

SC550 BSI IT-Grundschutz-Praktiker

Kurzbeschreibung:

Ein zertifizierter IT-Grundschutz-Praktiker kann Behörden und Unternehmen bei der Entwicklung von Sicherheitskonzepten unterstützen oder bei der Einführung eines Managementsystems zur Informationssicherheit begleiten.

Der Workshop **SC550 BSI IT-Grundschutz-Praktiker** erfüllt das Curriculum sowie die Qualifizierungsanforderungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und versetzt Sie in die Lage, die Aufgaben eines IT Sicherheitsbeauftragten (ITSiBe) oder Informationssicherheitsbeauftragten (ISB) zu übernehmen.

Der Fokus liegt auf der Vermittlung des erforderlichen Fachwissens aus dem Bereich der Informationssicherheit und dem Aufbau eines Managementsystems zur Informationssicherheit (ISMS). Sie erlernen, das Management bei der Wahrnehmung der Pflichten zur Sicherstellung eines angemessenen Informationssicherheitsniveaus zu unterstützen, angemessene Maßnahmen für Ihr Sicherheitskonzept zu bestimmen sowie den spezifischen Schutzbedarf Ihrer Informationen, Anwendungen und IT-Systeme zu identifizieren.

Das Seminar ist der Einstieg in das offizielle Zertifizierungsprogramm des BSI und entspricht der IT-Grundschutz-Basisbildung. Teilnehmer, die die Prüfung zum IT-Grundschutz-Praktiker bestehen, sind berechtigt, an der IT-Grundschutz-Aufbauschulung zum IT-Grundschutz-Berater teilzunehmen.

Zielgruppe:

- Angehende Informationssicherheitsbeauftragte
- Datensicherheitsbeauftragte
- Datenschutzbeauftragte
- IT-Leiter / IT-Administratoren
- Verantwortliche für den Bereich Informationssicherheit
- Verantwortliche für den Bereich Risikomanagement
- Verantwortliche für den Bereich Business Continuity Management
- Verantwortliche für die Bereiche Revision und IT-Revision
- Security Manager
- Führungskräfte / Projektleiter

Voraussetzungen:

Um den Inhalten und dem Lerntempo gut zu folgen, sind Grundkenntnisse in der IT-Sicherheit bzw. Informationssicherheit nötig. Generelles Interesse am Zertifikat **BSI IT-Grundschutz-Praktiker** wird vorausgesetzt.

Sonstiges:

Dauer: 4 Tage

Preis: 2200 Euro plus MwSt.

Ziele:

Schwerpunkte dieses Kurses sind:

- Fachbegriffe aus dem Bereich der Informationssicherheit
- Fachwissen für Planung, Aufbau und Betrieb sowie die Aufrechterhaltung und Verbesserung eines ISMS gemäß BSI-Grundschutz
- Sicherstellung eines angemessenen Informationssicherheitsniveaus
- Bestimmung der Maßnahmen für Ihr Sicherheitskonzept
- Identifizierung des spezifischen Schutzbedarfes Ihrer Informationen, Anwendungen und Ihrer IT-Systeme

Am letzten Kurstag können Sie Ihr Wissen bei einer Prüfung nachweisen.

Bei Erfolg, erhalten Sie das Zertifikat **BSI IT-Grundschutz-Praktiker**.

Prüfung: 50 Multiple-Choice-Fragen in 60 Minuten

Die Prüfung ist bestanden, wenn 60% der Fragen richtig beantwortet werden.

Inhalte/Agenda:

- **Einführung und Grundlagen der IT-Sicherheit und rechtliche Rahmenbedingungen**
 - ◆ Motivation für Informationssicherheit und Abgrenzung zum Datenschutz
 - ◆ Begriffsbestimmungen
 - ◇ (Arten und Wichtigkeit von Informationen, Sicherheitsziele, Aspekte der Integrität, Verfügbarkeit, Vertraulichkeit usw.)
 - ◆ IT Compliance und IT Governance
 - ◆ Rechtsvorschriften
 - ◇ (BSIG, IT-SiG etc.), Standards und Normen in der Informationssicherheit
- **Normen und Standards der Informationssicherheit**
 - ◆ Überblick, Zweck und Struktur über relevante Normen und Richtlinien (z.B. ISO 2700x usw.)
 - ◆ Cobit, ITIL usw.
 - ◆ IT-Grundschutz-Kompodium
 - ◆ Branchenspezifische Sicherheitsstandards und IT-Grundschutz-Profile
- **Einführung IT-Grundschutz**
 - ◆ IT-Grundschutz-Bestandteile
 - ◆ Standards: 200-1 "Managementsysteme für Informationssicherheit" / 200-2 "IT-Grundschutz-Methodik" / 200-3 "Risikoanalyse auf Basis von IT-Grundschutz" / 100-4 "Notfallmanagement"
 - ◆ IT-Grundschutz-Kompodium: Baueinstruktur und -inhalte wie: APP, CON, DER, IND, INF, ISMS, NET, OPS, ORP und SYS
 - ◆ Die Sicherheitsorganisation und Verantwortlichkeiten im ISMS
 - ◆ Sicherheitsprozess (Umsetzung eines ISMS als integriertes Managementsystem)
 - ◆ Dokumentation im Sicherheitsprozess (Leitlinie, Richtlinien, Referenzdokumente, Konzepte)
 - ◆ Rollen, Verantwortung und Aufgaben (Leitlinie, Informationssicherheitsbeauftragte, ICS-Informationssicherheitsbeauftragte, Informations-Management-Team, usw.)
 - ◆ Erstellen einer Sicherheitskonzeption nach den unterschiedlichen Vorgehensweisen des IT-Grundschutzes:
 - ◇ Basisabsicherung, Standardabsicherung, Kernabsicherung
- **IT-Grundschutz-Vorgehensweise (Überblick)**
 - ◆ Leitfragen zur IT-Grundschutz-Absicherung
 - ◆ Basis-Anforderungen
 - ◆ Standard-Anforderungen
 - ◆ Anforderungen für den erhöhten Schutzbedarf
 - ◆ Wahl der Vorgehensweise am Praxisbeispiel
- **Kompodium (Überblick)**
 - ◆ Aufbau und Anwendung des Kompodiums
 - ◆ ISMS (Managementsystem für Informationssicherheit)
 - ◆ Prozess-Bausteine
 - ◆ System-Bausteine
 - ◆ Umsetzungshinweise
- **Umsetzung der IT-Grundschutz-Vorgehensweise**
 - ◆ Festlegen des Geltungsbereichs und des Informationsverbundes
 - ◆ Strukturanalyse, Vereinfachten Netzplan erstellen, Netzplanerhebung
 - ◆ Geschäftsprozess und zugehörige Anwendungen sowie IT-Systeme, Räume erfassen
 - ◆ Schutzbedarfskategorien, Vorgehen und Vererbung (Maximumprinzip, Verteilungs- und Kumulationseffekt)
 - ◆ Modellierung eines Informationsverbundes gemäß IT-Grundschutz
 - ◇ (Vorgehensweise, Dokumentation, Anforderungen anpassen)
- **IT-Grundschutz-Check**
 - ◆ Was wird geprüft?
 - ◆ Vorbereitung und Durchführung
 - ◆ IT-Grundschutz-Check dokumentieren
 - ◆ Entscheidungskriterien
 - ◆ Beispiel für Dokumentation
 - ◆ Beispiel für Durchführung
- **Risikoanalyse gemäß 200-3**
 - ◆ Die elementaren Gefährdungen sowie andere Gefährdungsübersichten
 - ◆ Vorgehen bei der Risikobewertung und Risikobehandlung

- ◆ Beispiel für Risikobewertung

- **Umsetzungsplan**

- ◆ Maßnahmenplan entwickeln und dokumentieren
- ◆ Umsetzungsreihenfolge und Verantwortlichkeit bestimmen
- ◆ Begleitende Maßnahmen planen
- ◆ Aufwände schätzen

- **Aufrechterhaltung und kontinuierliche Verbesserung**

- ◆ Leitfragen für die Überprüfung
- ◆ Überprüfungsverfahren
- ◆ Kennzahlen
- ◆ Reifegradmodelle

- **Zertifizierung und Erwerb des IT-Grundschutz-Zertifikates auf Basis von ISO-27001**

- ◆ Arten von Audits z.B. Prozess und Produkt Audit
- ◆ Grundsätze der Auditierung 1st, 2nd, 3rdParty Auditoren
- ◆ Modell der Akkreditierung und Zertifizierung
- ◆ Ablauf des BSI-Zertifizierungsprozesses
- ◆ Tools und Hilfsmittel zur Umsetzung eines ISMS

- **IT-Grundschutz-Profile**

- ◆ Aufbau und Erstellung eines Profils
- ◆ Anwendung bzw. Nutzungsmöglichkeit veröffentlichter Profile

- **Vorbereitung eines Audits**

- ◆ Planung und Vorbereitung
 - ◇ Rollen, Verantwortlichkeiten, Unabhängigkeiten, Auditplan, Checklisten, Kombination von Audits, Synergieeffekte
- ◆ Auditprozess-Aktivitäten
 - ◇ Zusammenstellung eines Teams, Vorbereitung der Dokumente, Planung des Vor-Ort-Audits, Umgang mit Nichtkonformitäten
- ◆ Berichtswesen
 - ◇ Inhalt und Aufbau, Genehmigung und Verteilung, Aufbewahrung und Vertraulichkeit
- ◆ Folgemaßnahmen
 - ◇ Vor-Audit, Wiederholungsaudit, Überwachung, Korrekturmaßnahmen

- **Notfallmanagement**

- ◆ Überblick über den BSI-Standard 100-4
- ◆ Notfallmanagement-Prozess
 - ◇ initiieren, analysieren, einführen, üben, verbessern
- ◆ Business-Impact-Analyse (BIA)
- ◆ Notfälle bewältigen (Umgang mit Sicherheitsvorfällen)
- ◆ Vorgehensweise bei Sicherheitsvorfall und Meldeweg erarbeiten

- **Zusammenfassung und Vorbereitung auf die Prüfung**

- **Insgesamt erhalten Sie mit diesem Lehrgang 19 Theorie-Einheiten und 5 Praxis-Einheiten**