ISMS 27001 Professional — Syllabus

State: released - ID: 112 - Topic: ISMS 27001 - Version: 1 - language: deutsch - valid from 2017-10-01
Anzahl der Prüfungsfragen: 50
Schulungszeit in Minuten: 2400

Die verpflichtende Zeitvorgabe für die dazugehörige Schulung ist 5 Tage à min. 8 Stunden mit je 60 Minuten (= 2400 Minuten).

Für den Erhalt des ISMS 27001 Foundation Prüfungszertifikates muss die im Multiple-Choice-Verfahren gehaltene Prüfung erfolgreich bestanden werden.

- Version: DIN ISO/IEC 27000:2015
- Version: DIN ISO/IEC 27001:2015
- Sprache: Deutsch/Englisch
- Prüfungsdauer: 75 Minuten
- Format: 50 Multiple Choice-Fragen; zwei bis sechs Antwortmöglichkeiten von denen eine, mehrere oder auch alle Antworten korrekt sein können.
- min. Punkte: 33 von 50

Jede komplett richtig beantwortete Frage gibt einen Punkt. Bei falsch beantworteten Fragen gibt es 0 Punkte (aber keinen Punktabzug). Als falsch beantwortet gilt eine Frage wenn eine falsche Antwort markiert ist, oder nicht alle richtigen angekreuzt wurden.

Die hier beschriebenen Werte sind eine Kopie der Prüfungsordnung. Sollten sich Prüfungsordnung und dieser Lehrplan widersprechen, gelten die in der Prüfungsordnung angegebenen Prüfungsformate und Definitionen.

Der vorliegende Lehrplan ist keine Agenda. Die Schulungsorganisation ist frei in der Reihenfolge der Inhaltsvermittlung. Die vorgegebenen Zeiten zu den Kapitel sollten eingehalten werden. Die in Kapitel 1 aufgeführten Begriffe sind sinnvollerweise in den entsprechenden nachfolgenden Kapiteln an passender Stelle zu erklären.

Die oben genannten Dokumente sind in ihrer Gänze prüfungsrelevant.

1. Begriffe
(en: Terms)

Severity: 8.00% — Minutes: 192 — Min/avg/max number of questions: 3.0/4.0/5.0

Dokument: ISO/IEC DIS 27000:2015

Alle Definitionen sind zu erklären:

- 2.1 Zugangssteuerung (en: access control)
- 2.2 analytisches Modell (en: analytical model)
- 2.3 Angriff (en: attack)
- 2.4 Attribut (en:attribute)
- 2.5 Audit (en: audit)
- 2.6 Auditumfang (en: audit scope)
- 2.7 Authentisierung (en: authentication)
- 2.8 Authentizität (en: authenticity)
- 2.9 Verfügbarkeit (en: availability)
- 2.10 Elementarmaß (en: base measure)
- 2.11 Kompetenz (en: competence)
- 2.12 Vertraulichkeit (en: confidentiality)
- 2.13 Konformität (en: conformity)
- 2.14 Folge (en: consequence)
- 2.15 fortlaufende Verbesserung (en: continual improvement)
- 2.16 Maßnahme (en: control)
- 2.17 Maßnahmenziel (en: control objective)
- 2.18 Korrektur (en: correction)
- 2.19 Korrekturmaßnahme (en: corrective action)
- 2.20 Daten (en: data)
- 2.21 Entscheidungskriterien (en: decision criteria)
- 2.22 abgeleitetes Maß (en: derived measure)
- 2.23 dokumentierte Information (en: documented information)
- 2.24 Wirksamkeit (en: effectiveness)
- 2.25 Ereignis (en: event)
- 2.26 Geschäftsleitung (en: executive management)
- 2.27 externer Kontext (en: external context)
- 2.28 Steuerung der Informationssicherheit
- 2.29 Steuerungssgremium (en: governing body)

- 2.30 Indikator (en: indicator)
- 2.31 Informationsbedarf (en: information need)
- 2.32 informationsverarbeitende Einrichtungen (en: information processing facilities)
- 2.33 Informationssicherheit (en: information security)
- 2.34 Aufrechterhaltung der Informationssicherheit (en: information security continuity)
- 2.35 Informationssicherheitsereignis (en: information security event)
- 2.36 Informationssicherheitsvorfall (en: information security incident)
- 2.37 Handhabung von Informationssicherheitsvorfällen (en: information security incident management)
- 2.38 informationsaustauschende Gemeinschaft (en: information sharing community)
- 2.39 Informationssystem (en: information system)
- 2.40 Integrität (en: integrity)
- 2.41 Interessierte Partei (en: interested party)
- 2.42 interner Kontext (en: internal context)
- 2.43 ISMS-Projekt (en: ISMS project) 2.44 Risikoniveau (en: level of risk)
- 2.44 Risikoniveau (en: level of risk)
- 2.45 Wahrscheinlichkeit (en: likelihood)
- 2.46 Managementsystem (en: management system)
- 2.47 Maß (en: measure)
- 2.48 Messung (en: measurement)
- 2.49 Messfunktion (en: measurement function)
- 2.50 Messmethode (en: measurement method)
- 2.51 Messergebnisse (en: measurement results)
- 2.52 Überwachung (en: monitoring)
- 2.53 Nichtkonformität (en: nonconformity)
- 2.54 Nichtabstreitbarkeit (en: non-repudiation)
- 2.55 Objekt (en: object)
- 2.56 Ziel (en: objective)
- 2.57 Organisation (en: organization)
- 2.58 ausgliedern (Verb) (en: outsource, verb)
- 2.59 Leistung (en: performance)
- 2.60 Politik (en: policy)
- 2.61 Prozess (en: process)
- 2.62 Verlässlichkeit (en: reliability)
- 2.63 Anforderung (en: requirement)
- 2.64 Restrisiko (en: residual risk)
- 2.65 Überprüfung (en: review)
- 2.66 Überprüfungsobjekt (en: review object)
- 2.67 Ziel der Überprüfung (en: review objective)
- 2.68 Risiko (en: risk)
- 2.69 Risikoakzeptanz (en: risk acceptance)
- 2.70 Risikoanalyse (en: risk analysis)
- 2.71 Risikobeurteilung (en: risk assessment)
- 2.72 Risikokommunikation und –absprachen (en: risk communication and consultation)

- 2.73 Risikokriterien (en: risk criteria)
- 2.74 Risikobewertung (en: risk evaluation)
- 2.75 Risikoidentifizierung (en: risk identifikation
- 2.76 Risikomanagement (en: risk management)
- 2.77 Risikomanagementprozess (en: risk management process)
- 2.78 Risikoeigentümer (en: risk owner)
- 2.79 Risikobehandlung (en: risk treatment)
- 2.80 Skala (en: scale)
- 2.81 Standard zur Einführung von Sicherheit (en: security implementation standard)
- 2.82 Stakeholder (en: stakeholder)
- 2.83 Bedrohung (en: threat)
- 2.84 oberste Leitung (en: top management)
- 2.85 vertrauenswürdige Einheit zur Informationsverbreitung (en: trusted information communication entity)
- 2.86 Maßeinheit (en: unit of measurement)
- 2.87 Validierung (en: validation)
- 2.88 Verifizierung (en: verification)
- 2.89 Schwachstelle (en: vulnerability)

2. Managementsysteme für Informationssicherheit (ISMS)
(en: Information security management systems)

Severity: 4.00% — Minutes: 96 — Min/avg/max number of questions: 1.5/2.0/2.5

Dokument: DIN ISO/IEC 27000:2015

Die Inhalte folgender Kapitel sind zu erklären:

- 3.1 Einleitung (en: general)
- 3.2 Was ist ein ISMS? (en: what is an ISMS?)
    - 3.2.1 Übersicht und Grundsätze Informationssicherheitsanforderungen (en: overview and principles)
    - 3.2.2 Informationen (en: information)
    - 3.2.3 Informationssicherheit (en: information security)
    - 3.2.4 Management (en: management)
    - 3.2.5 Managementsystem (en: management system)
- 3.3 Prozessorientierter Ansatz (en: process approach)
- 3.4 Warum ist ein ISMS wichtig? (en: why an ISMS is important)
- 3.5 Einführung, Überwachung, Pflege und Verbesserung eines ISMS (en: establishing, monitoring, maintaining and improving an ISMS)
    - 3.5.1 Übersicht (en: overview)
    - 3.5.2 Identifizierung von Informationssicherheitsanforderungen (en: identifying information security requirements)
    - 3.5.3 Beurteilung von Informationssicherheitsrisiken (en: assessing information security risks)
    - 3.5.4 Behandlung von Informationssicherheitsrisiken (en: treating information security risks)
    - 3.5.5 Auswahl und Umsetzung von Maßnahmen (en: selecting and implementing controls)
    - 3.5.6 Überwachung, Aufrechterhaltung und Verbesserung der Wirksamkeit des ISMS (en: monitor, maintain and improve the effectiveness of the ISMS)
    - 3.5.7 Fortlaufende Verbesserung (en: continual improvement)
- 3.6 Kritische Faktoren für das ISMS (en: ISMS critical success factors)
- 3.7 Nutzen der ISMS-Normenfamilie (en: benefits of the ISMS family of standards)

3. Die ISMS-Normenfamilie (en: The family of ISMS standards)

Severity: 4.00% — Minutes: 96 — Min/avg/max number of questions: 1.5/2.0/2.5

Dokument: DIN ISO/IEC 27000:2015

Die Inhalte folgender Kapitel sind zu erklären:

- 4.1 Allgemeine Informationen (en: general information)
- 4.2 Normen, die einen Überblick geben und die Terminologie festlegen (en: standards describing an overview and terminology)
  - 4.2.1 ISO/IEC 27000 (dieses Dokument) (en: ISO/IEC 27000 (this International Standard))
- 4.3 Normen, die Anforderungen festlegen (en: standards specifying requirements)
  - 4.3.1 ISO/IEC 27001
  - 4.3.2 ISO/IEC 27006
- 4.4 Normen, die allgemeine Leitfäden beschreiben (en: standards describing general guidelines)
  - 4.4.1 ISO/IEC 27002
  - 4.4.2 ISO/IEC 27003
  - 4.4.3 ISO/IEC 27004
  - 4.4.4 ISO/IEC 27005
  - 4.4.5 ISO/IEC 27007
  - 4.4.6 ISO/IEC TR 27008
  - 4.4.7 ISO/IEC 27013
  - 4.4.8 ISO/IEC 27014
  - 4.4.9 ISO/IEC TR 27016
- 4.5 Normen, die branchenspezifische Leitfäden beschreiben (en: Standards describing sector-specific guidelines)
  - 4.5.1 ISO/IEC 27010
  - 4.5.2 ISO/IEC 27011
  - 4.5.3 ISO/IEC TR 27015
  - 4.5.4 ISO/IEC 27017
  - 4.5.5 ISO/IEC 27018
  - 4.5.6 ISO/IEC TR 27019
  - 4.5.7 ISO 27799

4. Kontext der Organisation (en: Context of the organization)

Severity: 6.00% — Minutes: 144 — Min/avg/max number of questions: 2.5/3.0/3.5

Dokument: DIN ISO/IEC 27001:2015

Die Inhalte folgender Kapitel sind zu erklären:

- 4.1 Verstehen der Organisation und ihres Kontextes (en: understanding the organization and its context)
- 4.2 Verstehen der Erfordernisse und Erwartungen interessierter Parteien (en: understanding the needs and expectations of interested parties)
- 4.3 Festlegen des Anwendungsbereichs des Informationssicherheitsmanagementsystems (en: determining the scope of the information security management system)
- 4.4 Informationssicherheitsmanagementsystem (en: information security management system)

mindestens 1 praktisch Übungen gefordert

für die Übungen müssen mindestens 60% der Zeit, die für diesen Abschnitt vorgesehen ist verwendet werden.

Beispiele: Gruppenarbeit mit Präsentation

• Erstellen einer Stakeholder-Analyse
  ◦ https://de.wikipedia.org/wiki/Stakeholder
  ◦ https://de.wikipedia.org/wiki/Projektumfeldanalyse
• Schriftliche Festlegung des Anwendungsbereichs

5. Führung
(en: leadership)

Severity: 6.00% — Minutes: 144 — Min/avg/max number of questions: 2.5/3.0/3.5

Dokument: DIN ISO/IEC 27001:2015

Die Inhalte folgender Kapitel sind zu erklären:

- 5.1 Führung und Verpflichtung (en: Leadership and commitment)
- 5.2 Politik (en: policy)
- 5.3 Rollen, Verantwortlichkeiten und Befugnisse in der Organisation (en: Organizational roles, responsibilities and authorities)

6. Planung
(en: planning)

Severity: 10.00% — Minutes: 240 — Min/avg/max number of questions: 4.0/5.0/6.0

Dokument: ISO/IEC 27001

Die Inhalte folgender Kapitel sind zu erklären:

- 6.1 Maßnahmen zum Umgang mit Risiken und Chancen (en: Actions to address risks and opportunities)
  - 6.1.1 Allgemeines (en: general)
  - 6.1.2 Informationssicherheitsrisikobeurteilung (en: Information security risk assessment)
  - 6.1.3 Informationssicherheitsrisikobehandlung (en: Information security risk treatment)
- 6.2 Informationssicherheitsziele und Planung zu deren Erreichung (en: Information security objectives and planning to achieve them)

mindestens 1 praktisch Übungen gefordert

für die Übungen müssen mindestens 40% der Zeit, die für diesen Abschnitt vorgesehen ist verwendet werden.

Beispiele: Gruppenarbeit mit Präsentation

• Erstellen eines Klassifizierungssystems für Risiken
in Bezug auf Auswirkung (Schaden) und Eintrittswahrscheinlichkeit
https://de.wikipedia.org/wiki/Klassifizierung
• Festlegen von konkreten Sicherheitszielen für ein fiktives Unternehmen

7. Unterstützung & Betrieb (en: support & operation)

Severity: 10.00% — Minutes: 240 — Min/avg/max number of questions: 4.0/5.0/6.0

Dokument: ISO/IEC 27001

Die Inhalte folgender Kapitel sind zu erklären:

- 7.1 Ressourcen (en: resources)
- 7.2 Kompetenz (en: competence)
- 7.3 Bewusstsein (en: awareness)
- 7.4 Kommunikation (en: communication)
- 7.5 Dokumentierte Information (en: documented information)
  - 7.5.1 Allgemeines (en: general)
  - 7.5.2 Erstellen und Aktualisieren (en: Creating and updating)
  - 7.5.3 Lenkung dokumentierter Information (en: Control of documented information)
- 8.1 Betriebliche Planung und Steuerung (en: Operational planning and control)
- 8.2 Informationssicherheitsrisikobeurteilung (en: Information security risk assessment)
- 8.3 Informationssicherheitsrisikobehandlung (en: Information security risk treatment)

8. Bewertung der Leistung & Verbesserung (en: performance evaluation & improvement)

Severity: 10.00% — Minutes: 240 — Min/avg/max number of questions: 4.0/5.0/6.0

Dokument: ISO/IEC 27001

Die Inhalte folgender Kapitel sind zu erklären:

- 9.1 Überwachung, Messung, Analyse und Bewertung (en: Monitoring, measurement, analysis and evaluation)
- 9.2 Internes Audit (en: internal audit)
- 9.3 Managementbewertung (en: management review)
- 10.1 Nichtkonformität und Korrekturmaßnahmen (en: Nonconformity and corrective action)
- 10.2 Fortlaufende Verbesserung (en: continual improvement)

9. Anhang A
(en: Appendix A)

Severity: 38.00% — Minutes: 912 — Min/avg/max number of questions: 15.0/19.0/23.0

Dokument: DIN ISO/IEC 27000:2015

A.5 Informationssicherheitsrichtlinien (en: Information security policies)

Der Inhalt von A.5 Informationssicherheitsrichtlinien (en: Information security policies) ist zu erklären:

A.5.1 Vorgaben der Leitung für Informationssicherheit (en: Management direction for information security)

- A.5.1.1 Informationssicherheitsrichtlinien (en: Policies for information security)
- A.5.1.2 Überprüfung der Informationssicherheitsrichtlinien (en: Review of the policies for information security)

A.6 Organisation der Informationssicherheit (en: Organization of information security)

Der Inhalt von A.6 Organisation der Informationssicherheit (en: Organization of information security) ist zu erklären:

- A.6.1 Interne Organisation (en: Internal organization)
  - A.6.1.1 Informationssicherheitsrollen und -verantwortlichkeiten (en: Information security roles and responsibilities)
  - A.6.1.2 Aufgabentrennung (en: Segregation of duties)
  - A.6.1.3 Kontakt mit Behörden (en: Contact with authorities)
  - A.6.1.4 Kontakt mit speziellen Interessensgruppen (en: Contact with special interest groups)
  - A.6.1.5 Informationssicherheit im Projektmanagement (en: Information security in project management)
- A.6.2 Mobilgeräte und Telearbeit (en: Mobile devices and teleworking)
  - A.6.2.1 Richtlinie zu Mobilgeräten (en: Mobile device policy)
  - A.6.2.2 Telearbeit (en: teleworking)

A.7 Personalsicherheit (en: Human resource security)

Der Inhalt von A.7 Personalsicherheit (en: Human resource security) ist zu erklären:

- A.7.1 Vor der Beschäftigung (en: Prior to employment)
  - A.7.1.1 Sicherheitsüberprüfung (en: Screening)
  - A.7.1.2 Beschäftigungs- und Vertragsbedingungen (en: Terms and conditions of employment)
- A.7.2 Während der Beschäftigung (en: During employment)
  - A.7.2.1 Verantwortlichkeiten der Leitung (en: Management responsibilities)
  - A.7.2.2 Informationssicherheitsbewusstsein, - ausbildung und -schulung (en: Information security awareness, education and training)
  - A.7.2.3 Maßregelungsprozess (en: Disciplinary process)
- A.7.3 Beendigung und Änderung der Beschäftigung (en: Termination and change of employment)
  - A.7.3.1 Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung (en: Termination or change of employment responsibilities)

A.8 Verwaltung der Werte (en: Asset management)

Der Inhalt von A.8 Verwaltung der Werte (en: Asset management) ist zu erklären:

- A.8.1 Verantwortlichkeit für Werte (en: Responsibility for assets)
  - A.8.1.1 Inventarisierung der Werte (en: Inventory of assets)
  - A.8.1.2 Zuständigkeit für Werte (en: Ownership of assets)
  - A.8.1.3 Zulässiger Gebrauch von Werten (en: Acceptable use of assets)
  - A.8.1.4 Rückgabe von Werten (en: Return of assets)
- A.8.2 Informationsklassifizierung (en: Information classification)
  - A.8.2.1 Klassifizierung von Information (en: Classification of information)
  - A.8.2.2 Kennzeichnung von Information (en: Labelling of information)
  - A.8.2.3 Handhabung von Werten (en: Handling of assets)
- A.8.3 Handhabung von Datenträgern (en: Media handling
  - A.8.3.1 Handhabung von Wechseldatenträgern (en: Management of removable media)
  - A.8.3.2 Entsorgung von Datenträgern (en: Disposal of media)
  - A.8.3.3 Transport von Datenträgern (en: Physical media transfer)

A.9 Zugangssteuerung (en: Access control)

Der Inhalt von A.9 Zugangssteuerung (en: Access control) ist zu erklären:

- A.9.1 Geschäftsanforderungen an die Zugangssteuerung (en: Business requirements of access control)
  - A.9.1.1 Zugangssteuerungsrichtlinie (en: Access control policy)
  - A.9.1.2 Zugang zu Netzwerken und Netzwerkdiensten (en: Access to networks and

network services)
- A.9.2 Benutzerzugangssverwaltung (en: User access management)
  - A.9.2.1 Registrierung und Deregistrierung von Benutzern (en: User registration and deregistration)
  - A.9.2.2 Zuteilung von Benutzerzugängen (en: User access provisioning)
  - A.9.2.3 Verwaltung privilegierter Zugangsrechte (en: Management of privileged access rights)
  - A.9.2.4 Verwaltung geheimer Authentisierungsinformation von Benutzern (en: Management of secret authentication information of users)
  - A.9.2.5 Überprüfung von Benutzerzugangsrechten (en: Review of user access Rights)
  - A.9.2.6 Entzug oder Anpassung von Zugangsrechten (en: Removal or adjustment of access rights)
- A.9.3 Benutzerverantwortlichkeiten (en: User responsibilities)
  - A.9.3.1 Gebrauch geheimer Authentisierungsinformation (en: Use of secret authentication information)
- A.9.4 Zugangssteuerung für Systeme und Anwendungen (en: System and application access control)
  - A.9.4.1 Informationszugangssbeschränkung (en: Information access restriction)
  - A.9.4.2 Sichere Anmeldeverfahren (en: Secure log-on procedures)
  - A.9.4.3 System zur Verwaltung von Kennwörtern (en: Password management system)
  - A.9.4.4 Gebrauch von Hilfsprogrammen mit privilegierten Rechten (en: Use of privileged utility programs)
  - A.9.4.5 Zugangssteuerung für Quellcode von Programmen (en: Access control to program source code)

A.10 Kryptographie (en: Cryptography)

Der Inhalt von A.10 Kryptographie (en: Cryptography) ist zu erklären:

- A.10.1 Kryptographische Maßnahmen (en: Cryptographic controls)
  - A.10.1.1 Richtlinie zum Gebrauch von kryptographischen Maßnahmen (en: Policy on the use of cryptographic controls)
  - A.10.1.2 Schlüsselverwaltung (en: Key management

A.11 Physische und umgebungsbezogene Sicherheit (en: Physical and environmental security)

Der Inhalt von A.11 Physische und umgebungsbezogene Sicherheit (en: Physical and environmental security) ist zu erklären:

- A.11.1 Sicherheitsbereiche (en: Secure areas)
  - A.11.1.1 Physischer Sicherheitsperimeter (en: Physical security perimeter) A.11.1.2 Physische Zutrittssteuerung (en: Physical entry controls)
  - A.11.1.3 Sichern von Büros, Räumen und Einrichtungen (en: Securing offices, rooms and facilities)

- A.11.1.4 Schutz vor externen und umweltbedingten Bedrohungen (en: Protecting against external and environmental threats)
- A.11.1.5 Arbeiten in Sicherheitsbereichen (en: Working in secure areas) A.11.1.6 Anlieferungs- und Ladebereiche (en: Delivery and loading areas)

- A.11.2 Geräte und Betriebsmittel (en: Equipment)
  - A.11.2.1 Platzierung und Schutz von Geräten und Betriebsmitteln (en: Equipment siting and protection)
  - A.11.2.2 Versorgungseinrichtungen (en: Supporting utilities)
  - A.11.2.3 Sicherheit der Verkabelung (en: Cabling security)
  - A.11.2.4 Instandhalten von Geräten und Betriebsmitteln (en: Equipment maintenance)
  - A.11.2.5 Entfernen von Werten (en: Removal of assets)
  - A.11.2.6 Sicherheit von Geräten, Betriebsmitteln und Werten außerhalb der Räumlichkeiten (en: Security of equipment and assets off-premises)
  - A.11.2.7 Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln (en: Secure disposal or reuse of equipment)
  - A.11.2.8 Unbeaufsichtigte Benutzergeräte (en: Unattended user equipment)
  - A.11.2.9 Richtlinie für eine aufgeräumte Arbeitsumgebung und Bildschirmsperren (en: Clear desk and clear screen policy)

A.12 Betriebssicherheit (en: Operations security)

Der Inhalt von A.12 Betriebssicherheit (en: Operations security) ist zu erklären:

- A.12.1 Betriebsabläufe und -verantwortlichkeiten (en: Operational procedures and responsibilities)
  - A.12.1.1 Dokumentierte Bedienabläufe (en: Documented operating procedures)
  - A.12.1.2 Änderungssteuerung (en: Change management)
  - A.12.1.3 Kapazitätssteuerung (en: Capacity management)
  - A.12.1.4 Trennung von Entwicklungs-, Test- und Betriebsumgebungen (en: Separation of development, testing and operational environments)
- A.12.2 Schutz vor Schadsoftware (en: Protection from malware)
  - A.12.2.1 Maßnahmen gegen Schadsoftware (en: Controls against malware)
- A.12.3 Datensicherung (en: Backup)
  - A.12.3.1 Sicherung von Information (en: Information backup)
- A.12.4 Protokollierung und Überwachung (en: Logging and monitoring)
  - A.12.4.1 Ereignisprotokollierung (en: Event logging)
  - A.12.4.2 Schutz der Protokollinformation (en: Protection of log information) A.12.4.3 Administratoren- und Bedienerprotokolle (en: Administrator and operator logs)
  - A.12.4.4 Uhrensynchronisation (en: Clock synchronisation)
- A.12.5 Steuerung von Software im Betrieb (en: Control of operational software)
  - A.12.5.1 Installation von Software auf Systemen im Betrieb (en: Installation of software on operational systems))

- A.12.6 Handhabung technischer Schwachstellen (en: Technical vulnerability management)
  - A.12.6.1 Handhabung von technischen Schwachstellen (en: Management of technical vulnerabilities)
  - A.12.6.2 Einschränkung von Softwareinstallation (en: Restrictions on software installation)
- A.12.7 Audit von Informationssystemen (en: Information systems audit considerations)
  - A.12.7.1 Maßnahmen für Audits von Informationssystemen (en: Information systems audit controls)>

A.13 Kommunikationssicherheit

(en: Communications security)

Der Inhalt von A.13 Kommunikationssicherheit (en: Communications security) ist zu erklären:

- A.13.1 Netzwerksicherheitsmanagement (en: Network security management)
  - A.13.1.1 Netzwerksteuerungsmaßnahmen (en: Network controls)
  - A.13.1.2 Sicherheit von Netzwerkdiensten (en: Security of network services)
  - A.13.1.3 Trennung in Netzwerken (en: Segregation in networks)
- A.13.2 Informationsübertragung (en: Information transfer)
  - A.13.2.1 Richtlinien und Verfahren zur Informationsübertragung (en: Information transfer policies and procedures)
  - A.13.2.2 Vereinbarungen zur Informationsübertragung (en: Agreements on information transfer)
  - A.13.2.3 Elektronische Nachrichtenübermittlung (en: Electronic messaging)
  - A.13.2.4 Vertraulichkeits- oder Geheimhaltungs-vereinbarungen (en: Confidentiality or nondisclosure agreements)

A.14 Anschaffung, Entwicklung und Instandhalten von Systemen (en: System acquisition, development and maintenance)

Der Inhalt von A.14 Anschaffung, Entwicklung und Instandhalten von Systemen (en: System acquisition, development and maintenance) ist zu erklären:

- A.14.1 Sicherheitsanforderungen an Informationssysteme (en: Security requirements of information systems)
  - A.14.1.1 Analyse und Spezifikation von Informationssicherheitsanforderungen (en: Information security requirements analysis and specification)
  - A.14.1.2 Sicherung von Anwendungsdiensten in öffentlichen Netzwerken (en: Securing application services on public networks)
  - A.14.1.3 Schutz der Transaktionen bei Anwendungsdiensten (en: Protecting application services transactions)

- A.14.2 Sicherheit in Entwicklungs- und Unterstützungsprozessen (en: Security in development and support processes)
    - A.14.2.1 Richtlinie für sichere Entwicklung (en: Secure development policy)
    - A.14.2.2 Verfahren zur Verwaltung von Systemänderungen (en: System change control procedures)
    - A.14.2.3 Technische Überprüfung von Anwendungen nach Änderungen an der Betriebsplattform (en: Technical review of applications after operating platform changes)
    - A.14.2.4 Beschränkung von Änderungen an Softwarepaketen (en: Restrictions on changes to software packages)
    - A.14.2.5 Grundsätze für die Analyse, Entwicklung und Pflege sicherer Systeme (en: Secure system engineering principles)
    - A.14.2.6 Sichere Entwicklungsumgebung (en: Secure development environment)
    - A.14.2.7 Ausgegliederte Entwicklung (en: Outsourced development)
    - A.14.2.8 Testen der Systemsicherheit (en: System security testing)
    - A.14.2.9 Systemabnahmetest (en: System acceptance testing)
- A.14.3 Testdaten (en: Test data)
    - A.14.3.1 Schutz von Testdaten (en: Protection of test data)

A.15 Lieferantenbeziehungen (en: Supplier relationships)

Der Inhalt von A.15 Lieferantenbeziehungen (en: Supplier relationships) ist zu erklären:

- A.15.1 Informationssicherheit in Lieferantenbeziehungen (en: Information security in supplier relationships)
    - A.15.1.1 Informationssicherheitsrichtlinie für Lieferantenbeziehungen (en: Information security policy for supplier relationships)
    - A.15.1.2 Behandlung von Sicherheit in Lieferantenvereinbarungen (en: Addressing security within supplier agreements)
    - A.15.1.3 Lieferkette für Informations- und Kommunikationstechnologie (en: Information and communication technology supply chain)
- A.15.2 Steuerung der Dienstleistungserbringung von Lieferanten (en: Supplier service delivery management)
    - A.15.2.1 Überwachung und Überprüfung von Lieferantendienstleistungen (en: Monitoring and review of supplier services)
    - A.15.2.2 Handhabung der Änderungen von Lieferantendienstleistungen (en: Managing changes to supplier services)

A.16 Handhabung von Informationssicherheitsvorfällen (en: Information security incident management)

Der Inhalt von A.16 Handhabung von Informationssicherheitsvorfällen (en: Information security

incident management) ist zu erklären:

- A.16.1 Handhabung von Informationssicherheitsvorfällen und Verbesserungen (en: Management of information security incidents and improvements)
    - A.16.1.1 Verantwortlichkeiten und Verfahren (en: Responsibilities and procedures)
    - A.16.1.2 Meldung von Informationssicherheitsereignissen (en: Reporting information security events)
    - A.16.1.3 Meldung von Schwächen in der Informationssicherheit (en: Reporting information security weaknesses)
    - A.16.1.4 Beurteilung von und Entscheidung über Informationssicherheitsereignisse (en: Assessment of and decision on information security events)
    - A.16.1.5 Reaktion auf Informationssicherheitsvorfälle (en: Response to information security incidents)
    - A.16.1.6 Erkenntnisse aus Informationssicherheitsvorfällen (en: Learning from information security incidents)
    - A.16.1.7 Sammeln von Beweismaterial (en: Collection of evidence)

A.17 Informationssicherheitsaspekte beim Business Continuity Management (en: nformation security aspects of business continuity management)

Der Inhalt vonA.17 Informationssicherheitsaspekte beim Business Continuity Management (en: Information security aspects of business continuity ist zu erklären:

- A.17.1 Aufrechterhalten der Informationssicherheit (en: Information security continuity)
    - A.17.1.1 Planung zur Aufrechterhaltung der Informationssicherheit (en: Planning information security continuity)
    - A.17.1.2 Umsetzen der Aufrechterhaltung der Informationssicherheit (en: Implementing information security continuity)
    - A.17.1.3 Überprüfen und Bewerten der Aufrechterhaltung der Informationssicherheit (en: Verify, review and evaluate information security continuity)
    - A.17.2 Redundanzen (en: Redundancies)
    - A.17.2.1 Verfügbarkeit von informationsverarbeitenden Einrichtungen (en: Availability of information processing facilities)

A.18 Compliance (en:Compliance)

Der Inhalt von A.18 Compliance ist zu erklären:

- A.18.1 Einhaltung gesetzlicher und vertraglicher Anforderungen (en: Compliance with legal
  and contractual requirements)
  - A.18.1.1 Bestimmung der anwendbaren Gesetzgebung und der vertraglichen Anforderungen (en: Identification of applicable legislation and contractual requirements)
  - A.18.1.2 Geistige Eigentumsrechte (en: Intellectual property rights)
  - A.18.1.3 Schutz von Aufzeichnungen (en: Protection of records)
  - A.18.1.4 Privatsphäre und Schutz von personenbezogener Information (en: Privacy
    and protection of personally identifiable information)
  - A.18.1.5 Regelungen bezüglich kryptographischer Maßnahmen (en: Regulation of
    cryptographic controls)
- A.18.2 Überprüfungen der Informationssicherheit (en: Information security reviews)
  - A.18.2.1 Unabhängige Überprüfung der Informationssicherheit (en: Independent review of information security)
  - A.18.2.2 Einhaltung von Sicherheitsrichtlinien und -standards (en: Compliance with
    security policies and standards)
  - A.18.2.3 Überprüfung der Einhaltung von technischen Vorgaben (en: Technical compliance review)

mindestens 3 praktisch Übungen gefordert

für die Übungen müssen mindestens 40% der Zeit, die für diesen Abschnitt vorgesehen ist verwendet werden.

Beispiele: Gruppenarbeit mit Präsentation

•
Erstellung eines Asset Inventories inklusive eines Klassifizierungssystems für eine fiktive Organisation (A8)
•

Erstellung einer Richtlinie (A5) für die Verwendung von kryptografischen Maßnahmen (A10)
•
Erstellung eines dokumentierten Bedienablaufs zur Veränderung von Firewall-Regeln (A12.1)
•
Entwicklung eines Konzeptes zur Übergabe von Daten aus dem Lifesystem ins Testsystem (Anonymisierung – A14.3)
•
Erstellung eines risikobasierten Klassifizierungssystems zur Einordnung von Lieferanten (A15)
•
Erstellung eines Prozesses zur Handhabung von Informationssicherheitsvorfällen (A16.1)
Hinweise:
• https://de.wikipedia.org/wiki/Klassifizierung
• FitSM Anfoderungen
http://fitsm.itemo.org/sites/default/files/FitSM-1_Anforderungen.pdf
    ◦ PR12 Change Management (CHM)
    ◦ PR9 Incident & Service Request Management (ISRM)
• BSI Behandlung von Sicherheitsvorfällen
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b01/b01008.html
• Standard Operating Procedure
https://de.wikipedia.org/wiki/Standard_Operating_Procedure
• Anonymisierung und Pseudonymisierung
https://de.wikipedia.org/wiki/Anonymisierung_und_Pseudonymisierung

23. Verwandte Themen
Related Topics

Severity: 4.00% — Minutes: 96 — Min/avg/max number of questions: 1.5/2.0/2.5

- Zertifizierung von Managementsystemen
  - Darlegung des typischen Ablaufes einer Unternehmenszertifizierung
  - https://www.beuth.de/de/norm/din-en-iso-iec-17021-1/231355332
    DIN EN ISO/IEC 17021-1:2015-11
    Titel (Deutsch): Konformitätsbewertung - Anforderungen an Stellen, die Managementsysteme auditieren und zertifizieren
    Teil 1: Anforderungen (ISO/IEC 17021-1:2015); Deutsche und Englische Fassung EN ISO/IEC 17021-1:2015
    Dieser Teil von ISO/IEC 17021 legt Anforderungen an Stellen fest, die Managementsysteme auditieren und zertifizieren. Diese Norm enthält Grundsätze für und Anforderungen an die Kompetenz, Folgerichtigkeit und Unparteilichkeit von Stellen, die Audits und Zertifizierungen von Managementsystemen jeglicher Art. Sie liefert allgemeine Anforderungen für solche Stellen, die Audits und Zertifizierungen auf dem Gebiet der Qualität, Umwelt und anderer Formen von Managementsystemen durchführen. Solche Stellen werden als Zertifizierungsstellen bezeichnet. Eine Zertifizierungsstelle kann staatlich oder nichtstaatlich, mit oder ohne Regulierungsbefugnis sein. Die Einhaltung dieser Anforderungen ist vorgesehen, um sicherzustellen, dass Zertifizierungsstellen die Zertifizierung von Managementsystemen kompetent, konsistent und unparteilich durchführen und dadurch die Anerkennung solcher Stellen und die Akzeptanz ihrer Zertifizierungen auf nationaler und internationaler Ebene zu fördern. Dieser Teil von ISO/IEC 17021 gilt für die Auditierung und Zertifizierung beliebiger Arten von Managementsystemen.
  - https://www.beuth.de/de/norm/iso-iec-27006/243238004
    ISO/IEC 27006:2015-10
    Titel (Deutsch): Informationstechnik - IT-Sicherheitsverfahren - Anforderungen an Institutionen, die Audits und Zertifizierungen von Informationssicherheits-Managmentsystemen anbieten.
- Risikomanagement
  - https://www.beuth.de/de/norm/iso-iec-27005/143000568
    ISO/IEC 27005:2011-06
    Titel (Deutsch): Informationstechnik - IT-Sicherheitsverfahren - Informationssicherheits-Risikomanagement
  - https://www.beuth.de/de/norm/iso-31000/124279874

ISO 31000:2009-11
Titel (Deutsch): Risikomanagement - Allgemeine Anleitung zu den Grundsätzen und zur Implementierung eines Risikomanagements

- Auditprogramm- und Auditmanagement
  - https://de.wikipedia.org/wiki/ISO_19011
    1. Anwendungsbereiche
    2. Normative Verweisungen
    3. Begriffe und Definitionen
    4. Auditprinzipien
    5. Leiten und Lenken eines Auditprogramms
    6. Durchführung eines Audit
       1. Allgemeines
       2. Veranlassen des Audits
       3. Vorbereiten der Audittätigkeiten
       4. Durchführen der Audittätigkeiten
       5. Erstellen und Verteilen des Auditberichts
       6. Abschließen des Audits
       7. Durchführen von Auditfolgemaßnahmen
    7. Kompetenz und Bewertung von Auditoren
  - https://www.beuth.de/de/norm/dineniso19011/144285002
    DIN EN ISO 19011: Die neue internationale Norm für alle Management-Audits:
    Dieser Leitfaden richtet sich an alle Organisationen und Personen, die interne oder externe Audits von Managementsystemen durchführen oder für das Management des Auditprogramms verantwortlich sind.
    Andere mögliche Anwender dieser Norm sind Organisationen, die auf dem Gebiet der Auditor-Zertifizierung und -Schulung sowie Akkreditierung und Normung von Konformitätsbewertungen tätig sind.
    Deutliche Erweiterung des Anwendungsbereichs von DIN EN ISO 19011
    Die deutliche Erweiterung des Anwendungsbereichs von DIN EN ISO 19011 auf alle Arten von Managementsystemen stellt einen Meilenstein in der Normung dar:
    Es ist erstmals gelungen, die Prinzipien und den Umgang im Auditieren von Managementsystemen in einem einheitlichen Leitfaden zusammenzufassen.
    Die Leitlinien der Norm beschreiben damit einen systematischen, unabhängigen und dokumentierten Prozess zur akkuraten Durchführung von Audits und deren objektiven Auswertung.
    DIN EN ISO 19011: Leitlinien für Audits leisten Beitrag zum Erfolg von Organisationen
    Die enthaltenen Leitlinien in der Norm DIN EN ISO 19011 können auf beliebige andere Arten von Audits erweitert und angewendet werden. Durch die Beachtung dieser Leitlinien ist es möglich, dass gut gemanagte Audits einen weiteren Beitrag zum Erfolg der Organisationen leisten.
- https://de.wikipedia.org/wiki/Klassifizierung
- https://de.wikipedia.org/wiki/Klassifikationsverfahren
- https://de.wikipedia.org/wiki/Ontologie_(Informatik)