Ziel des Seminars

Der Schwerpunkt des Seminars liegt in der Vermittlung der Anforderungen aus der BAIT. Insbesondere werden die einzelnen Handlungsbereiche der BAIT vertiefend erläutert und die angemessene Umsetzung der resultierenden Maßnahmen aus den Handlungsbereichen aufgezeigt. Die umfangreichen Arbeitsunterlagen zum Seminar enthalten ein Musterkonzept für den Nachweis der Umsetzung der Maßnahmen aus den Handlungsbereichen der BAIT.

Voraussetzungen

Dieses Seminar richtet sich an Einsteiger, Fortgeschrittene und externe Dienstleister, die als relevante Stakeholder in die Umsetzung der BAIT involviert sind. Vorkenntnisse hinsichtlich bankenspezifischer Bedürfnisse sollten vorhanden sein. Darüber hinaus ist dieses Seminar ebenso für die relevanten Stakeholder für die Umsetzung der VAIT, KAIT und ZAIT geeignet.

Zielgruppe

- IT-Sicherheitsbeauftragte / CISO
- Verantwortliche in den Bereichen Datenschutz und Informationssicherheit
- Revisoren / IT-Revisoren
- Wirtschaftsprüfer im Bankenumfeld
- Mitarbeiter aus den Bereichen Informationstechnik (IT)
- Business Continuity Manager und Auslagerungsbeauftragte
- Compliance-Beauftragte

DGI®

Unseren **Seminarkatalog** sowie unsere **aktuellen Termine** finden Sie unter

www.DGI-AG.de

Gerne senden wir Ihnen **weiteres Informationsmaterial** zu.

Akademie der
DGI Deutsche Gesellschaft
für Informationssicherheit AG

Kurfürstendamm 57
D - 10707 Berlin

Telefon +49 30 31 51 73 89 - 10
Fax +49 30 31 51 73 89 - 20

E-Mail AKADEMIE@DGI-AG.de
Web www.DGI-AG.de

DGI®

Die Umsetzung der BAIT angemessen planen und konzipieren (DGI®)

AKADEMIE der DGI® Deutsche Gesellschaft für Informationssicherheit AG

Die Umsetzung der BAIT angemessen planen und konzipieren

Die nachweisliche **Umsetzung der BAIT** ist für Kreditinstitute und Finanzdienstleistungsinstitute sowie für deren IT-Dienstleister von **existenzieller Bedeutung**.

Die BAIT konkretisiert die aktuellen Einwirkungen auf einen sicheren IT-Betrieb und sieht **signifikante Verschärfungen** bei der **Sanktionierung** von Verstößen seitens der relevanten Unternehmen vor. Überdies muss davon ausgegangen werden, dass künftige Überprüfungen und Audits von aufsichtsrechtlicher Seite sowie von Wirtschaftsprüfern weniger Spielraum hinsichtlich der Reife der Maßnahmen für die Umsetzung der Anforderungen der BAIT zulassen.

Der **unternehmensspezifischen Umsetzung** von Maßnahmen für einen ordnungsgemäßen, sicheren und konformen Betrieb der IT muss vor diesem Hintergrund eine hohe Bedeutung beigemessen werden.

Eine dedizierte Auseinandersetzung mit der BAIT muss dazu führen, dass erforderliche Projektierungen des IT-Betriebs und explizit die Entwicklung angemessener Maßnahmen der **Informationssicherheit zielgerichtet** umgesetzt werden. Darüber hinaus sollten alle relevanten Stakeholder für die Erfüllung der Anforderungen aus der BAIT ausreichend informiert und sensibilisiert werden.

DGI®

Inhalt des Seminars

Erwerben Sie die spezifischen Kenntnisse zur Umsetzung der „Bankenaufsichtliche Anforderung an die IT (BAIT)“

- Die MaRisk
  - Anforderungen an die Informationssicherheit
  - Pflichten für die Dokumentation
  - Prüfung und Audits
  - Sanktionen und Bußgelder
- Informationsrisikomanagement
  - Risk Impact Analyse (RIA)
  - Berichtspflichten und Überwachungsanforderungen
  - Schutzbedarfsfeststellung
- Informationssicherheitsmanagement
  - Leitlinie zur Informationssicherheit
  - Verantwortlichkeiten in der Informationssicherheit
  - Anforderungen an die Informationssicherheit
  - Dokumentation des ISMS
- Operative Informationssicherheit
  - Umsetzung von Maßnahmen
  - Informationssicherheitsvorfallmanagement
- Identitäts- und Rechtemanagement
  - Zutritt, Zugang und Zugriff
  - Überwachungsanforderungen und Rezertifizierung von Rechten
- IT-Projekte und Anwendungsentwicklung
  - Planung und Ablauf
  - Projektrisiken
- IT-Betrieb
  - Anforderungen an den Betrieb der IT-Systeme
  - Anforderungen an die Dokumentation
  - Portfoliomanagement der IT-Systeme
  - Prozesse des IT Service Managements
  - Bestimmung der Service Level
- Auslagerungen und sonstiger Fremdbezug von IT-Dienstleistungen
  - Supplier Management
  - Cloud Management
  - Risikoanalyse und Risikobewertung
  - Überwachung von Dritten
- IT-Notfallmanagement
  - Business Continuity Management
  - Business Impact Analysen (BIA)
  - Bedrohungen und Gefährdungen sowie entsprechende Mindestszenarien
  - Notfallkonzepte
  - Business Continuity Planning (BCP)
  - Übungen und Tests
- Kritische Infrastrukturen
  - Aufsichtsbehörde und § 8a BSIG
  - Meldepflichten