

Umsetzungshinweise für ISMS-Projekte nach ISO 27001

ISO/IEC 27001

Die ISO 27001 ist eine internationale Norm, die Anforderungen an das Management von Informationssicherheit festlegt. Sie beschreibt, wie Unternehmen und Organisationen ihre Informationen systematisch schützen können, um Risiken wie Datenverlust, Cyberangriffe oder unbefugten Zugriff zu minimieren.

Motivation

Aufgrund des steigenden Wettbewerbsdrucks wird es branchenübergreifend immer wichtiger neue und langjährige Mitarbeiter*innen effizient in neue Themen einzuarbeiten. Damit Expert*innen Mitarbeiter*innen nichtmehr einzeln einarbeiten müssen, ist es wichtig Ihr Wissen sorgfältig zu dokumentieren und allen Mitarbeiter*innen zur Verfügung zu stellen. Durch umfangreiche Umsetzungshinweise können Mitarbeiter*innen effizienter in neue Themen eingearbeitet werden und dies ermöglicht damit eine schnellere Umsetzung von Kundenprojekten. Deshalb ist essenziell das Wissensmanagement kontinuierlich zu verbessern und erweitern.

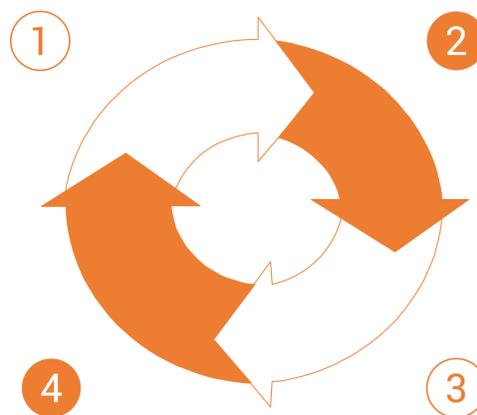
Erfahrungen in Kundenprojekten sammeln

- Aktive Mitarbeit in Projekten
- Welche Methoden und Lösungen funktionieren
- Austausch mit Kolleginnen und Kundinnen
- Identifikation neuer Anforderungen oder Probleme

Wissen verteilen

- Bereitstellung in der Knowledge-Base
- Interne Präsentationen, Workshops oder Meetings
- Austausch in Fachgruppen
- Einholen von Feedback zur kontinuierlichen Verbesserung

Durchführung



Herausforderungen und Lösungen dokumentieren

- Erfassung erlebter Probleme und deren Auswirkungen
- Dokumentation erfolgreicher Lösungsansätze
- Sammlung der Best Practices und Lessons Learned

Wissen aufbereiten

- Strukturierung der Informationen
- Zusammenfassung der wichtigsten Erkenntnisse
- Anonymisierung sensibler Kundendaten
- Vorlagen, Leitfäden, Checklisten oder Best Practices

Beispielhafte Ergebnisse

ISO/IEC 27002:2022

5.7 Informationen über die Bedrohungslage

Maßnahme / Control

Maßnahme: Informationen über Bedrohungen der Informationssicherheit sollten erhoben und analysiert werden, um Informationen über die Bedrohungslage zu gewinnen.	Control: Information relating to information security threats should be collected and analysed to produce threat intelligence.
--	--

Zweck / Purpose

Anleitung / Guidance

Weitere Informationen / Other information

Best Practices

ISF Paper
Das ISF hat 2022 das Paper "Threat Intelligence - React and prepare" überarbeitet und neu herausgebracht. Dieses beschäftigt sich mit den Zielen der Threat Intelligence und der Herangehensweise, um Informationen über die aktuelle Bedrohungslage zu erhalten.

Weekly Best Practice
Am 28.08.2024 wurde das Thema im wöchentlichen Weekly Best Practice diskutiert, die Aufzeichnung ist [hier](#) zu finden.

ISO/IEC 27002:2022

7.7 Aufgeräumte Arbeitsumgebung und Bildschirmsperren

Maßnahme / Control

Maßnahme: Es sollten klare Regeln für eine aufgeräumte Arbeitsumgebung hinsichtlich Unterlagen und Wechselspeichermedien und klare Regeln für Bildschirmsperren für informationsverarbeitende Einrichtungen festgelegt und angemessen durchgesetzt werden.	Control: Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities should be defined and appropriately enforced.
--	---

Zweck / Purpose

Anleitung / Guidance

Weitere Informationen / Other information

Best Practices

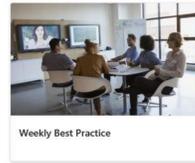
Regelmäßige Überprüfung

Englische Formulierung

Herzlich Willkommen in der Knowledge Base!



Security Consulting



Weitere usd-Wikis

