Bundesamt
für Sicherheit in der
Informationstechnik

Curriculum

zum Schulungskonzept IT-Grundschutz-Praktiker und IT-Grundschutz-Berater

Version 1.1 vom 24.09.2024

Legende/Erklärung

Die nachfolgende Tabelle gibt eine Übersicht über die für den IT-Grundschützer erforderlichen Themenfelder und Lerninhalte.

In den rechten Spalten wird je nach Qualifikation zwischen den folgenden Vertiefungsstufen unterschieden:

I : „Kenntnisse, die verstanden sind und erläutert werden können“ (Reproduktion)

II : „Kenntnisse und Fertigkeiten, die auf eigene Prozesse und Komponenten angewendet und umgesetzt werden können“ (Transfer)

III: „Analysen und Methoden, die auf andere Institutionen, Prozesse und Komponenten angewendet und bewertet werden können“ (Reflexion)

Jede theoretische Unterrichtseinheit (UE) sollte min. 1/3 Praxisanteil enthalten.

Das Verhältnis von theoretischen und praktischen Anteil soll bei der IT-Grundschutz-Basisschulung (-Praktiker) 50%-50% betragen.

Das Verhältnis von theoretischem und praktischen Anteil soll bei der IT-Grundschutz-Aufbauschulung (-Berater) 25%-75% betragen.

Eine UE (Unterrichtseinheit) entspricht einer Zeitstunde ohne Pausen.

Nr.	Themenfelder und Lerninhalte	IT-GS-Praktiker Gewichtung in UE	Vertiefungs-grad	IT-GS-Berater Gewichtung in UE	Vertiefungs-grad
1	Einführung und Grundlagen der Informationssicherheit und rechtliche Rahmenbedingungen	2	I + II	0	/
	Begriffe (Arten und Wichtigkeit von Informationen, Aspekte der Integrität, Verfügbarkeit, Vertraulichkeit usw.)				
	Unterschied zwischen IT und OT sowie Security und Safety				
	Gesetzliche Grundlagen (BSIG, IT-SiG usw.)				
2	Normen und Standards der Informationssicherheit	2	I	2	II + III
	Evaluation von relevanten Normen				
	Synergieeffekte herausstellen				
	integrierte Managementsysteme, VSA, C5, HV-Benchmark				
	Überblick, Zweck und Struktur über relevante Normen und Richtlinien z. B. ISO 2700x usw.)				
	Cobit, ITIL usw.				
	IT-Grundschutz-Kompendium				
	Branchenspezifische Sicherheitsstandards und IT-Grundschutz-Profile				
3	Einführung IT-Grundschutz	2	II	0	/
	IT-Grundschutz – Bestandteile				
	Sicherheitsprozess				
	Rollen, Verantwortung und Aufgaben (Institutionsleitung, Informationssicherheitsbeauftragte, ICS-Informationssicherheitsbeauftragte, Information-Management-Team usw.)				
	Sicherheitskonzept				
	Leitlinie erstellen				
4	IT-Grundschutz-Vorgehensweise (Überblick)	1	I + II	2	III

Nr.	Themenfelder und Lerninhalte	IT-GS-Praktiker Gewichtung in UE	Vertiefungs-grad	IT-GS-Berater Gewichtung in UE	Vertiefungs-grad
	Leitfragen zur IT-Grundschutz-Absicherung				
	Basis-Anforderungen				
	Standard-Anforderungen				
	Anforderungen für den erhöhten Schutzbedarf				
	Wahl der Vorgehensweise am Praxisbeispiel	1			
5	Kompendium (Überblick)	1	I + II	2	I + II
	Aufbau und Anwendung des Kompendiums				
	ISMS				
	Prozess-Bausteine				
	System-Bausteine				
	Umsetzungshinweise				
	Erstellung eines Bausteins				
6	Umsetzung der IT-Grundschutz-Vorgehensweise	1	II	0	/
	Netzplan erstellen				
	Geschäftsprozess und zugehörige Anwendungen sowie IT-Systeme, Räume erfassen				
	Schutzbedarfskategorien, Vorgehen und Vererbung				
	Modellierung gemäß IT-Grundschutz (Vorgehen, Dokumentation, Anforderungen anpassen)				
7	IT-Grundschutz-Check	1	II	0	/
	Was wird geprüft?				
	Vorbereitung und Durchführung				
	IT-Grundschutz-Check dokumentieren				
	Entscheidungskriterien				
	Beispiel für die Dokumentation	1			
	Beispiel für die Durchführung	1			
8	Risikoanalyse	1	II	1	II
	Die elementaren Gefährdungen sowie andere Gefährdungsübersichten				

Nr.	Themenfelder und Lerninhalte	IT-GS-Praktiker Gewichtung in UE	Vertiefungs-grad	IT-GS-Berater Gewichtung in UE	Vertiefungs-grad
	Vorgehen bei der Risikobewertung und Risikobehandlung				
	Beispiel für die Risikobewertung	1			
9	Umsetzungsplanung	1	II	0	/
	Maßnahmenplan entwickeln und dokumentieren, Aufwand schätzen, Umsetzungsreihenfolge und Verantwortlichkeit bestimmen, begleitende Maßnahmen planen				
	Aufwände schätzen				
10	Aufrechterhaltung und kontinuierliche Verbesserung	1	II	1	II
	Leitfragen für die Überprüfung				
	Überprüfungsverfahren				
	Kennzahlen				
	Reifegradmodelle				
	Beispiel für Anwendung kontinuierlicher Verbesserungsprozess (KVP)				
11	Zertifizierung und Erwerb des IT-Grundschutz-Zertifikats auf Basis von ISO-27001	1	I	0	/
	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				
12	IT-Grundschutz-Profile	1	I + II	2	I + III
	Aufbau eines IT-Grundschutz-Profils				
	Nutzung/Erstellung eines IT-Grundschutz-Profils				
	Anwendung bzw. Nutzungsmöglichkeit veröffentlichter Profile				
13	Vorbereitung auf ein Audit	1	II	2	II + III

Nr.	Themenfelder und Lerninhalte	IT-GS-Praktiker Gewichtung in UE	Vertiefungs-grad	IT-GS-Berater Gewichtung in UE	Vertiefungs-grad
	Planung und Vorbereitung auf ein Audit (Rollen und Verantwortlichkeiten, Unabhängigkeit, Auditplan, Checklisten, Kombination von Audits, Synergieeffekte) Audit-prep/defens				
	Auditprozess-Aktivitäten (Zusammenstellung eines Teams, Dokumente vorbereiten, Planung des Vor-Ort-Audits, Umgang mit Nichtkonformitäten)				
	Berichtswesen (Inhalt und Aufbau eines Berichtes, Genehmigung und Verteilung, Aufbewahrung und Vertraulichkeit)				
	Folgemaßnahmen (Vor-Audit, Wiederholungsaudit, Überwachung, Korrekturmaßnahmen)				
	Qualifikation von Auditoren (Berufserfahrung, Schulung, persönliche Eigenschaften, Aufrechterhaltung der Qualifikation)				
14	Sicherheitsvorfallbehandung Management	2	II	2	III
15	BCM Prozess	2	I	2	II
	Überblick über den BSI-Standard 200-4				
	Überblick über den BCM-Prozess, in Anlehnung an das IT-Grundschutz-Kompendium, insbesondere DER.4 Notfallmanagement.				
	Summe der UE (ohne Pausen)	**24**		**16**	

Tabelle 1: Curriculum Schulungskonzept