriebsmodells. Vorgaben fließen nach unten, Nachweise und Kennzahlen entstehen im Betrieb und fließen zurück in die Steuerung.

04 Vorgehen in sechs Phasen

Das Vorgehen ist iterativ: Es beginnt mit wenigen geschäftskritischen Services und wird schrittweise ausgeweitet. Gesteuert wird es als Projekt mit Governance, Statusberichten und Risikomanagement bis zur Übergabe in den Linienbetrieb.

01 Bestandsaufnahme und Zielbild

Erhoben werden geschäftskritische Prozesse, die unterstützenden IT-Leistungen, Prozess- und Werkzeuglandschaft, Rollen, Gremien sowie bekannte Schwachstellen aus Audits und Störungen. Parallel klärt die Leitung ihre Ziele – Transparenz, Kostenkontrolle, Audit-Fähigkeit, Qualität. Eine Reifegradeinschätzung, etwa angelehnt an das Reifegradmodell von COBIT, macht den Ausgangspunkt vergleichbar.

02 Regelwerke identifizieren, Anforderungen ableiten

Relevante Gesetze, Normen, Verträge und Richtlinien werden in prüfbare Anforderungen an Daten, Systeme und Abläufe übersetzt, jeweils mit Quelle und Verantwortlichem. Ob etwa die NIS2-Umsetzung greift, ist rechtlich zu klären; die Ableitung der betrieblichen Anforderungen ist Aufgabe des Betriebsmodells. Das Anforderungsregister macht Dopplungen sichtbar, die sich mit einer gemeinsamen Kontrolle bedienen lassen.

03 Servicekatalog definieren

Jeder Service wird mit Zweck, unterstütztem Geschäftsprozess, Leistungsumfang, Servicezeiten, Abhängigkeiten und Service Owner beschrieben – getrennt nach

geschäftlichem und technischem Katalog. Eine festgelegte Kritikalität bzw. ein Schutzbedarf steuert später, wie streng Kontrollen greifen.

04 Practices, Rollen und Kontrollen gestalten

Kern sind meist Incident, Service Request, Problem, Change Enablement, Service Configuration, Service Level, Supplier und Information Security Management. Je Practice werden Zweck, Ein- und Ausgaben, Rollen und Entscheidungspunkte beschrieben. Dort werden die Kontrollen verankert – mit ausführender Rolle, Frequenz und einem Nachweis, der möglichst im Werkzeug entsteht.

05 Werkzeugunterstützung und Einführung

Die Werkzeugfrage folgt den Anforderungen, nicht umgekehrt. Workflows, Pflichtfelder, Genehmigungen und Berichte bilden die Kontrollen ab; Wiederkehrendes wie Standard-Changes oder Berechtigungsrezertifizierungen wird automatisiert. Schulungen je Rolle und ein Pilot mit ausgewählten Services gehen der Ausweitung voraus. Ob eine vorhandene Plattform angepasst oder Standardsoftware neu ausgewählt wird, entscheidet eine Bewertung gegen die zuvor beschriebenen Anforderungen.

06 Steuerung und kontinuierliche Verbesserung

Kennzahlen, Service-Reviews mit den Fachbereichen, interne Kontrolltests und Management-Reviews schließen den Kreislauf. Erkenntnisse fließen in ein priorisiertes Verbesserungsregister – im Sinne von ITIL 4 (Continual Improvement) und des Plan-Do-Check-Act-Zyklus der Managementsystem-Normen. Damit das Modell das Projektende überdauert, sind Owner, Termine und Berichtswege des Regelbetriebs bereits vor der Übergabe festgelegt.

HYPOTHETISCHES BEISPIEL: DREI QUELLEN, EINE KONTROLLE

Ein Unternehmen stellt fest, dass ISMS, ein Kundenvertrag und eine interne Richtlinie gleichermaßen verlangen, Änderungen an produktiven Systemen zu bewerten, zu genehmigen und nachvollziehbar zu dokumentieren. Statt dreier Nachweise wird eine Kontrolle „Genehmigung normaler Changes vor Umsetzung“ im Change-Workflow verankert: ausgeübt durch die Change Authority, belegt durch den Genehmigungsschritt im Ticket, quartalsweise per Stichprobe geprüft. Alle drei Quellen verweisen im Register auf diese Kontrolle.

05 Verantwortlichkeiten und Steuerung

Zu unterscheiden sind Verantwortung für einen Service (Service Owner), für eine Practice (Practice Owner) und für eine Kontrolle (Control Owner). In kleineren Organisationen kann eine Person mehrere Rollen tragen – entscheidend ist die ausdrückliche Zuordnung.

Die RACI-Matrix legt je Aktivität fest, wer durchführt (Responsible), wer verantwortet und entscheidet (Accountable), wer einzubeziehen (Consulted) und wer zu informieren ist (Informed). Wirksam wird sie durch zwei Regeln: genau ein A je Aktivität, und Rollen statt Personen – die Personenzuordnung wird getrennt gepflegt. Die Matrix darf nach Risiko differenzieren: Für vorab genehmigte Standard-Changes entfällt die Einzelgenehmigung, für Changes mit hohem Risiko wird die Change Authority erweitert.

Aktivität	Antrags-steller	Service Owner	Change Manager	Change Authority	Techn. Betrieb	ISB
Change beantragen und begründen	R	A	I	–	C	–
Risiko und Auswirkung bewerten	C	A	R	–	C	C
Change genehmigen	I	C	R	A	I	C
Change umsetzen und testen	I	A	I	–	R	–
Review nach Umsetzung	I	C	A/R	I	C	I

Abb. 2: Hypothetisches Beispiel einer RACI-Matrix für Change Enablement (Ausschnitt). R = Responsible, A = Accountable, C = Consulted, I = Informed; je Aktivität genau ein A. Die konkrete Zuordnung hängt von Organisation und Kritikalität des Services ab.

Gremien und Kennzahlen

Das Modell braucht wenige, klar zugeschnittene Gremien: ein Steuerungsgremium auf Leitungsebene für Prioritäten, Risikoakzeptanzen und Budget, Service-Reviews mit den Fachbereichen und eine risikoabhängig besetzte Change Authority – jeweils mit Zweck, Teilnehmern, Befugnissen und Rhythmus. Die NIS2-Richtlinie sieht zudem vor, dass Leitungsorgane betroffener Einrichtungen die Cybersicherheits-Risikomanagementmaßnahmen billigen, ihre Umsetzung überwachen und an Schulungen teilnehmen; durchgängige Entscheidungs- und Berichtswege schaffen dafür die organisatorische Grundlage.

Kennzahlen sollen Entscheidungen auslösen: Ergebniskennzahlen je Service (z. B. Einhaltung vereinbarter Servicezeiten), Leistungskennzahlen je Practice (z. B. Anteil erfolgreicher Changes, Wiederholungsstörungen) und Kontrollkennzahlen (z. B. fristgerecht durchgeführte Kontrollen, offene Feststellungen). Zielwerte sind je Organisation festzulegen; allgemeingültige Richtwerte gibt es nicht.

06 Artefakte und Deliverables

Am Ende des Vorhabens sollten die folgenden Ergebnisse vorliegen. Umfang und Detaillierungsgrad richten sich nach Größe und Regulierungsdichte der Organisation; wichtiger als Vollständigkeit ist, dass die Artefakte im Betrieb tatsächlich genutzt werden.

Steuerung und Organisation

- Zielbild mit Ebenen, Gremien und Entscheidungsrechten
- Rollenbeschreibungen und RACI-Matrizen je Practice
- Gremienordnungen
- Kennzahlenmodell mit Definitionen und Datenquellen
- Reifegradeinschätzung, Roadmap, Verbesserungsregister

Services, Practices und Kontrollen

- Servicekatalog mit Service Ownern und Kritikalität
- Practice-Beschreibungen mit Entscheidungspunkten
- Anforderungsregister mit Quelle und Kontrollbezug
- Kontrollkatalog mit Control Owner, Frequenz, Nachweisart
- Werkzeugkonzept und Schulungsunterlagen je Rolle

Register und Kontrollkatalog bilden zusammen die Kette Regelwerk → Anforderung → Kontrolle → Rolle → Nachweis. Diese Rückverfolgbarkeit zeigt bei jeder Änderung eines Regelwerks, einer Rolle oder eines Werkzeugs, was betroffen ist. Jedes Artefakt braucht einen Owner und einen Aktualisierungsrhythmus.

07 Erfolgsfaktoren und Risiken

Erfolgsfaktoren

- **Mandat der Leitung** mit verbindlicher Zuweisung von Entscheidungsrechten
- **Vom Service her denken** statt von Prozessen oder Werkzeugen
- **Klein starten** mit kritischen Services und Kern-Practices
- **Nachweise im Werkzeug** als Nebenprodukt der Arbeit
- **Ein gemeinsames Register** für Betrieb, Sicherheit und Compliance

Risiken

- **Framework-Dogmatismus:** ITIL komplett „einführen“ statt zuschneiden
- **Werkzeug zuerst:** Die Plattform zementiert den Ist-Zustand
- **Papiercompliance:** Richtlinien ohne Verankerung im Ablauf
- **Überregulierung:** gleich strenge Kontrollen für alle Services
- **Dienstleisterlücken und fehlender Regelbetrieb** nach Projektende

Besondere Aufmerksamkeit verdienen Dienstleister: Viele Betriebsleistungen erbringen externe Partner oder Cloud-Anbieter, die Verantwortung für das Ergebnis bleibt jedoch in der Regel beim Auftraggeber. Verträge, Leistungsscheine und Schnittstellen müssen deshalb Servicequalität, Sicherheitsanforderungen und Nachweispflichten bis zum Dienstleister durchreichen – und ausgelagerte Leistungen gehören in Servicekatalog, RACI und Kontrollkatalog.

HYPOTHETISCHES BEISPIEL: PAPIERCOMPLIANCE

Eine Richtlinie schreibt die halbjährliche Überprüfung privilegierter Berechtigungen vor, im Werkzeug ist dafür aber nichts hinterlegt. Die Kontrolle erhält einen Control Owner, einen wiederkehrenden Auftrag mit Frist und einen Bericht über offene Rezertifizierungen. Die Richtlinie bleibt gleich – neu ist, dass ihre Einhaltung sichtbar wird.

08 Checkliste

Jede mit „nein“ oder „unklar“ beantwortete Frage markiert ein Handlungsfeld.

- Ordnet ein aktueller Servicekatalog Services den unterstützten Geschäftsprozessen zu?
- Hat jeder Service einen Service Owner und eine festgelegte Kritikalität?
- Sind Servicezeiten und Qualitätsziele mit den Fachbereichen vereinbart?
- Sind ausgelagerte Leistungen mit Verantwortlichen auf beiden Seiten erfasst?
- Sind die Kern-Practices beschrieben, im Werkzeug abgebildet und mit einem Owner versehen?

- Bildet die CMDB Abhängigkeiten zwischen Services und Komponenten nachvollziehbar ab?
- Ist die Anwendbarkeit der Regelwerke (etwa NIS2 oder sektorspezifischer Vorgaben) geklärt?
- Ist jede Anforderung im Register einer Quelle und einer Kontrolle zugeordnet?
- Hat jede Kontrolle Control Owner, Frequenz und Nachweisart – und entsteht der Nachweis im Werkzeug?
- Gibt es je Aktivität genau eine verantwortliche Stelle (A) in den RACI-Matrizen?
- Entscheidet ein Steuerungsgremium auf Basis von Kennzahlen, Risiken und Feststellungen?
- Wird ein priorisiertes Verbesserungsregister nach Audits, Störungen und Reviews fortgeschrieben?

09 Nächster Schritt

Ein sinnvoller Einstieg ist eine kompakte Bestandsaufnahme entlang der Checkliste für wenige geschäftskritische Services. Sie zeigt, wo Services, Rollen und Kontrollen tragen, und ergibt eine priorisierte Maßnahmenliste für eine Roadmap.

Die DIP unterstützt dabei in einzelnen Abschnitten oder über das gesamte Vorhaben: von der Erfassung geschäftskritischer Prozesse und der Definition von Rollen über die Gestaltung der IT-Organisation auf Basis von Best-Practice-Ansätzen wie ITIL und COBIT, die Ableitung von Anforderungen und Kontrollmechanismen aus relevanten Regelwerken und die Evaluierung von Standardsoftware bis zu Einführung, Schulung und Projektsteuerung.

10 Quellen und Standards

Dieses Whitepaper dient der fachlichen Orientierung; es ist keine Rechtsberatung, Prüfung oder Zertifizierung und sichert keine Konformität zu. Anwendbarkeit und Auslegung von Regelwerken sind im Einzelfall mit Fachfunktionen, Prüfern oder Rechtsberatern zu klären; alle Beispiele sind hypothetisch. Maßgeblich sind die Originaldokumente in ihrer aktuellen Fassung:

- **ITIL 4** – Leitfaden für IT Service Management (AXELOS, heute PeopleCert)
- **ISO/IEC 20000-1** – Service management system requirements
- **ISO/IEC 27001:2022** – Information security management systems – Requirements
- **COBIT 2019** – Governance und Management der Unternehmens-IT (ISACA)
- **BSI IT-Grundschutz** – BSI-Standards 200-1 bis 200-3 und IT-Grundschutz-Kompodium
- **Richtlinie (EU) 2022/2555** (NIS2) einschließlich nationaler Umsetzung
- **Verordnung (EU) 2022/2554** (DORA) für den Finanzsektor

Lassen Sie uns sprechen

Für Infos zu diesem und weiteren spannenden Themen freuen wir uns auf den Austausch mit Ihnen!

UNTERNEHMEN

DIP Deutsche IT und
Projektberatungsgesellschaft mbH
Rahmannstraße 11 · 65760 Eschborn
info@dip-consulting.de
dip-consulting.de

IHR ANSPRECHPARTNER

Manuel Fernandez

Management Consultant, Geschäftsführer
info@dip-consulting.de

Seit 2013 ist Herr Fernandez Geschäftsführer der Deutschen IT und Projektberatungsgesellschaft und seit 16 Jahren als IT-Berater in vielfältigen Rollen bei strategischen als auch bei implementierungsnahen Projekten im Einsatz.

