Bundesamt
für Sicherheit in der
Informationstechnik

Curriculum

für die Basisschulung für den IT-Grundschutz-Praktiker und die Aufbauschulung für den IT-Grundschutz-Berater

Legende/Erklärung

Die 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.
Unterrichtseinheiten die eine umfangreiche praktische Auseinandersetzung vorsehen, sind mit grau hinterlegt gekennzeichnet.
Das Verhältnis von theoretischem und praktischen Anteil soll bei der GS-Basisschulung 50%-50% betragen.
Das Verhältnis von theoretischem und praktischen Anteil soll bei der GS-Aufbauschulung 25%-75% betragen.

Nr.	Themenfelder und Lerninhalte	IT-GS-Basisschulung für den IT-GS-Praktiker (gesamt 24 UE)		IT-GS-Aufbauschulung für den IT-GS-Berater (gesamt 16 UE)	
		(gesamt 24 UE)	Unterrichts-einheiten	(gesamt 16 UE)	Unterrichts-einheiten
1	Einführung und Grundlagen der IT-Sicherheit und rechtliche Rahmenbedingungen	I+II	2		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	I	2	II+III	1
	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	II	2		0
	IT-Grundschutz – Bestandteile				
	Sicherheitsprozess				
	Rollen, Verantwortung und Aufgaben (Leitung, Informationssicherheitsbeauftragte, ICS-Informationssicherheitsbeauftragte, Information-Management-Team usw.)				
	Sicherheitskonzept				
	Leitlinie erstellen				
4	IT-Grundschutz-Vorgehensweise (Überblick)	I+II	1	III	1
	Leitfragen zur IT-Grundschutz-Absicherung				
	Basis-Anforderungen				
	Standard-Anforderungen				
	Anforderungen für den erhöhten Schutzbedarf				
	Wahl der Vorgehensweise am Praxisbeispiel		1		1
5	Kompendium (Überblick)	I+II	1		1
	Aufbau und Anwendung des Kompendiums				
	ISMS (Managementsystem für Informationssicherheit)				
	Prozess-Bausteine				
	System-Bausteine				
	Umsetzungshinweise				
	Erstellung eines Bausteins				1
6	Umsetzung der IT-Grundschutz-Vorgehensweise	II	1		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	II	1		0
	Was wird geprüft?				
	Vorbereitung und Durchführung				
	IT-Grundschutz-Check dokumentieren				
	Entscheidungskriterien				
	Beispiel für die Dokumentation		1		

	Beispiel für die Durchführung		1		1
8	Risikoanalyse	II	1		0
	Die elementaren Gefährdungen sowie andere Gefährdungsübersichten				
	Vorgehen bei der Risikobewertung und Risikobehandlung				
	Beispiel für die Risikobewertung		1		1
9	Umsetzungsplanung	II	1		0
	Maßnahmenplan entwickeln und dokumentieren, Aufwand schätzen, Umsetzungsreihenfolge und Verantwortlichkeit bestimmen, begleitende Maßnahmen planen				
	Aufwände schätzen				
10	Aufrechterhaltung und kontinuierliche Verbesserung	II	1		0
	Leitfragen für die Überprüfung				
	Überprüfungsverfahren				
	Kennzahlen				
	Reifegradmodelle				
	Beispiel für Anwendung kontinuierlicher Verbesserungsprozess (KVP)				1
11	Zertifizierung und Erwerb des IT-Grundschutz-Zertifikats auf Basis von ISO-27001	I	1		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	I+II	1	I+III	2
	Aufbau eine Profils				
	Erstellung eines Profils				
	Anwendung bzw. Nutzungsmöglichkeit veröffentlichter Profile				
13	Vorbereitung auf ein Audit	II	1	II+III	2
	Planung und Vorbereitung (Rollen und Verantwortlichkeiten, Unabhängigkeit, Auditplan, Checklisten, Kombination von Audits, Synergieeffekte)				
	Auditprozess-Aktivitäten (Zusammenstellung eines Team, 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	Notfallmanagement Prozess (initiieren, analysieren, einführen, üben, verbessern)	II	2	II+III	2
	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		1		1
	Zusammenfassung und Vorbereitung auf die Prüfung	I	1	I	1