

Information

Ort und Hotel

Arcotel Camino, Tel.: 0711/25858-0
Günnewig Hotel Stadtpalais, Tel.: 0221/88042-0
Hilton Bonn, Tel.: 0228/7269-0

ComConsult hat in ausgesuchten Hotels ein Zimmerkontingent für Sie vorgebucht, nutzen Sie unsere Vorzugspreise. Das Seminar beginnt am ersten Tag um 10:00 Uhr und endet am letzten Tag um 15:00 Uhr.

Kosten und Leistungen

Der Preis beinhaltet neben der Teilnahmegebühr die Veranstaltungsunterlagen, ein Teilnehmerzertifikat, Getränke und Mittagsmenues an allen Tagen sowie die „Happy Hour“ am ersten Veranstaltungstag, zu der alle Teilnehmer herzlich eingeladen sind.

Die Unterlagen enthalten das gesamte Arbeitsmaterial der Veranstaltung und bieten dem Teilnehmer zahlreiche wichtige Informationen für die zukünftige berufliche Praxis.

Seminarbedingungen

Bis zu 14 Tagen vor Seminarbeginn behält sich der Veranstalter das Recht vor, das Seminar zu stornieren. Schriftliche Absagen von Teilnehmern sind bis 15 Tage vor Veranstaltungsbeginn kostenlos möglich, ab dem 14. Tag vor Veranstaltungsbeginn sind 50 % des Teilnahmebetrages zu zahlen. Bei Nichterscheinen oder Stornierung am Veranstaltungstag wird der gesamte Teilnahmebetrag fällig; der Teilnehmer erhält nach Ablauf der Veranstaltung die kompletten Schulungsunterlagen per Post. Die Übertragbarkeit auf andere Mitarbeiter ist möglich. Bitte informieren Sie uns. Die Seminargebühr ist im Voraus zu entrichten. Der Veranstalter behält sich Änderungen im Programm vor.

Der Veranstalter

Die ComConsult Akademie ist einer der führenden deutschen Anbieter für herstellerneutrale Netzwerk Seminare. Unter Federführung des anerkannten Kommunikationsspezialisten Dr. Jürgen Suppan sind Aktualität und praktische Umsetzbarkeit der Information stets gewährleistet.

Die Referenten

Dipl.-Inform. Oliver Flüs, Dr. Simon Hoff

**Fax-Antwort: 02408/955-399
02408/955-398**

Anmeldung

Sicherheitsmanagement mit BSI-Grundschutzmethodik/ ISO 27001

Ich melde mich verbindlich für das Seminar zum Preis von 1.890,- € zzgl. MwSt. für folgenden Termin an:

- 26.03. - 28.03.12 in Stuttgart**
- 04.06. - 06.06.12 in Köln**
- 12.11. - 14.11.12 in Bonn**

Ich benötige keine Hotelreservierung

Bitte buchen Sie für mich ein Zimmer

vom _____ bis _____

Vorname, Nachname

Firma

Abteilung

Straße

PLZ, Ort

Telefon, Fax

eMail

Ich habe die Seminarbedingungen zur Kenntnis genommen.

Unterschrift

ComConsult Akademie
Pascalstraße 25 • 52076 Aachen
Tel. 02408/955-300 • Fax 955-399
mail@comconsult-akademie.com
www.comconsult-akademie.de

Sicherheitsmanagement mit BSI-Grundschutzmethodik/ ISO 27001

Seminar



26.03. - 28.03.12 in Stuttgart

04.06. - 06.06.12 in Köln

12.11. - 14.11.12 in Bonn

**ComConsult
Akademie**

Sicherheitsmanagement mit BSI-Grundschutzmethodik/ ISO 27001

Motivation

Informationssicherheit ist heutzutage ein Muss, sei es aus rechtlichen oder wettbewerbstechnischen Gründen. Den vielfältigen „Compliance“-Ansprüchen gesellt sich der Aspekt einer Konformität zu BSI-Methodik bzw. ISO 27001 hinzu und die Anforderung, sich an den zugehörigen Kontrollfragen und Maßnahmenkatalogen erfolgreich messen zu können. Längst sind ISO 27001 und BSI-IT-Grundschutz nicht mehr nur eine Möglichkeit, sich „werb wirksam“ zertifizieren zu lassen. Vielfach liefert ihre Anwendung die erwartete plausible Antwort auf die Frage nach Erreichung eines „best-practice“-Mindest-Sicherheitsniveaus oder nach angemessenem (!) Sicherheitsaufwand bei erhöhtem Sicherheitsbedarf. So nützlich diese Hilfestellung bei Aufbau und Aufrechterhaltung der nötigen Sicherheit sind, so sehr kann bei mangels Erfahrung „ungeschickter“ Anwendung ein enormer, vermeidbarer Arbeitsaufwand entstehen.

In diesem Seminar lernen Sie

- die Methodik der BSI-Standards 100-1 - 100-3 anzuwenden
- die Rolle eines Sicherheitsbeauftragten bzw. eines Sicherheitsmanagement-Teams mit Leben zu füllen • wie man auf dieser Basis ein Sicherheitsmanagement aufbaut
- wie man mit Hilfe der BSI-Methodik und der Grundschutzkataloge das erreichte Sicherheitsniveau bewertet und ggf. optimiert
- wie die Methodik in Fällen funktioniert, in denen die Grundschutzkataloge nicht ausreichen
- wie die IT-Grundschutzmethodik mit ITIL, internem Qualitätsmanagement u.Ä. harmonisch kombinierbar ist
- wie Baustein „Datenschutz“ und Standard 100-4 Notfallmanagement die Grundschutzkataloge abrunden
- wie und wo Werkzeuge (GSTOOL, Verinice u.Ä.) unterstützen können
- neue IT-Lösungen sicherheitstechnisch mittels Grundschutzmethodik konzipiert und in den Betrieb eingeführt werden können.

Der Inhalt

ISMS als Teil eines bewussten Risikomanagement

- Beispiele für Risikomanagement-Systeme und -auflagen
- Typische Elemente eines bewussten Risikomanagements
- Bedienung dieser Elemente durch ISO 27001 bzw. BSI-Standards • Analysephasen nach BSI-IT-Grundschutzmethodik • Change Management und Sicherheitsmanagement
- Sicherheitsmanagement benötigt einen „Prozess“: P-D-C-A-Modell nach ISO 27001 / BSI-Standard 100-2

Übergreifende Aspekte des Sicherheitsmanagements

- Grundwerte der Sicherheit, Sicherheitsziele
- Sicherheit durch Gesamtpakete aus technischen und organisatorischen Maßnahmen
- ohne Rückendeckung „von oben“ funktioniert Sicherheit nicht
- abgestimmte Gesamtpakete nur durch „Organisation“ des Sicherheitsmanagement • vom Management bis zum IT-Nutzer: jeder muss mitwirken - aber wie?

ISO-Standards und BSI-Methodik als Anleitung

- Verhältnis von ISO 27001 und BSI-Standards zueinander
- ITIL als Gestaltungshilfe einsetzen - ohne unnötige Blindleistung, weil abgestimmt • ISO 27001 und BSI-GS-Kataloge, Schicht 1 „übergreifende Aspekte“ • Ausblick auf Themenschwerpunkt Notfallmanagement (BSI-Standard 100-4)

Übergreifendes: typische Referenzdokumente mit Sicherheitsrelevanz

- Dokumentensystem zum ISMS - konform zu BSI-Bausteinen, praktikabler Aufwand • Explizite Forderungen gemäß Bausteinen „Sicherheitsmanagement“ und „Organisation“
- Details zur Organisation des Sicherheitsmanagement gemäß BSI-Standards • Aufgaben von Sicherheitsbeauftragtem und ggf. eines Sicherheitsmanagement-Teams
- Outsourcing im Sicherheitsmanagement?!
- Inhalte einer Sicherheitsleitlinie • Umsetzung im Alltag: Gesamtheit sicherheitsrelevanter Dokumentation

BSI-Grundschutzmethodik in der Praxis - Teil 1

- Systematische Darstellung der Methodik
- Ablauf der Analyse im Gesamtüberblick
- Anwendungsszenarien: ISMS für Gesamtumgebung vs. Sicherheitskonzept für bestimmten IT-Service in grundschutzkonformer Umgebung • Strukturanalyse, insbesondere: Abgrenzung, Objekte, Abhängigkeiten, bereinigter Netzplan
- Strukturanalyse: Hilfsmittel zur (Vor-)Erfassung, Tipps zur Objektbenennung • Netzplan: die Übersicht behalten, alltagstaugliche Gestaltung • Schutzbedarfsfeststellung: Vorgehensweise, Beteiligte und Hilfen zur Durchführung
- Schutzbedarfsfeststellung: „Vererbung“ im Sinne festgestellter Abhängigkeiten, Regeln • Modellierung, systematische Lagebestimmung mittels Grundschutz-Basis-Check
- Option Tooleinsatz zur Verringerung des Aufwands/ zur Erleichterung der Zielkontrolle und Überwachung notwendiger Anpassungsarbeiten (mit erster Demo)
- Ausblick auf ggf. notwendige Folgeschritte und deren Aufwand zur Bewältigung

Spezialthema: (Baustein) Datenschutz

- Vorstellung des Bausteins
- Hinweise zu im Umgang mit IT/ Informationssicherheit relevanten Aspekten in der Praxis
- Berücksichtigung formaler Detailanforderungen („Grundwerte des Datenschutzes“) z.B. gemäß Landesdatenschutz-Gesetzgebung bei Anwendung der Grundschutzmethodik

Spezialthema: Notfallmanagement/ Notfallvorsorge und Informationssicherheit

- Motivation, Situation im IT-Umfeld
- BSI-Standard 100-4: Einordnung, Abgrenzung, Begrifflichkeiten • Baustein Notfallvorsorgekonzept
- (Anforderungen an) Dokumentation zum Notfallmanagement • Details zur Organisation des Notfallmanagement gem. BSI-Standard
- Business Impact Analyse nach BSI-Standard 100-4 « ISMS
- weitere Aspekte/ Anregungen aus BSI-Standard 100-4
- Teilbeitrag zur Notfallvorsorge im IT-Bereich: Rollen (verteilung), Notfallprozess und deren Festschreibung in einem Notfallhandbuch IT
- Sicherheitsvorfälle mit (möglichem) Notfallcharakter: keine abweichende Organisation, sondern Behandlung als mögliche/ reduzierte Ausprägung zum Notfallprozess
- Notfallvorsorge: Notfallpläne, Ausweich- und Notbetriebsüberlegungen, Reserveteilhaltung, Supportverträge, usw. mit Praxistipps • Notfallübungen „mit Plan“
- Notfallvorsorge: fest im Change Management verankern

BSI-Grundschutzmethodik in der Praxis - Teil 2

- Ergänzende Sicherheitsanalyse - wann, durch wen und wie?
- Risikoanalyse nach BSI-Standard 100-3, Berücksichtigung von ISO 27005:2008 als Hinweisgeber • insbesondere: bewusste Risikübernahme und Risikotransfer als Optionen
- Hinweise/ Beispiele, insb.: Quellen für umgebungsspezifische Maßnahmenfindung für besondere Risiken/ Gefährdungen und erhöhten Schutzbedarf
- Dokumentation - für Entscheidungsfindung und Ergebnis
- Option Dokumentation per Tool

Zertifizierung(sverfahren) - Kurzeinführung

- Vorgesehener Ablauf gemäß BSI bzw. ISO
- Erfahrungen bzgl. Aufwand und Zeitrahmen für die Vorbereitung • Praxiserfahrung: worauf Auditoren insbesondere achten • Alternative bzw. vorbereitender Selbsttest: „interne“ Audits zur Standortbestimmung im Rahmen des eigenen Risiko- und Sicherheitsmanagement

(weitere) Praxisaspekte, Ausblick auf absehbare Ergänzungen der Grundschutzkataloge, u.Ä.