Muster-Prüfprogramm

Change Management

13 Prüfschritte · BSI, ISO 27001

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

BSI OPS.1.1.3 · ISO/IEC 27001:2022 Anhang A 8.32 · ISO/IEC 27001:2022 Anhang A 8.31 · ISO/IEC 27001:2022 Anhang A 8.9 · ISO/IEC 27001:2022 Anhang A 8.2

Prüfungsziel und Geltungsbereich

Die Prüfung beurteilt, ob Änderungen an produktiven IT-Systemen kontrolliert erfolgen: mit einem Antrag, einer Bewertung der Auswirkungen, einer Genehmigung vor der Umsetzung, einem Test, einem Rückfallplan und einer Dokumentation. Sie beurteilt außerdem, ob tatsächlich alle Änderungen durch das Verfahren laufen.

GELTUNGSBEREICH

- Änderungen an Anwendungen, Infrastruktur, Konfigurationen und Netzwerkkomponenten im produktiven Betrieb
- Standardänderungen, normale Änderungen und Notfalländerungen
- Rollen im Verfahren, etwa Antragsteller, Genehmiger und Umsetzer, sowie Entwicklungs-, Test- und Produktivumgebung
- Nicht Gegenstand: die Methodik der Softwareentwicklung selbst, sofern nicht gesondert vereinbart

Prüfschritte 1 bis 3

Schritt 01 BSI OPS.1.1.3; ISO/IEC 27001:2022 Anhang A 8.32

Ein Change-Prozess besteht, ist freigegeben und unterscheidet Standard-, normale und Notfalländerungen.

Prüfhandlung Prozessbeschreibung lesen und prüfen, ob Kategorien, Rollen und Abläufe je Kategorie festgelegt sind.

Nachweise Prozessbeschreibung mit Freigabe, Katalog der Standardänderungen

Schritt 02 BSI OPS.1.1.3

Jede Änderung wird mit Beschreibung, Begründung, betroffenen Systemen und Rückfallplan beantragt.

Prüfhandlung Zehn Änderungen der letzten sechs Monate auswählen und die Anträge auf Vollständigkeit prüfen.

Nachweise Änderungsanträge oder Tickets

Schritt 03 ISO/IEC 27001:2022 Anhang A 8.32

Auswirkungen und Risiken, auch für die Informationssicherheit, werden vor der Genehmigung bewertet.

Prüfhandlung In der Stichprobe prüfen, ob und wie Auswirkungen und Sicherheitsaspekte bewertet wurden.

Nachweise Bewertungsvermerke, Risikoeinstufung im Ticket

Prüfschritte 4 bis 6

Schritt 04

ISO/IEC 27001:2022 Anhang A 8.32

Änderungen werden vor der Umsetzung von einer befugten Stelle genehmigt.

Prüfhandlung Genehmigungszeitpunkt mit dem Zeitpunkt der Umsetzung vergleichen und Befugnisse der Genehmigenden prüfen.

Nachweise Genehmigungen mit Zeitstempel, Befugnisliste, Protokolle des Änderungsgremiums

Schritt 05

ISO/IEC 27001:2022 Anhang A 8.31

Antragsteller, Genehmiger und Umsetzer sind getrennt, Entwicklung, Test und Produktion sind voneinander getrennt.

Prüfhandlung Rollen in der Stichprobe vergleichen und Zugriffsrechte auf die Umgebungen prüfen.

Nachweise Rollenmatrix, Berechtigungsauszug der Umgebungen

Schritt 06

BSI OPS.1.1.3

Vor der Inbetriebnahme finden Tests und eine dokumentierte Abnahme statt.

Prüfhandlung Für die Stichprobe Testplan, Ergebnisse und Abnahme ansehen.

Nachweise Testprotokolle, Abnahmevermerke

Prüfschritte 7 bis 9

Schritt 07 — BSI OPS.1.1.3

Ein Rückfallplan besteht und wird bei kritischen Änderungen getestet oder zumindest geprüft.

Prüfhandlung Rückfallpläne der Stichprobe lesen und bei fehlgeschlagenen Änderungen prüfen, ob sie angewendet wurden.

Nachweise Rückfallpläne, Protokolle fehlgeschlagener Änderungen

Schritt 08 — BSI OPS.1.1.3

Notfalländerungen folgen festgelegten Kriterien und werden nachträglich innerhalb einer Frist genehmigt und dokumentiert.

Prüfhandlung Alle Notfalländerungen des letzten Halbjahres auswählen und Begründung, Nachgenehmigung und Dokumentation prüfen.

Nachweise Liste der Notfalländerungen, nachträgliche Genehmigungen

Schritt 09 — ISO/IEC 27001:2022 Anhang A 8.9

Nach einer Änderung werden Konfigurations- und Systemdokumentation aktualisiert.

Prüfhandlung In der Stichprobe prüfen, ob die Konfigurationsverwaltung die geänderten Daten enthält.

Nachweise Auszug der Konfigurationsverwaltung vor und nach der Änderung

Prüfschritte 10 bis 13

Schritt 10 — ISO/IEC 27001:2022 Anhang A 8.32

Alle tatsächlichen Änderungen laufen durch das Verfahren; nicht erfasste Änderungen werden erkannt.

Prüfhandlung Protokolle der Systeme, Bereitstellungen und Konfigurationsänderungen eines Zeitraums mit den Änderungsanträgen abgleichen.

Nachweise Systemprotokolle, Bereitstellungsprotokolle, Abgleichsliste

Schritt 11 — BSI OPS.1.1.3

Betroffene Stellen werden rechtzeitig informiert, Wartungsfenster sind abgestimmt.

Prüfhandlung Kommunikation zu den Änderungen der Stichprobe prüfen.

Nachweise Ankündigungen, Wartungskalender

Schritt 12 — ISO/IEC 27001:2022 Anhang A 8.2

Der Zugriff auf Änderungen an der Produktion ist auf befugte Personen beschränkt und wird protokolliert.

Prüfhandlung Berechtigte für Änderungen an der Produktion auslesen, mit den Rollen vergleichen und die Protokollierung prüfen.

Nachweise Berechtigungsauszug, Protokollkonfiguration

Schritt 13 — ISO/IEC 27001:2022 Anhang A 8.32

Abgeschlossene Änderungen werden nachbetrachtet, Kennzahlen zu Erfolgsquote und Notfalländerungen werden ausgewertet.

Prüfhandlung Nachbetrachtungen fehlgeschlagener Änderungen und die Kennzahlenberichte der letzten zwölf Monate ansehen.

Nachweise Nachbetrachtungen, Kennzahlenberichte, Maßnahmenliste

Unterlagenanforderung

Diese 8 Unterlagen vor Prüfungsbeginn anfordern

1. Prozessbeschreibung zum Change Management mit Katalog der Standardänderungen
2. Liste aller Änderungen der letzten sechs bis zwölf Monate mit Kategorie und Status
3. Änderungsanträge, Genehmigungen und Testprotokolle der Stichprobe
4. Liste der Notfalländerungen mit nachträglicher Genehmigung
5. Rollenmatrix und Berechtigungsauszug für die produktiven Umgebungen
6. Systemprotokolle und Bereitstellungsprotokolle für den Abgleich
7. Protokolle des Änderungsgremiums
8. Kennzahlenberichte zu Änderungen

TYPISCHE FESTSTELLUNGEN

Änderungen werden nach der Umsetzung beantragt, die Genehmigung liegt zeitlich hinter der Änderung.

Anträge enthalten keinen Rückfallplan, bei fehlgeschlagenen Änderungen fehlt der Nachweis der Wiederherstellung.

Administratoren ändern Systeme direkt, ohne Ticket; der Abgleich mit den Systemprotokollen zeigt Lücken.

Antragsteller und Genehmiger sind dieselbe Person.

Notfalländerungen machen einen hohen Anteil aus und werden nicht nachträglich genehmigt.

Die Konfigurationsverwaltung wird nach Änderungen nicht aktualisiert.

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