S E M I N A R E

Quality Management (QM) and Information Security (IS)

2282

Praktische Implementierung von ISO/IEC 27001:2022 in der Softwareindustrie

o Zielgruppe
Software- oder IT-Dienstleistungsorganisation verstehen möchten – sowohl technische als auch nicht-technische Rollen.

Geeignet für: Mitarbeiter in Softwareunternehmen, Projekt-, Produkt- und Teamleiter, Software-Engineering-, QA-, DevOps-, IT-Operations- und Service-Delivery-Mitglieder, Qualitäts-, Compliance-, Informationssicherheits- und Risikomanagement-Rollen, interne Auditoren, Prozessverantwortliche, Manager und Berater.

o Voraussetzungen
Grundkenntnisse in Softwareentwicklung, IT-Projektmanagement oder Informationssicherheit sind nützlich, aber nicht erforderlich. Keine vorherige ISO-27001-Erfahrung notwendig.

o Seminarziel
Ziel des Seminars ist es, den Teilnehmern zu helfen, ISO/IEC 27001:2022 als praktisches Managementsystem für Informationssicherheit zu verstehen. Die Teilnehmer lernen, wie die Schlüsselelemente eines ISMS zusammenwirken und wie sie Implementierung, Pflege und Verbesserung der Informationssicherheit in einer Softwareorganisation unterstützen können.

o Seminarinhalt
Tag 1 – ISO-27001-Grundlagen, ISMS-Geltungsbereich und Risikomanagement

1. Einführung in ISO/IEC 27001:2022
- o Was ISO 27001 in IT- und Softwareorganisationen löst
- o Struktur der Norm: Hauptabschnitte und Anhang A
- o ISMS als Betriebsmodell, nicht nur als Dokumentensammlung
- o Häufige Geschäftstreiber: Kundenanforderungen, Ausschreibungen, Compliance und Produktsicherheit

2. Kontext, Geltungsbereich und Verantwortlichkeiten
- o Interessierte Parteien, Unternehmenskontext und Sicherheitserwartungen
- o Definition von ISMS-Grenzen in einem Softwarehaus, Produktunternehmen oder Outsourcing-Organisation
- o Managementverpflichtung, Sicherheitsbeauftragter, Risiko- und Asset-Eigentümer
- o Übung: Entwurf eines ISMS-Geltungsbereichs für eine Beispiel-Softwareorganisation

3. Risikobewertung und -behandlung
- o Risikobasierter Ansatz in ISO 27001:2022
- o Informationswerte: Quellcode, Repositories, Kundendaten, Testumgebungen
- o Typische Bedrohungen und Schwachstellen in der Softwareentwicklung
- o Übung: Risikoanalyse für einen Beispiel-Entwicklungsprozess

4. ISMS-Dokumentation und Statement of Applicability
- o Erforderliche Dokumente vs. nützliche Betriebsaufzeichnungen
- o Informationssicherheitspolitik, Risikoregister und Risikobehandlungsplan
- o Zweck, Struktur und Verbindung des SoA mit der Risikobewertung
- o Wie Auditoren Dokumentation, Kontrollen und Nachweise prüfen

Tag 2 – Anhang A, sichere Softwareentwicklung, Audit und ISMS-Pflege

5. Anhang A in der IT-Praxis
- o Vier Kontrollgruppen: organisatorisch, personell, physisch und technologisch

München
Berghamer Straße 10
85435 Erding
Tel.: 0 81 22 / 97 40 - 0
Fax: 0 81 22 / 97 40 - 10

Erfurt
Michaelisstraße 13a
99084 Erfurt
Tel.: 03 61 / 5 65 93 - 0
Fax: 03 61 / 5 65 93 - 10

Internet
www.md-consulting.de

E-Mail
info@md-consulting.de

Bankverbindung
HypoVereinsbank
Erfurt

IBAN:
DE84 8202 0086
0003 9840 95

SWIFT/BIC:
HYVEDEMM 498

Geschäftsführer
Dr. Martin Diestelmann

HRB München 289362

USt.Id Nr.:
DE 150 108 446

Quality Management (QM) and Information Security (IS)

2282

- Zugangsverwaltung, Informationsklassifizierung und Vorfallmanagement
- Remote- und Hybridarbeit, Endpunktschutz, Backup, Protokollierung und Überwachung
- Schwachstellenmanagement

6. ISO 27001 im SDLC

- Sichere Softwareentwicklung als Teil des ISMS
- Sicherheitsanforderungen in IT-Projekten und Produktentwicklung

7. Lieferanten, Kunden und Implementierungs-Roadmap

- Bewertung von Cloud-Anbietern, SaaS-Tools und Unterauftragnehmern
- Verträge, NDAs, DPAs, SLAs und Sicherheitsanforderungen
- Gap-Analyse und Implementierungs-Roadmap

8. Audit, Zertifizierung und kontinuierliche Verbesserung

- Internes Audit: Planung, Fragen, Nachweise, Nichtkonformitäten und Korrekturmaßnahmen
- Managementbewertung, KPIs/KRIs und Sicherheitsberichte
- Überblick über Stufe-1- und Stufe-2-Zertifizierungsaudit
- Abschluss-Workshop: Beispielgeltungsbereich, Risikobewertung, Anhang-A-Kontrollenauswahl

- **Seminardauer:** 2 Tage

Im Preis enthalten sind kursbegleitende Seminarunterlagen.
Das Seminar wird in englischer Sprache durchgeführt.

- **Preis pro Person: 1.500 EUR netto**