ISMS 27001 Foundation — Syllabus

State: released - ID: 105 - Topic: ISMS 27001 - Version: 1 - language: deutsch - valid from 2017-10-01
Anzahl der Prüfungsfragen: 30
Schulungszeit in Minuten: 960

Die verpflichtende Zeitvorgabe für die dazugehörige Schulung ist 2 Tage à min. 8 Stunden mit je 60 Minuten (= 960 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: 45 Minuten
- Format: Multiple Choice-Fragen; mit zwei oder drei Antwortmöglichkeiten, von denen eine, zwei oder auch alle drei Antworten korrekt sein können.
- min. Punkte: 20 von 30
- 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.

1. Begriffe
(en: Terms and definitions)

Severity: 5.00% — Minutes: 48 — Min/avg/max number of questions: 1.0/1.5/2.0

Dokument: ISO/IEC DIS 27000:2015

Folgenden Definitionen sind zu erklären:

- 2.5 Audit
- 2.9 Verfügbarkeit (en: availability)
- 2.12 Vertraulichkeit (en: confidentiality)
- 2.13 Konformität (en: conformity)
- 2.15 fortlaufende Verbesserung (en: continual improvement)
- 2.16 Maßnahme (en: control)
- 2.17 Maßnahmenziel (en: control objective)
- 2.23 dokumentierte Information (en: documented information)
- 2.24 Wirksamkeit (en: effectiveness)
- 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)
- 2.40 Integrität (en: integrity)
- 2.41 Interessierte Partei (en: interested party)
- 2.43 ISMS-Projekt (en: ISMS project)
- 2.44 Risikoniveau (en: level of risk)
- 2.46 Managementsystem (en: management system)
- 2.53 Nichtkonformität (en: nonconformity)
- 2.56 Ziel (en: objective)
- 2.57 Organisation (en: organization)
- 2.60 Politik (en: policy)
- 2.61 Prozess (en: process)
- 2.63 Anforderung (en: requirement)
- 2.65 Überprüfung (en: review)
- 2.68 Risiko (en: risk)
- 2.69 Risikoakzeptanz (en: risk acceptance)
- 2.76 Risikomanagement (en: risk management)

- 2.82 Stakeholder (en: stakeholder)
- 2.83 Bedrohung (en: threat)
- 2.84 oberste Leitung (en: top management)
- 2.89 Schwachstelle (en: vulnerability)

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

Severity: 20.00% — Minutes: 192 — Min/avg/max number of questions: 5.0/6.0/7.0

Dokument: ISO/IEC DIS 27000:2015

Folgenden Abschnitte im Kapitel 3 Managementsysteme für Informationssicherheit (ISMS) (en: Information security management systems) sind zu erklären:

- Aus 3.2 Was ist ein ISMS? (en: What is an ISMS?)
  - 3.2.1 Übersicht und Grundsätze (en: Overview and principles) - EINSCHRÄNKUNG Abschnitt 1 nur bis "... trägt zu der erfolgreichen Umsetzung eines ISMS bei." - Die elementaren Grundsätze müssen nicht erklärt werden.
  - 3.2.2 Informationen
  - 3.2.3 Informationssicherheit (en: Information security)
  - 3.2.4 Management
- Aus 3.4 Warum ist ein ISMS wichtig? (en: Why an ISMS is important?) EINSCHRÄNKUNG Abschnitt 1 und 2 bis "... Anforderungen der Organisation skaliert und aktualisiert wird."
- Aus 3.5 Einführung, Überwachung, Pflege und Verbesserung eines ISMSig? (en: Establishing, monitoring, maintaining and improving an ISMS)
  - 3.5.1 Übersicht (en: Overview)
- 3.7 Nutzen der ISMS-Normenfamilie (en: 3.7 Benefits of the ISMS family of standards)

Folgenden Abschnitte im Kapitel 4 ISMS-Normenfamilie (en: 4 ISMS family of standards) 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)
- 4.3.1 ISO/IEC 27001 aus Normen, die Anforderungen festlegen (en: 4.3.1 ISO/IEC 27001 from Standards specifying requirements)
- 4.4.1 ISO/IEC 27002 aus Normen, die allgemeine Leitfäden beschreiben (en: 4.4.1 ISO/IEC 27002 from Standards describing general guidelines)

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

Severity: 5.00% — Minutes: 48 — Min/avg/max number of questions: 1.0/1.5/2.0

Dokument: DIN ISO/IEC 27001:2015-03

Folgenden Abschnitte im Kapitel **4 Kontext der Organisation** (en: Context of the organization) 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: 4.3 Determining the scope of the information security management system) EINSCHRÄNKUNG nur bis "... um dessen Anwendungsbereich festzulegen"
- 4.4 Informationssicherheitsmanagement-system (en: Information security management system)

4. Führung
(en: Leadership)

Severity: 5.00% — Minutes: 48 — Min/avg/max number of questions: 1.0/1.5/2.0

Dokument: DIN ISO/IEC 27001:2015-03

Folgenden Abschnitte im Kapitel 5 Führung (en: Leadership) sind zu erklären:

- 5.1 Führung und Verpflichtung (en: Leadership and commitment)
- 5.2 Politik (en: Policy)
  EINSCHRÄNKUNG erst ab "Die Informationssicherheitspolitik muss: .."
- 5.3 Rollen, Verantwortlichkeiten und Befugnisse in der Organisation (en: Organizational roles, responsibilities and authorities)
  EINSCHRÄNKUNG nur bis "... und bekannt gemacht werden."

5. Planung
(en: Planning)

Severity: 15.00% — Minutes: 144 — Min/avg/max number of questions: 3.5/4.5/5.5

Folgenden Abschnitte im Kapitel 6 Planung (en: Planning) sind zu erklären:

- 6.1.2 Informationssicherheitsrisikobeurteilung (en: Information security risk assessment)
- 6.1.3 Informationssicherheitsrisiko-behandlung (en: Information security risk treatment)

6. Unterstützung (en: Support)

Severity: 5.00% — Minutes: 48 — Min/avg/max number of questions: 1.0/1.5/2.0

Folgenden Abschnitte im Kapitel 7 Unterstützung (en: Support) sind zu erklären:

- 7.1 Ressourcen (en: Resources)
- 7.2 Kompetenz (en: Competence)
  EINSCHRÄNKUNG nur bis "... Schulung oder Erfahrung kompetent sind;"
- 7.3 Bewusstsein (en: Awareness)
- 7.4 Kommunikation (en: Communication)
- 7.5 Dokumentierte Information (en: Documented information)
- 7.5.1 Allgemeines (en: General)
  EINSCHRÄNKUNG ohne ANMERKUNG
- 7.5.2 Erstellen und Aktualisieren (en: Creating and updating)
  EINSCHRÄNKUNG nur bis "... f) Aufbewahrung und Verfügung über den weiteren Verbleib"

7. Betrieb
(en: Operation)

Severity: 5.00% — Minutes: 48 — Min/avg/max number of questions: 1.0/1.5/2.0

Folgenden Abschnitte im Kapitel 8 Betrieb (en: Operation) sind zu erklären:

- 8.2 Informationssicherheitsrisikobeurteilung (en: Information security risk assessment)
- 8.3 Informationssicherheitsrisikobehandlung (en: Information security risk treatment)

8. Bewertung der Leistung (en: Performance evaluation)

Severity: 10.00% — Minutes: 96 — Min/avg/max number of questions: 2.5/3.0/3.5

Folgenden Abschnitte im Kapitel 9 Bewertung der Leistung (en: Performance evaluation) sind zu erklären:

- 9.1 Überwachung, Messung, Analyse und Bewertung (en: Monitoring, measurement, analysis and evaluation)
  EINSCHRÄNKUNG nur bis "... Wirksamkeit des Informationssicherheits-managementsystems bewerten."
- 9.2 Internes Audit (en: Internal audit)
  EINSCHRÄNKUNG nur bis "... b) wirksam verwirklicht und aufrechterhalten wird."
- 9.3 Managementbewertung (en: Management review)
  EINSCHRÄNKUNG nur bis "... fortdauernde Eignung, Angemessenheit und Wirksamkeit sicherzustellen."

9. Verbesserung (en: Improvement)

Severity: 5.00% — Minutes: 48 — Min/avg/max number of questions: 1.0/1.5/2.0

Folgenden Abschnitte im Kapitel 10 Verbesserung (en: Improvement) sind zu erklären:

- 10.2 Fortlaufende Verbesserung (en: Continual improvement)

10. Anhang A - Referenzmaßnahmenziele (en: Annex A - Reference control objectives)

Severity: 20.00% — Minutes: 192 — Min/avg/max number of questions: 5.0/6.0/7.0

Es sind die Ziel für alle Maßnahmen zu den Kapiteln (clauses) 5 -18 zu erklären, sowie die Struktur des Anhangs A in Kapitel (clause), Maßnahmenziele (control objectives) und Maßnahmen (controls).

11. Verwandte Themen

Severity: 5.00% — Minutes: 48 — Min/avg/max number of questions: 1.0/1.5/2.0

Demingkreis - Quelle: https://de.wikipedia.org/wiki/Demingkreis
oder auch Deming-Rad, PDCA-Zyklus beschreibt einen iterativen vierphasigen Prozess für Lernen und Verbesserung. Die Ursprünge des Prozesses liegen in der Qualitätssicherung. Vier Phasen des PDCA-Zyklus
Plan - der jeweilige Prozess muss vor seiner eigentlichen Umsetzung geplant werden: Plan umfasst das Erkennen von Verbesserungspotentialen (in der Regel durch den Arbeitnehmer beziehungsweise Teamleiter vor Ort), die Analyse des aktuellen Zustands sowie das Entwickeln eines neuen Konzeptes (unter intensiver Einbindung des Arbeitnehmers).
Do - Do bedeutet entgegen weit verbreiteter Auffassung nicht die Einführung und Umsetzung auf breiter Front, sondern das Ausprobieren beziehungsweise Testen und praktische Optimieren des Konzeptes mit schnell realisierbaren, einfachen Mitteln (z. B. provisorische Vorrichtungen) an einem einzelnen Arbeitsplatz [wieder unter starker Einbindung des Arbeitnehmers (Gemba)].
Check - der im Kleinen realisierte Prozessablauf und seine Resultate werden sorgfältig überprüft und bei Erfolg für die Umsetzung auf breiter Front allgemein freigegeben.
Act - in der Phase Act wird die neue allgemeine Vorgabe auf breiter Front eingeführt, festgeschrieben und regelmäßig auf Einhaltung überprüft (Audits). Hier handelt es sich tatsächlich um eine „große Aktion“, die im Einzelfall umfangreiche organisatorische Aktivitäten (z. B. Änderung von Arbeitsplänen, NC-Programmen, Stammdaten, die Durchführung von Schulungen, Anpassung von Aufbau- und Ablauforganisation) sowie erhebliche Investitionen (an allen vergleichbaren Arbeitsplätzen, in allen Werken) umfassen kann. Die Verbesserung dieses Standards beginnt wiederum mit der Phase Plan.

ISO 9000 - Quelle: https://de.wikipedia.org/wiki/Qualitätsmanagementnorm
Eine Qualitätsmanagementnorm beschreibt, welchen Anforderungen das Managementsystem eines Unternehmens genügen muss, um einem bestimmten Standard bei der Umsetzung des Qualitätsmanagements zu entsprechen. Es kann sowohl informativ für die Umsetzung innerhalb eines Unternehmens als auch zum Nachweis bestimmter Standards gegenüber Dritten dienen. Der Nachweis wird durch einen Zertifizierungsprozess mit anschließender Ausstellung eines zeitlich befristeten Zertifikates durch unabhängige Zertifizierungsstellen erbracht.
Des Weiteren werden die acht Grundsätze des Qualitätsmanagements aufgelistet:
1) Kundenorientierung
2) Verantwortlichkeit der Führung
3) Einbeziehung der beteiligten Personen
4) Prozessorientierter Ansatz
5) Systemorientierter Managementansatz

6) Kontinuierliche Verbesserung
7) Sachbezogener Entscheidungsfindungsansatz
8) Lieferantenbeziehungen zum gegenseitigen Nutzen

ISO 20000 - Quelle: https://de.wikipedia.org/wiki/ISO/IEC_20000
Die ISO/IEC 20000 ist eine international anerkannte Norm zum IT Service Management (ITSM). Innerhalb der ISO/IEC 20000 werden die folgenden Anforderungen und Prozesse definiert:

Kap 4 Service Management System - Allgemeine Anforderungen (en: Service management system - general requirements)

1. Verantwortung des Managements (en: Management responsibility)
2. Steuerung von Prozessen, die von Drittparteien durchgeführt werden (en: Governance of processes operated by oher parties)
3. Dokumentenmanagement (en: Documentation management)
4. Ressourcen Management
5. Einrichten und Verbessern der SMS (en: Establish and improve the SMS)

Kap 5 Design und Überführung neuer oder geänderter Services (en: Design and transition of new or changed services)

1. Allgemeines (en: general)
2. Planen neuer oder geänderter Services (en: Plan new or changed services)
3. Design und Entwicklung neuer oder geänderter Services (en: Design and development of new or changed services)
4. Überführung neuer oder geänderter Services (en: Transition of new or changed services)

Kap 6 Service Delivery Prozesse

1. Service Level Management
2. Service Reporting
3. Service Continuity and Availability Management
4. Budgetplanung und Buchführung für Service (en: Budgeting and accounting for services)
5. Capacity Management
6. Information Security Management

Kap 7 Beziehungsprozesse (en: Relationship processes)

1. Business Relationship Management
2. Supplier Management

Kap 8 Lösungsprozesse (en: Resolution processes)

1. Incident und Service Request Management
2. Problem Management

Kap 9 Control Prozesse

1. Configuration Management
2. Change Management
3. Release und Deployment Management

IT-Grundschutz-Kataloge - Quelle: https://de.wikipedia.org/wiki/IT-Grundschutz-Kataloge
Die IT-Grundschutz-Kataloge (vor 2005: IT-Grundschutzhandbuch) sind eine Sammlung von Dokumenten des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI), die der Erkennung und Bekämpfung sicherheitsrelevanter Schwachstellen in IT-Umgebungen (IT-Verbund) dienen. Die Sammlung umfasst mit Einleitung und Katalogen über 4.800 Seiten (15. Ergänzungslieferung aus 2016) und dient Unternehmen und Behörden als Grundlage zum Erlangen einer Zertifizierung nach IT-Grundschutz. Durch die Zertifizierung zeigt ein Unternehmen, dass es geeignete Maßnahmen zur Absicherung seiner IT-Systeme gegen IT-Sicherheitsbedrohungen unternommen hat.

ISIS12 - Quelle: https://de.wikipedia.org/wiki/ISIS12
ISIS12 (kurz für Informations-Sicherheitsmanagement System in 12 Schritten) ist ein Modell zur Einführung eines Information Security Management System (ISMS). Es beinhaltet eine Untermenge der Forderungen der IT-Grundschutz-Kataloge und der ISO/IEC 27001 und soll es auf diese Weise dem Mittelstand einfacher machen, Informationssicherheit systematisch herzustellen. ISIS12 bildet eine unabhängig zertifizierbare Einstiegsstufe in ein ISMS, wobei eine Kompatibilität zu IT-Grundschutz und ISO/IEC 27001 und somit die Möglichkeit für ein späteres "Upgrade" gewahrt bleibt.
Die Einführung eines ISMS nach ISIS12 wird in 12 Schritten vollzogen:
1) Mitarbeiter sensibilisieren
2) Informationssicherheitsteam aufbauen
3) IT-Dokumentationsstruktur festlegen
4) IT-Servicemanagement-Prozess einführen
5) Kritische Applikationen identifizieren
6) IT-Struktur analysieren
7) Sicherheitsmaßnahmen modellieren
8) Ist-Soll vergleichen
9) Umsetzung planen
10)Umsetzen
11) Revision
Die Schritte werden zeitabhängig iterativ durchlaufen, so dass sich ein PDCA-Zyklus einstellt.

ISO/IEC 15408 (Common Criteria) - Quelle: https://de.wikipedia.org/wiki/Common_Criteria_for_Information_Technology_Security_Evaluation
Die Common Criteria for Information Technology Security Evaluation (kurz auch Common Criteria oder CC; zu deutsch: Allgemeine Kriterien für die Bewertung der Sicherheit von Informationstechnologie) sind ein internationaler Standard zur Prüfung und Bewertung der Sicherheitseigenschaften von IT-Produkten. Durch die Verabschiedung der Norm ISO/IEC 15408 am 1. Dezember 1999 sind die Common Criteria ein allgemeiner und weltweit anerkannter Standard.

Die Common Criteria unterscheiden zwischen der Funktionalität (Funktionsumfang) des betrachteten Systems und der Vertrauenswürdigkeit (Qualität). Die Unterscheidung zwischen der Funktionalität eines Systems auf der einen Seite und dem Vertrauen, das durch eine Prüfung in diese Funktionalität entstehen kann, ist eines der wesentlichen Paradigmen der Common Criteria. Die Vertrauenswürdigkeit wird nach den Gesichtspunkten der Wirksamkeit der verwendeten Methoden und der Korrektheit der Implementierung betrachtet.