Muster-Prüfprogramm

Sichere Softwareentwicklung

12 Prüfschritte · ISO 27001, BSI, NIS2

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

ISO/IEC 27001:2022 Anhang A 8.25 · BSI CON.8 · ISO/IEC 27001:2022 Anhang A 8.26 · BSI APP.3.1 · ISO/IEC 27001:2022 Anhang A 8.27 · ISO/IEC 27001:2022 Anhang A 8.28 · ISO/IEC 27001:2022 Anhang A 8.28 und 8.29 · ISO/IEC 27001:2022 Anhang A 8.29 · NIS2-Richtlinie Art. 21 Abs. 2 lit. e · § 30 Abs. 2 Nr. 5 BSIG · ISO/IEC 27001:2022 Anhang A 8.31 · ISO/IEC 27001:2022 Anhang A 8.4 · ISO/IEC 27001:2022 Anhang A 8.32 · ISO/IEC 27001:2022 Anhang A 8.30

Prüfungsziel und Geltungsbereich

Die Prüfung beurteilt, ob die Organisation einen Entwicklungsprozess betreibt, der Sicherheit von Beginn an berücksichtigt: Anforderungen, Architekturprinzipien, sichere Codierung, Prüfung und Test vor der Freigabe, Schutz des Quellcodes und der Entwicklungsumgebungen sowie Steuerung ausgelagerter Entwicklung. Sie beurteilt außerdem, ob Schwachstellen in eigener Software behandelt werden.

GELTUNGSBEREICH

- Eigenentwicklungen und angepasste Software, einschließlich Webanwendungen, Schnittstellen und Skripten für den Betrieb
- Entwicklungs-, Test- und Bereitstellungsprozesse, Werkzeuge und Umgebungen
- Ausgelagerte Entwicklung durch Dienstleister
- Nicht Gegenstand: Standardsoftware ohne Anpassung und die Änderungssteuerung im Betrieb, die in einem eigenen Muster behandelt wird

Prüfschritte 1 bis 3

Schritt 01

ISO/IEC 27001:2022 Anhang A 8.25; BSI CON.8

Ein Rahmen für den Entwicklungsprozess mit Sicherheitsanforderungen an jede Phase ist festgelegt, freigegeben und wird angewendet.

Prüfhandlung Prozessbeschreibung lesen und an zwei Projekten prüfen, ob die Sicherheitsanforderungen je Phase umgesetzt wurden.

Nachweise Entwicklungsrichtlinie, Projektunterlagen der Stichprobe

Schritt 02

ISO/IEC 27001:2022 Anhang A 8.26; BSI APP.3.1

Sicherheitsanforderungen werden für jede Anwendung zu Beginn erhoben, abgestimmt und nachverfolgt, auch zu Schnittstellen und Daten.

Prüfhandlung Anforderungsdokumente von drei Anwendungen auf Sicherheitsanforderungen und deren Umsetzung durchsehen.

Nachweise Anforderungsdokumente, Rückverfolgung bis zum Test

Schritt 03

ISO/IEC 27001:2022 Anhang A 8.27

Architektur- und Konstruktionsprinzipien für sichere Systeme sind festgelegt und werden bei neuen Systemen angewendet und überprüft.

Prüfhandlung Architekturvorgaben lesen und für zwei neue Systeme die Anwendung nachvollziehen.

Nachweise Architekturvorgaben, Entwurfsdokumente, Entscheidungsvermerke

Prüfschritte 4 bis 6

Schritt 04 ISO/IEC 27001:2022 Anhang A 8.28

Für sichere Codierung bestehen verbindliche Vorgaben, die Entwickler kennen und anwenden; Schulungen sind nachgewiesen.

Prüfhandlung Codierrichtlinie, Schulungsnachweise und Beispiele aus der Code-Prüfung ansehen.

Nachweise Codierrichtlinie, Schulungsnachweise, Protokolle der Code-Prüfung

Schritt 05 ISO/IEC 27001:2022 Anhang A 8.28 und 8.29

Änderungen am Quellcode werden von einer zweiten Person geprüft, bevor sie in den Hauptzweig gelangen; Werkzeuge zur statischen Analyse sind im Einsatz.

Prüfhandlung Zehn Änderungen auswählen und prüfen, ob eine Prüfung durch eine zweite Person und ein Lauf der Analysewerkzeuge nachgewiesen sind.

Nachweise Auszug der Änderungsanfragen, Ergebnisse der Analysewerkzeuge

Schritt 06 ISO/IEC 27001:2022 Anhang A 8.29; NIS2-Richtlinie Art. 21 Abs. 2 lit. e

Sicherheitstests sind Teil der Entwicklung und Abnahme: Test auf Schwachstellen, Abhängigkeiten und Konfiguration vor der Freigabe.

Prüfhandlung Testpläne, Ergebnisse und Behandlung der Befunde für zwei Freigaben prüfen.

Nachweise Testpläne, Testberichte, Freigabeprotokolle

Prüfschritte 7 bis 9

Schritt 07 — NIS2-Richtlinie Art. 21 Abs. 2 lit. e; § 30 Abs. 2 Nr. 5 BSIG

Bekannte Schwachstellen in Bibliotheken und Komponenten werden erkannt, bewertet und behoben; eingesetzte Komponenten sind erfasst.

Prüfhandlung Verfahren zur Erfassung und Prüfung von Abhängigkeiten ansehen und die Behandlung von Befunden der letzten sechs Monate nachvollziehen.

Nachweise Komponentenliste, Berichte zur Prüfung von Abhängigkeiten, Maßnahmenliste

Schritt 08 — ISO/IEC 27001:2022 Anhang A 8.31

Entwicklung, Test und Produktion sind getrennt, Produktivdaten werden in Tests nicht oder nur geschützt verwendet.

Prüfhandlung Umgebungen und Zugriffsrechte prüfen und feststellen, ob Testumgebungen Produktivdaten enthalten.

Nachweise Umgebungsübersicht, Berechtigungsauszug, Verfahren zu Testdaten

Schritt 09 — ISO/IEC 27001:2022 Anhang A 8.4

Der Zugriff auf Quellcode und Entwicklungswerkzeuge ist auf Befugte beschränkt und wird protokolliert; Zugangsdaten und Schlüssel liegen nicht im Quellcode.

Prüfhandlung Berechtigungen auf Repositories und Build-Systeme auslesen und Quellcode auf hinterlegte Zugangsdaten durchsuchen.

Nachweise Berechtigungsauszug, Ergebnis der Suche nach Geheimnissen, Protokolle

Prüfschritte 10 bis 12

Schritt 10 ISO/IEC 27001:2022 Anhang A 8.32; BSI CON.8

Die Bereitstellung in die Produktion erfolgt über einen kontrollierten Ablauf mit Freigabe, nicht über direkte Eingriffe einzelner Personen.

Prüfhandlung Bereitstellungsprotokolle der letzten drei Monate mit Freigaben abgleichen.

Nachweise Bereitstellungsprotokolle, Freigaben, Rechte auf Produktivsysteme

Schritt 11 ISO/IEC 27001:2022 Anhang A 8.30

Bei ausgelagerter Entwicklung sind Sicherheitsanforderungen vertraglich festgelegt, ihre Einhaltung wird überwacht und das Ergebnis geprüft.

Prüfhandlung Verträge und Abnahmen von zwei ausgelagerten Entwicklungen prüfen, insbesondere Prüfrechte und Rechte am Quellcode.

Nachweise Verträge, Abnahmeprotokolle, Prüfberichte

Schritt 12 NIS2-Richtlinie Art. 21 Abs. 2 lit. e

Schwachstellen in eigener Software werden gemeldet, bewertet und behoben; es gibt einen Weg für Meldungen von außen.

Prüfhandlung Verfahren zur Behandlung gemeldeter Schwachstellen und die Bearbeitung der letzten Meldungen prüfen.

Nachweise Verfahren, Meldekanal, Schwachstellenregister

Unterlagenanforderung

Diese 8 Unterlagen vor Prüfungsbeginn anfordern

1. Richtlinie zur sicheren Entwicklung und zum Entwicklungsprozess
2. Codierrichtlinie und Schulungsnachweise
3. Anforderungsdokumente der Stichprobe mit Sicherheitsanforderungen
4. Architekturvorgaben und Entwurfsdokumente
5. Auszug der Änderungsanfragen mit Prüfvermerken
6. Testpläne, Testberichte und Freigabeprotokolle
7. Berechtigungsauszug für Repositories und Build-Systeme
8. Verträge und Abnahmen ausgelagerter Entwicklung

TYPISCHE FESTSTELLUNGEN

- Sicherheitsanforderungen werden erst kurz vor der Freigabe betrachtet, nicht zu Beginn.
- Änderungen gelangen ohne Prüfung durch eine zweite Person in den Hauptzweig.
- Zugangsdaten und Schlüssel sind im Quellcode hinterlegt.
- Bekannte Schwachstellen in Bibliotheken werden nicht systematisch erkannt, eingesetzte Komponenten sind nicht erfasst.
- Testumgebungen enthalten unverändert Produktivdaten.
- Verträge mit Entwicklungsdienstleistern regeln weder Prüfrechte noch Rechte am Quellcode.

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