Muster-Prüfprogramm

IT-Projekte

12 Prüfschritte · ISO 27001, DSGVO, GoBD

12 Prüfschritte mit Kriterium, Fundstelle, Prüfhandlung und erwarteten Nachweisen. 8 Unterlagen zur Anforderung und die typischen Feststellungen.

ISO 21502:2020 · ISO/IEC 27001:2022 Anhang A 5.8 · ISO/IEC 27001:2022 Anhang A 5.8 und 8.26 · Art. 25 und 35 DSGVO · ISO/IEC 27001:2022 Anhang A 8.29 · GoBD Rz. 142 · ISO/IEC 27001:2022 Anhang A 8.32

Prüfungsziel und Geltungsbereich

Die Prüfung beurteilt, ob ein IT-Projekt mit klarem Auftrag, geeigneter Organisation und wirksamer Steuerung von Zeit, Budget, Umfang und Risiken durchgeführt wird. Sie beurteilt außerdem, ob Anforderungen an Informationssicherheit und Datenschutz eingebracht, Tests und Abnahmen dokumentiert, Daten vollständig und richtig migriert und der Betrieb ordnungsgemäß übergeben werden.

GELTUNGSBEREICH

- Ein ausgewähltes laufendes oder kürzlich abgeschlossenes IT-Projekt
- Projektauftrag, Projektorganisation, Planung, Berichterstattung und Änderungssteuerung
- Sicherheits- und Datenschutzanforderungen, Test, Abnahme, Datenmigration und Betriebsübergabe
- Nicht Gegenstand: die fachliche Richtigkeit einzelner Lösungsentscheidungen

Prüfschritte 1 bis 3

Schritt 01 ISO 21502:2020; ISO/IEC 27001:2022 Anhang A 5.8

Für Projekte gilt eine verbindliche Methode mit Phasen und Entscheidungspunkten.

Prüfhandlung Methode lesen und für das ausgewählte Projekt prüfen, ob die vorgesehenen Entscheidungspunkte durchlaufen wurden.

Nachweise Projektmanagementhandbuch, Nachweise der Phasenentscheidungen

Schritt 02 ISO 21502:2020

Ein freigegebener Projektauftrag beschreibt Ziel, Nutzen, Umfang, Budget und Termine.

Prüfhandlung Projektauftrag und Wirtschaftlichkeitsbetrachtung lesen und Freigabe durch den Auftraggeber prüfen.

Nachweise Projektauftrag, Wirtschaftlichkeitsbetrachtung, Freigabevermerk

Schritt 03 ISO 21502:2020

Die Projektorganisation mit Auftraggeber, Lenkungsausschuss und Projektleitung ist festgelegt und arbeitet nachweisbar.

Prüfhandlung Organigramm des Projekts und Protokolle des Lenkungsausschusses auf Entscheidungen und Eskalationen prüfen.

Nachweise Projektorganigramm, Protokolle des Lenkungsausschusses

Prüfschritte 4 bis 6

Schritt 04 ISO/IEC 27001:2022 Anhang A 5.8 und 8.26

Informationssicherheit ist im Projekt verankert: Schutzbedarf und Sicherheitsanforderungen sind früh ermittelt.

Prüfhandlung Prüfen, ob Schutzbedarf und Sicherheitsanforderungen dokumentiert und vom Sicherheitsbeauftragten bewertet wurden.

Nachweise Schutzbedarfsfeststellung, Sicherheitsanforderungen, Stellungnahme der Informationssicherheit

Schritt 05 Art. 25 und 35 DSGVO

Datenschutz ist durch Technikgestaltung berücksichtigt; wo nötig ist eine Datenschutz-Folgenabschätzung durchgeführt.

Prüfhandlung Einbindung des Datenschutzes nachvollziehen und die Schwellwertprüfung oder Folgenabschätzung ansehen.

Nachweise Stellungnahme des Datenschutzbeauftragten, Schwellwertprüfung, Folgenabschätzung

Schritt 06 ISO 21502:2020; ISO/IEC 27001:2022 Anhang A 5.8

Projektrisiken einschließlich der Risiken für die Informationssicherheit werden geführt, bewertet und mit Maßnahmen und Verantwortlichen nachverfolgt.

Prüfhandlung Risikoliste auf Aktualität prüfen und für drei Risiken Maßnahmen und Status nachvollziehen.

Nachweise Risikoliste, Statusberichte

Prüfschritte 7 bis 9

Schritt 07 — ISO 21502:2020

Fortschritt, Budget und Termine werden regelmäßig gemessen und an den Auftraggeber berichtet.

Prüfhandlung Statusberichte mit Plan-Ist-Vergleich von Kosten und Terminen auswerten.

Nachweise Statusberichte, Projektplan, Budgetübersicht

Schritt 08 — ISO 21502:2020

Änderungen am Projektumfang werden beantragt, bewertet und genehmigt.

Prüfhandlung Änderungsanträge auf Bewertung von Kosten, Zeit und Risiko sowie auf Genehmigung prüfen.

Nachweise Änderungsanträge, Genehmigungen

Schritt 09 — ISO/IEC 27001:2022 Anhang A 8.29

Tests und Abnahme erfolgen nach dokumentierten Kriterien; Sicherheitstests sind einbezogen.

Prüfhandlung Testkonzept, Testergebnisse und Abnahmeprotokoll ansehen und offene Fehler bei Abnahme bewerten.

Nachweise Testkonzept, Testprotokolle, Abnahmeprotokoll

Prüfschritte 10 bis 12

Schritt 10 — GoBD Rz. 142

Datenmigrationen werden auf Vollständigkeit und Richtigkeit geprüft; Altdaten bleiben für die Aufbewahrungsfrist auswertbar.

Prüfhandlung Migrationskonzept und Abstimmungsnachweise wie Summen und Satzzahlen prüfen und den Umgang mit dem Altsystem klären.

Nachweise Migrationskonzept, Abstimmungsprotokolle, Konzept für Altdaten

Schritt 11 — ISO/IEC 27001:2022 Anhang A 8.32

Die Übergabe in den Betrieb erfolgt über den Änderungsprozess mit Betriebsdokumentation und Verantwortlichen.

Prüfhandlung Übergabeprotokoll und Änderungsantrag für die Inbetriebnahme prüfen.

Nachweise Übergabeprotokoll, Betriebshandbuch, Änderungsantrag

Schritt 12 — ISO 21502:2020

Das Projekt wird formal abgeschlossen; Erfahrungen und Nutzenerreichung werden ausgewertet.

Prüfhandlung Abschlussbericht lesen und prüfen, ob eine Nutzenbewertung geplant oder durchgeführt ist.

Nachweise Abschlussbericht, Auswertung der Erfahrungen, Nutzenbewertung

Unterlagenanforderung

Diese 8 Unterlagen vor Prüfungsbeginn anfordern

1. Projektmanagementhandbuch
2. Projektauftrag und Wirtschaftlichkeitsbetrachtung
3. Protokolle des Lenkungsausschusses und Statusberichte
4. Risikoliste und Änderungsanträge
5. Schutzbedarfsfeststellung und Sicherheitsanforderungen
6. Stellungnahme des Datenschutzes und gegebenenfalls Folgenabschätzung
7. Testkonzept, Testprotokolle und Abnahmeprotokoll
8. Migrationskonzept mit Abstimmungsnachweisen

TYPISCHE FESTSTELLUNGEN

- Der Projektauftrag ist nie formal freigegeben worden.
- Der Lenkungsausschuss tagt selten und trifft keine dokumentierten Entscheidungen.
- Sicherheit und Datenschutz werden erst kurz vor dem Start eingebunden.
- Umfangsänderungen werden ohne Bewertung umgesetzt.
- Die Abnahme erfolgt trotz offener schwerwiegender Fehler.
- Die Datenmigration ist nicht abgestimmt, Altdaten sind nach Abschaltung nicht mehr lesbar.

Bibliothek Muster-Prüfprogramme

29 Muster-Prüfprogramme online

proauditmap.com/pruefprogramme/

Vollständiges Prüfpaket in ProAuditMap

proauditmap.com

ProAuditMap

Muster ohne Gewähr und keine Rechtsberatung. Gesetze, Verordnungen und Standards erscheinen nur als Fundstelle, Normtexte sind nicht abgedruckt. Passen Sie Umfang und Tiefe vor der Verwendung an Ihre Organisation, Ihre Risiken und die aktuelle Fassung der für Sie geltenden Vorschriften an. Stand: 13. Oktober 2026