

SC550 BSI IT-Grundschutz-Praktiker

Kurzbeschreibung:	Ziele:																
<p><u>Diese Ausbildung vermittelt Ihnen:</u></p> <ul style="list-style-type: none"> - Fachbegriffe aus dem Bereich der Informationssicherheit - Erforderliches Fachwissen für Planung, Aufbau und Betrieb sowie die Aufrechterhaltung und Verbesserung eines ISMS gemäß BSI-Grundschutz bis hin zur Zertifizierungsreife <p>Nach dem Training sind Sie in der Lage, die Leitung Ihrer Organisation in folgenden Punkten zu unterstützen:</p> <ul style="list-style-type: none"> - Sicherstellung eines angemessenen Informationssicherheitsniveaus - Bestimmung der Maßnahmen für Ihr Sicherheitskonzept - Identifizierung des spezifischen Schutzbedarfes Ihrer Informationen, Anwendungen und Ihrer IT-Systeme - Am vierten Kurstag findet die Prüfung zum BSI IT-Grundschutz-Praktiker statt. Prüfungsdauer: 60 Minuten <p>Prüfungsinhalt: 50 Multiple-Choice-Fragen</p> <p>Die Prüfung ist bestanden wenn 60% aller Fragen richtig beantwortet werden.</p>	<ul style="list-style-type: none"> - Sie lernen, wie Sie ein Informationssicherheitssystem bzw. ein komplettes IT-Sicherheitssystem gemäß BSI IT-Grundschutz in der eigenen Organisation implementieren und managen. - Sie kennen das Fachvokabular und sind in der Lage, die kritischen Informationen Ihres Unternehmens durch die Einführung eines ISMS zu schützen. - Am vierten Kurstag findet eine Prüfung statt anhand deren Sie Ihre Fachkenntnisse und Kompetenzen nachweisen. Bei Bestehen der Prüfung erhalten Sie ein Zertifikat mit dem Titel: "BSI IT-Grundschutz-Praktiker" <p>Der Gesamtpreis des Trainings beinhaltet die Prüfung zum IT-Grundschutz Praktiker.</p>																
Zielgruppe:	Termine																
<ul style="list-style-type: none"> - 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 	<p>Dieser Workshop findet an folgenden Terminen statt: Am ersten Tag ist Kursbeginn um 10:00 Uhr und der Kurs endet am letzten Tag um ca. 16:00.</p> <table border="1" style="width: 100%; text-align: center;"> <thead> <tr> <th style="width: 15%;">Ort</th> <th style="width: 15%;"></th> <th style="width: 20%;">Beginn</th> <th style="width: 20%;">Ende</th> </tr> </thead> <tbody> <tr style="background-color: #e0e0e0;"> <td>Virtuell</td> <td> Virtuell Karte</td> <td>30.06.2020</td> <td>03.07.2020</td> </tr> <tr style="background-color: #e0e0e0;"> <td>Nürnberg</td> <td> Nürnberg Karte</td> <td>07.09.2020</td> <td>10.09.2020</td> </tr> <tr style="background-color: #e0e0e0;"> <td>Nürnberg</td> <td> Nürnberg Karte</td> <td>30.11.2020</td> <td>03.12.2020</td> </tr> </tbody> </table>	Ort		Beginn	Ende	Virtuell	 Virtuell Karte	30.06.2020	03.07.2020	Nürnberg	 Nürnberg Karte	07.09.2020	10.09.2020	Nürnberg	 Nürnberg Karte	30.11.2020	03.12.2020
Ort		Beginn	Ende														
Virtuell	 Virtuell Karte	30.06.2020	03.07.2020														
Nürnberg	 Nürnberg Karte	07.09.2020	10.09.2020														
Nürnberg	 Nürnberg Karte	30.11.2020	03.12.2020														

Voraussetzungen:

Grundkenntnisse in der IT-Sicherheit bzw.
Informationssicherheit

Sonstiges:

Dauer: 4 Tage

Preis: 2450 Euro plus MwSt.

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-Kompendium
 - ◆ 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-Kompendium: 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
- **Kompendium (Überblick)**
 - ◆ Aufbau und Anwendung des Kompendiums
 - ◆ 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**

Empfänger:
qSkills GmbH & Co. KG
Südwestpark 65
90449 Nürnberg
eMail: info@qskills.de
Fax: +49 (0)911-80103-39



Absender:

Firma: _____
Strasse: _____
PLZ/Ort: _____

Anmeldung zum Workshop SC550 BSI IT-Grundschutz-Praktiker

Termin: Von _____ bis _____
Dauer: 4 Tage
Preis: 2450 EUR + MWST. pro Teilnehmer

Teilnehmer 1: Name: _____ Vorname: _____
Abteilung: _____
Telefon: _____ Mobil: _____
Telefax: _____
eMail: _____
eMail2: _____

Teilnehmer 2: Name: _____ Vorname: _____
Abteilung: _____
Telefon: _____ Mobil: _____
Telefax: _____
eMail: _____
eMail2: _____

Hotelwunsch: Bitte zutreffendes Ankreuzen: [] Ja | [] Nein

An- Abreise Teilnehmer 1: Von _____ bis _____

An- Abreise Teilnehmer 2: Von _____ bis _____

Rechnungsanschrift: Firma: _____
Ansprechpartner: _____
Abteilung: _____
Strasse: _____
Ort: _____

Hiermit bestätige ich die verbindliche Anmeldung zu o.g. Workshop. Ich besitze die notwendigen Vorkenntnisse.
Es gelten die AGB der qSkills GmbH & Co. KG

Ort, Datum _____ Unterschrift _____