

Abstimmung der Vorgaben zur Leistungserbringung

Professionelles Management der vertraglichen Anforderungen in IT-Projekten

Präzise Prüfung der vertraglichen Vorgaben



Systematischer Soll-Ist-Vergleich

Die kontinuierliche Prüfung der Leistungserbringung erfolgt ausschließlich anhand der vertraglich vereinbarten Grundlagen. Vertrag, Leistungsbeschreibung und SLA dienen als verbindliche Referenz – nicht das subjektive Bauchgefühl.

Der regelmäßige Soll-Ist-Vergleich umfasst alle wesentlichen Dimensionen: Leistungsumfang, Qualitätskriterien, Terminplanung, Zuständigkeiten und erforderliche Nachweise. Jede Änderung muss über einen formalen Change-Request erfolgen, um schlechrenden Scope-Creep zu verhindern.

Nachweisführung und Dokumentation

Tickets

Strukturierte Aufzeichnung aller Anfragen, Incidents und Service-Requests mit Status und Bearbeitungszeit

Protokolle

Meeting-Protokolle, Statusberichte und Entscheidungsdokumentationen als Nachweis der Projektkommunikation

Test-Ergebnisse

Abnahmeergebnisse, Testprotokolle und Qualitätsnachweise für alle gelieferten Komponenten

Schulungsnachweise

Dokumentierte Übergaben, Einweisungen und Schulungsbestätigungen der relevanten Stakeholder

Diese systematische Nachweisführung schafft Transparenz und rechtliche Sicherheit für alle Projektbeteiligten. Nur dokumentierte Leistungen gelten als erbracht.

Prüffragen zur Leistungsabstimmung

1

Vertragliche Vorgaben

Welche vertraglichen Vorgaben prüfst du in einem IT-Projekt regelmäßig, und in welcher Form (Nachweis)?

2

Scope-Creep Erkennung

Wie erkennst du „Scope-Creep“ früh, und wie stoppst du ihn sauber?

3

Soll-Ist-Vergleich

Welche Informationen müssen in einem Soll-Ist-Vergleich stehen, damit er im Streitfall taugt?

4

Abnahme vs. Erbringung

Was ist der Unterschied zwischen „Leistung erbracht“ und „Leistung abgenommen“?

Stilllegung von Altsystemen & Inbetriebnahme neuer Systeme



Ein strukturierter Abschaltplan minimiert Risiken und stellt die Kontinuität des Betriebs sicher.

Decommissioning Excellence

Die Stilllegung von Altsystemen erfordert eine systematische Prüfung aller Abhängigkeiten: Schnittstellen, aktive Nutzer, automatisierte Jobs und bestehende Datenflüsse.

Der Abschaltplan definiert präzise den Zeitpunkt, Verantwortliche und einen detaillierten Rückfallplan (Rollback) für den Notfall. Sicherheitsrelevante Elemente wie Accounts, Keys, Zertifikate, Firewall-Regeln und Zugriffe werden vollständig entfernt.

Qo-Live und Cutover-Management

Strukturierte Inbetriebnahme

Der Cutover-Plan definiert alle notwendigen Schritte mit präzisen Zeitfenstern, einen umfassenden Kommunikationsplan und kontinuierliches Monitoring während der kritischen Phase.

Vor dem Go-Live erfolgen Smoke-Tests zur Basisprüfung. Nach der Inbetriebnahme startet die Hypercare-Phase mit intensivem Engpass-Handling und erhöhter Supportbereitschaft.

Die Akzeptanzkriterien müssen vor dem Go-Live eindeutig definiert und von allen Stakeholdern bestätigt sein. Das Asset-Management wird aktualisiert: Inventar/CMDB, Lizenzverwaltung und bei Bedarf Hardware-Entsorgung.



Abschaltplan

Zeitpunkt, Rückfallplan,
Verantwortliche



Sicherheit

Entfernung aller Zugriffe und
Credentials



Qo-Live

Tests, Monitoring, Hypercare-Phase

Archivierung: Langfristige Datensicherung

Archiv ist nicht Backup

Während Backups der kurzfristigen Wiederherstellung nach Fehlern oder Datenverlust dienen, ermöglicht das Archiv eine langfristige, unveränderbare und prüfbare Aufbewahrung gemäß Compliance-Anforderungen.

Zentrale Entscheidungen: Welche Daten, Formate und Metadaten müssen archiviert werden? Wie lange gelten Aufbewahrungsfristen? Wer erhält Zugriff? Wie erfolgt die Löschung nach Fristablauf?

Bei der Datenmigration sind Format-Kompatibilität, Lesbarkeit über Jahre, Integrität durch Checksums und ein durchdachtes Zugriffskonzept entscheidend. Nicht lesbare Archivdaten nach Systemabschaltung sind rechtlich und operativ fatal.

Dokumentation der erbrachten Leistung

Nachweis, Betriebssicherheit und professionelle Übergabe

Die vollständige Dokumentation dient drei zentralen Zwecken: dem rechtssicheren Nachweis erbrachter Leistungen, der Gewährleistung der Betriebssicherheit und der professionellen Übergabe an den laufenden Betrieb.

01

Leistungsnachweise

Protokolle über gelieferte Leistungen mit präziser zeitlicher und inhaltlicher Dokumentation

02

Konfigurationen

Vollständige Dokumentation von Netzwerk, Systemen, Accounts, Rollen, Policies und Versionsständen

03

Test- und Abnahme

Testprotokolle, Abnahmeprotokoll und strukturierte Restpunkteliste (Open Issues)

04

Betriebsdokumentation

Monitoring-Konzept, Backup/Restore-Prozeduren, Notfallwege, Wartungsanleitungen sowie Nutzer- und Admin-Handbücher

Entscheidend ist: Die Dokumentation muss jederzeit auffindbar, aktuell und versionssicher sein. Nur so entfaltet sie ihren vollen Wert für den Projektabschluss und den stabilen Betrieb.