

## Zertifizierungsordnung für das Seminar IT-Grundschutz-Manager

### A) Gegenstand

#### (was legt die Ordnung fest)

Diese Zertifizierungsordnung gilt für die Weiterbildung mittels dem Seminar IT-Grundschutz-Manager.

Sie bestimmt die Soll-Definition des Qualifikationsniveaus, Regelungen der Prüfung des Nachweises durch die Teilnehmer und der Bestätigung durch ein Personenzertifikat.

### B) Qualifikationsniveau

#### (welche Qualifikation soll erreicht werden)

Inhaltliches Verständnis der BSI-Standards bzw. Vorgehensweisen zu IT-Grundschutz auf Entscheider-Niveau, d.h. um diese beurteilen zu können und/oder Entscheidungen hierzu treffen und/oder vorbereiten zu können. Dies betrifft die BSI-IT-Grundschutz-Standards 200-1, 200-2, 200-3, 100-4 umfassend, jedoch kompaktifiziert mit Themen und Kompetenzen mit einem zugehörigen Lehrumfang von 12 Kalenderstunden. Die Themenbereiche sind:

#### **Grundlagen:**

Begriffe und Motivation / Nutzen der Informationssicherheit (Schutz, Rechtskonformität, ...); rechtliche Rahmenbedingungen (IT-Sicherheitsgesetz, BSI-Kritisverordnung, ...); Ziele / Anforderungen (Vertraulichkeit, Integrität, Verfügbarkeit, ...); Schutzbedarfsfeststellung und Informationssicherheitsniveau; Informationssicherheits-Management mit Bedeutung, Prinzip, Lebenszyklus, Informationssicherheits-Managementsystem und Realisierung via IT-Grundschutz

#### **BSI-Standard 200-1 Managementsysteme für Informationssicherheit**

Motivation; Übersicht; Sicherheitsprozess (Motivation, Lebenszyklus, Ermittlung von Rahmenbedingungen, Identifikation und Festlegung allgemeiner Sicherheitsziele, Erarbeitung einer Sicherheitsstrategie, ...); Sicherheitskonzept (Auswahl einer Methode zur Risikoanalyse, Erstellung eines qualitativen Klassifikationsschemas, Durchführung der Risikoanalyse, ...); Management-Prinzipien (Motivation und Aufgaben der Leitungsebene, Kommunikation und Wissen, Erfolgskontrolle im Sicherheitsprozess, ...); Ressourcen und Mitarbeiter für Informationssicherheit

#### **BSI-Standard 200-2 IT-Grundschutz-Methodik**

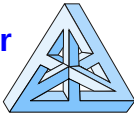
Motivation und Übersicht (Vorgehen, Managementsystem, Verantwortung, ...), Sicherheitsprozess Initiierung (Übernahme der Verantwortung durch die Leitungsebene, Konzeption und Planung des Sicherheitsprozesses, ...), Organisation (Aufbau, Grundregeln, Informationssicherheitsbeauftragter, ...), Dokumentation (Klassifikation von Informationen, Informationsfluss) und Aufrechterhaltung und Verbesserung (Überprüfung des Prozesses, der Strategie, ...), Sicherheitskonzeption Erstellung (Basis-, Kern-, Standard-Absicherung) und Umsetzung (Sichtung der Ergebnisse, Kosten- und Aufwandsschätzung, ...), Zertifizierung

#### **BSI-Standard 200-3 Risikoanalyse auf der Basis von IT-Grundschutz**

Motivation und Übersicht, Gefährdungsermittlung, Risikoeinstufung (mit Risikomatrix und -kategorien), Risikobehandlung (Vermeidung, Reduktion, Transfer, Akzeptanz, Beobachtung), Konsolidierung und Rückführung in den Sicherheitsprozess

#### **BSI-Standard 100-4 Notfallmanagement**

Motivation und Begriffe; Notfallmanagement-Prozess Übersicht (Initiierung, Konzeption, ...), Initiierung (Leitungsebene übernimmt die Verantwortung, Notfallmanagement-Prozess konzipieren und planen, Notfall-Organisation definieren, ...), Notfallvorsorgekonzept Konzeption (Business



Impact Analyse durchführen, Risikoanalyse durchführen, IST-Zustand erfassen, ...) und Umsetzung (Kosten- und Aufwandschätzung, Festlegung der Umsetzungsreihenfolge, ...); Notfallbewältigung und Krisenmanagement (Ablauforganisation Phasen, Meldung/Alarmierung/Eskalation, Krisenstab, Notfallhandbuch...), Tests und Übungen inklusive Rollen und Dokumentation; Aufrechterhaltung und Verbesserung (Überwachung, Überprüfung, Aktualisierung, ...)

## C) Prüfungsregelungen

### (wie wird gemessen, ob Teilnehmer das Qualifikationsniveau haben)

#### **Gegenstand**

In einer Prüfung wird festgestellt, ob der Teilnehmer das Qualifikationsniveau erfüllt.

#### **Anmeldung**

Die Anmeldung erfolgt automatisch zusammen mit der Anmeldung zum Seminar.

#### **Rücktritt**

Will ein Teilnehmer an der Prüfung nicht teilnehmen, so hat er dies vor Beginn des Seminars, spätestens am Anfang des Seminars, dem Seminarleiter mitzuteilen. In diesem Fall gilt die Prüfung als nicht durchgeführt und verzichtet der Teilnehmer auf die Prüfung ersatzlos.

Tritt ein Teilnehmer nach Beginn des Seminars aufgrund gravierender, vom Teilnehmern nicht zu vertretender Gründe zurück wie Krankheit oder Höhere Gewalt, so gilt die Prüfung als nicht durchgeführt und verzichtet der Teilnehmer auf die Prüfung ersatzlos. Die Gründe sind dem Seminarleiter unverzüglich mitzuteilen, bei Bedarf auch nachzuweisen.

Tritt ein Teilnehmer ansonsten nach Beginn des Seminars zurück, so gilt die Prüfung als nicht bestanden.

#### **Identitätsnachweis**

Der Teilnehmer muss sich vor Seminarbeginn mit einem gültigen Lichtbildausweis ausweisen.

#### **Termin, Ort, Form, Dauer, Sprache**

Die Prüfung erfolgt in den Seminarablauf integriert, Termin und Ort ergeben sich entsprechend.

Es werden Prüfungsfragen zu den Themenfeldern während dem Seminar gestellt.

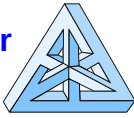
Dazu werden in der Regel je Seminarteil Fragebögen ausgeteilt und von jedem Teilnehmer eigenständig, ohne Hilfsmittel und schriftlich in kurzer Zeit von 5 Minuten beantwortet, dann sofort an den Seminarleiter zurückgegeben.

Die Prüfung erfolgt in deutscher Sprache.

#### **Online-Prüfung:**

Eine Prüfung ist online möglich. Zur geeigneten Beaufsichtigung hat der Teilnehmer das von der DresPleier GmbH eingesetzte Videokonferenz-System zu nutzen und die Übertragung von Bild (Video mit sichtbarem Teilnehmer) und Ton (Audio) zu aktivieren. Das Equipment des Teilnehmers muss dies ermöglichen.

Ablauf: Die Prüfungsfragen bekommt der Teilnehmer per Mail zugesendet im Open Document Format (ODT für Textdokumente). Er beantwortet die Fragen direkt im Dokument durch Ankreuzen. Zum Ende jedes Teils speichert er das Dokument als PDF ab und sendet es sofort per Mail als PDF an den Prüfer zurück. Zusenden, PDF-Speichern und Zurücksenden erfolgen außerhalb der Prüfungszeit. Ein Austreten während der Prüfung ist nur zeitlich begrenzt (wenige Minuten) gestattet. Bei gravierenden technischen Störungen wird die Prüfung abgebrochen und kostenlos wiederholt.



### **Fragen, Bewertung**

Zu den Themenfeldern ist ein Fragenpool erstellt mit 80 Fragen, die alle Themenfelder abdecken und mit Ja oder Nein zu beantworten sind.

Zur Prüfung werden daraus per Zufall 50 Fragen ausgewählt, die alle Themenfelder abdecken.

Zum Bestehen der Prüfung müssen 50%, also 25 Fragen korrekt beantwortet sein (jede korrekt beantwortete Frage wird gewertet, jede nicht korrekt beantwortete nicht).

### **Hilfsmittel**

Der Prüfling darf zur Beantwortung der Fragen keinerlei Hilfsmittel benutzen, sondern muss diese eigenständig beantworten.

### **Betrug, Störung**

Im Falle eines Betrugs dokumentiert der Seminarleiter dies und entscheidet je nach Bedeutung des Vorfalls über eine Verwarnung oder den Ausschluss aus der Prüfung. Bei einem Ausschluss gilt die Prüfung als nicht bestanden. Werden Verstöße nach der Prüfung festgestellt, so kann ein ausgestelltes Personenzertifikat widerrufen werden.

Stört ein Teilnehmer die Prüfung, so kann er vom Seminar bzw. der Prüfung ersatzlos ausgeschlossen werden. Die Prüfung gilt dann als nicht bestanden.

### **Einsicht, Wiederholung**

Ist die Prüfung nicht bestanden, so kann der Teilnehmer auf Antrag eine Prüfungseinsicht nach Abstimmung mit der DresPleier GmbH vornehmen. Anfallende Kosten hat der Teilnehmer zu erstatten.

Eine nicht bestandene Prüfung kann wiederholt werden.

Dazu ist eine individuell zu vereinbarende Prüfung mit entsprechenden Kosten zu vereinbaren. Die vorbereitende Buchung einer Prüfungsvorbereitung oder eines Seminars ist empfohlen.

## **D) Zertifikat**

**(wie wird das Qualifikationsniveau bestätigt)**

### **Ausstellung**

Die Fragebögen werden nach dem Seminar zeitnah ausgewertet.

Bei einer erfolgreichen Prüfung wird dem Teilnehmer ein Personenzertifikat als Bestätigung mit der Post zugesendet. Ansonsten wird der Teilnehmer über das Nichtbestehen informiert.

### **Inhalte**

Das Personenzertifikat enthält:

- Familienname, Vorname(n), ggfls. Titel, Geburtsdatum
- Seminartitel
- Qualifikationsniveau
- Prüfungsdatum und Prädikat "mit Erfolg bestanden"
- Aussteller und Ausstellungsdatum
- Nummer des Personenzertifikats
- Gültigkeitsdauer des Zertifikats

### **Verwendung**

Das Personenzertifikat darf nur in der ausgestellten Form verwendet werden.

Es darf nicht verändert, in Teilen oder in täuschender Absicht genutzt werden.

Im Falle von Missbrauch kann das Personenzertifikat nachträglich widerrufen werden.



### **Dauer, Rezertifizierung**

Das Personenzertifikat hat eine zeitlich begrenzte Gültigkeit, da es die Aktualität einer Qualifikation bestätigt.

Das Personenzertifikat hat eine Gültigkeit von 5 Jahren ab dem Zeitpunkt der Prüfung.

Eine Rezertifizierung ist durch erneute Teilnahme mit Prüfung und Personenzertifikat in einem dann aktuell angebotenen Seminar mit extra Anmeldung und Kosten möglich.

### **Widerruf**

Wird ein Personenzertifikat vom Aussteller widerrufen, so ist dies vom Zertifikatsinhaber unverzüglich auf dessen Kosten an den Aussteller im Original per Post zuzusenden und darf dieses vom Zertifikatsinhaber nicht weiter verwendet werden.

## **E) Sonstiges**

### **(was ist zudem relevant)**

#### **Aufbewahrungsfrist**

Prüfungsunterlagen werden 1 Jahr lang aufbewahrt, Informationen zum Zertifikat für die Gültigkeitsdauer des Zertifikats von 5 Jahren.

#### **Inkrafttreten**

Die Zertifizierungsordnung tritt am 21.09.2020 in Kraft und ersetzt alle früheren Zertifizierungsordnungen.

Die Geschäftsführung