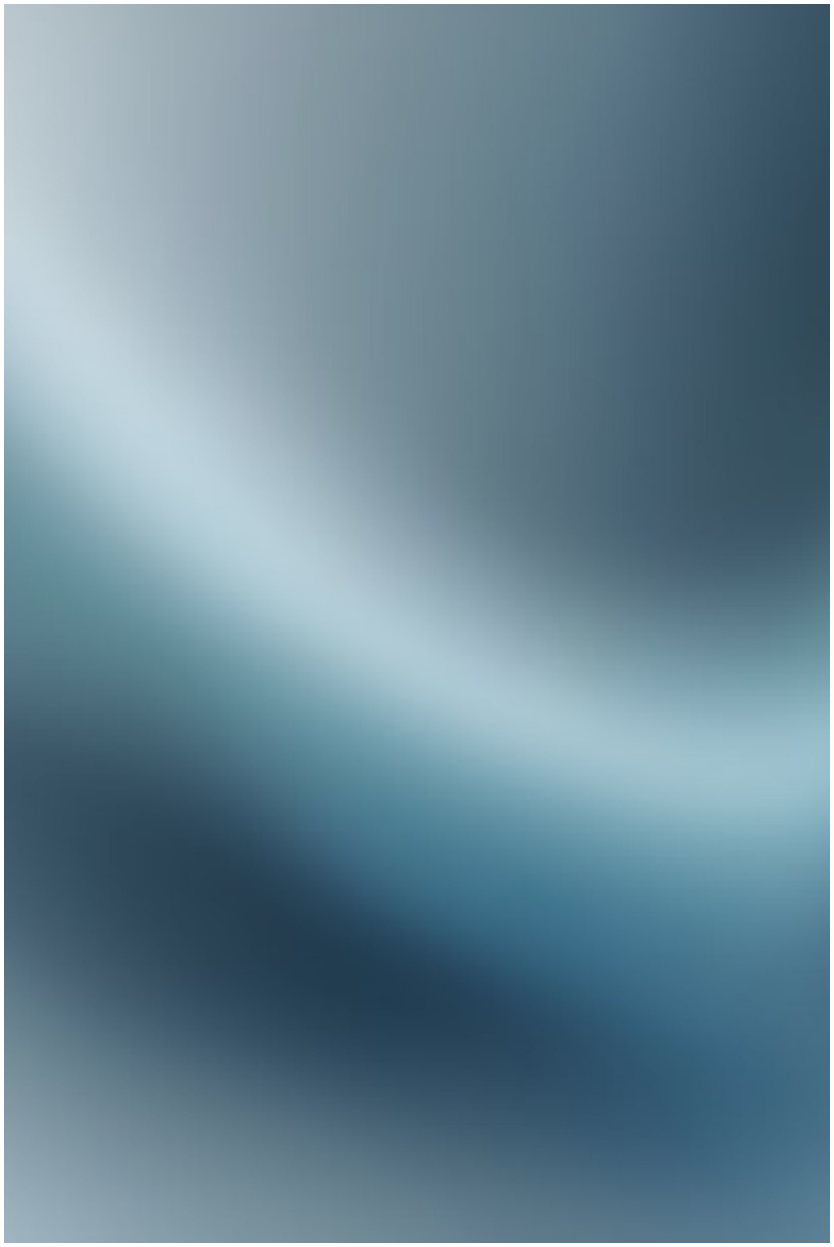


# Leistungserbringung bewerten (AP1 8.8)

*Die systematische Bewertung der Leistungserbringung ist ein kritischer Erfolgsfaktor im Projektabschluss. Sie prüft, ob vereinbarte Leistungen tatsächlich wie spezifiziert geliefert wurden – und bewertet deren Qualität objektiv anhand messbarer Kriterien.*

*Die Kernkette folgt einer klaren Logik: Zunächst erfolgen Abnahme und Nachweisprüfung, dann der strukturierte Soll-Ist-Vergleich, gefolgt von der Abweichungsanalyse und schließlich der Ableitung konkreter Maßnahmen sowie Lessons Learned für zukünftige Projekte.*

# Die fünf Bewertungsdimensionen

### Leistung

*Sind alle Muss-Anforderungen erfüllt? Wurden vereinbarte Funktionen vollständig implementiert?*

### Zeit

*Wurden Meilensteine und Endtermine eingehalten? Wie groß sind zeitliche Abweichungen?*

### Kosten

*Liegt das Projekt im Budget? Welche Mehrkosten sind entstanden und warum?*

### Qualität

*Entspricht die Ausführung den Qualitätsstandards? Sind Tests erfolgreich?*

### Umfang (Scope)

*Wurde der vereinbarte Leistungsumfang vollständig umgesetzt ohne ungenehmigte Änderungen?*

*Ohne lückenlose Belege und Protokolle ist eine Aussage „fertig" im Streitfall wertlos. Dokumentation ist nicht Bürokratie, sondern Rechtssicherheit.*

# Abnahme & Nachweise: Was wirklich übergeben wird

## Formelle Abnahme

*Das Abnahme-/Übergabeprotokoll bildet die formelle Bestätigung mit Datum, Unterschriften aller Beteiligten und eindeutigem Ergebnis.*

## Technische Nachweise

- *Installations-/Lieferschein-Nachweise dokumentieren, was wo installiert oder geliefert wurde*
- *Testprotokolle belegen HA-Failover, Backup-Restore, Performance-Durchsatz und Security-Checks*
- *Technische Dokumentation umfasst Konfiguration, Übergabe kritischer Informationen und Betriebsanleitungen*
- *Schulungs-/Einweisungsnachweise zeigen, wer in welchen Bereichen eingewiesen wurde*

PRAXISFALL

# Firewall-Tausch: Welche Nachweise erwarten Sie?

1

## Installations-Nachweis

*Lieferschein der neuen Firewall-Hardware, Standort-Dokumentation, Netzwerkanbindung mit Port-Zuordnung*

2

## Testprotokolle

*Funktionstest aller Regeln, HA-Failover-Test, Performance-Messung, Security-Scan, Backup/Restore-Verifikation*

3

## Konfigurationsdokumentation

*Regelwerk dokumentiert, Netzwerkplan aktualisiert, Monitoring-Anbindung, Backup-Konzept, Rollback-Plan*

4

## Einweisung & Übergabe

*Admin-Schulung durchgeführt, Zugangskonzept übergeben, Supportweg definiert, Incident-Ablauf geklärt*

*Ein Abnahmeprotokoll ist mehr als Papierkram – es schützt beide Seiten vor späteren Missverständnissen und ist die Grundlage für Gewährleistungsansprüche.*

# Das Abnahmeprotokoll im Detail

## Pflichtinhalte

*Ein prüfungsfestes Abnahmeprotokoll muss sechs zentrale Elemente enthalten, um rechtssicher und nachvollziehbar zu sein.*

01

### Gegenstand & Umfang

*System, Version, exakte Leistungsbeschreibung*

02

### Beteiligte & Rollen

*Alle Parteien mit Funktion und Unterschrift*

03

### Ort, Datum, Uhrzeit

*Präzise zeitliche und örtliche Einordnung*

04

### Eindeutiges Ergebnis

*Abgenommen / mit Mängeln / nicht abgenommen*

05

### Detaillierte Mängelliste

*Beschreibung, Priorität, Frist, Verantwortlicher*

06

### Nachvollziehbarkeit

*Referenzen auf Testprotokolle und Dokumentation*

# Testprotokolle & Dokumentationsübergabe

## Testprotokoll-Standards

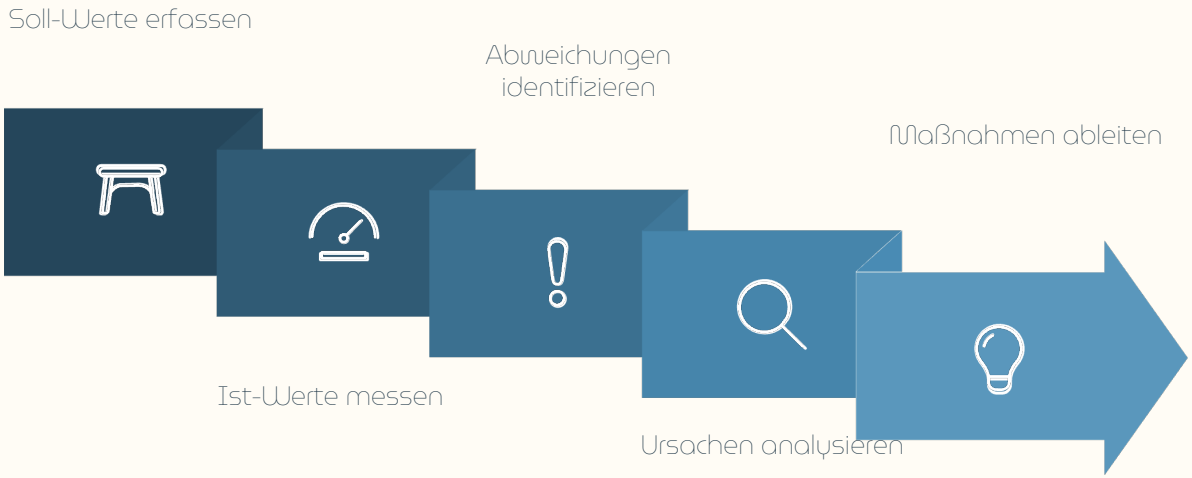
*Ein reproduzierbares Testprotokoll enthält Testziel, detaillierten Testaufbau, Schritt-für-Schritt-Anleitung, Soll-Ergebnis, dokumentiertes Ist-Ergebnis sowie Nachweise in Form von Logs oder Screenshots. Bei HA- und Backup-Tests sind Wiederholbarkeit und klare Erfolgskriterien essenziell.*

## Betriebsdokumentation

*Die Betriebsübergabe umfasst Konfigurationsdateien, Netzwerkpläne mit Regelwerk, Monitoring- und Alarmierungskonzept, Backup/Restore-Prozeduren sowie einen detaillierten Rollback-Plan.*

*Bei Schnittstellen sind Endpunkte, Datenformate, Authentifizierungsmethoden und Beispiel-Requests zu dokumentieren. Die Einweisung klärt Bedienung, Admin-Zugangs-Prozesse, Supportwege und den Notfall-/Incident-Ablauf – damit der Kunde nicht am ersten Betriebstag eskaliert.*

# Soll-Ist-Vergleich: Systematische Abweichungsanalyse




## Typische Ursachen-Kategorien

- *Anforderungen oder Informationen zu spät oder unklar kommuniziert*
- *Technische Probleme, Kompatibilitätsfehler oder unerwartete Bugs*
- *Ressourcenengpässe, verlängerte Lieferzeiten, verzögerte Freigaben*
- *Zu optimistische Planungsannahmen ohne ausreichende Puffer*
- *Langwierige Kommunikations- und Entscheidungsprozesse*

*Die Impact-Bewertung erfolgt in drei Stufen: kritisch (Betrieb gefährdet), mittel (Einschränkungen möglich) oder gering (keine unmittelbaren Auswirkungen).*

# Praxisfall: Firewall-HA-Projekt

## Situation

***Geplant:*** *12 Stunden Implementierungszeit*

***Ist-Aufwand:*** *16 Stunden (33% Überschreitung)*

***Ursache:*** *DNS/Proxy-Konfiguration komplexer als erwartet, Failover-Test musste wiederholt werden*

## Lessons Learned

***Vor Umsetzung:*** *Abnahmekriterien und alle Testfälle (HA, DNS, Proxy) im Vorfeld fixieren und dokumentieren*

***Planung:*** *Realistische Zeitpuffer einplanen, Abhängigkeiten (Freigaben, externe Infos) transparent machen*

***Prozess:*** *Standard-Checkliste und Rollback-Plan verpflichtend in jedem Change einsetzen*

> *Konkrete Maßnahmen: Projektleiter erstellt bis KW 12 eine erweiterte Change-Checkliste mit DNS/Proxy-spezifischen Prüfpunkten. IT-Betrieb definiert bis KW 14 Mindest-Zeitpuffer für HA-Implementierungen (20%). Team lead etabliert bis KW 10 verpflichtende Pre-Implementation-Reviews.*