SC145 BAIT - Bankenaufsichtliche Anforderungen an die IT

Kurzbeschreibung:

In diesem Intensivtraining erhalten die Teilnehmer umfassende und praxisgerechte Lösungswege für die operative Umsetzung und Gewährleistung von Informationssicherheit und Risikomanagement - unter Berücksichtigung aufsichtsrechtlicher Pflichten und dem Anspruch an eine ganzheitliche, risikosensible und funktionale Sicherheitsstrategie. Nach diesem Training sind die Teilnehmer in der Lage, den Herausforderungen des regulatorischen Umfelds revisionssicher zu begegnen. Sie kennen die Anforderungen aufsichtsrechtlicher Prüfungen und sind in der Lage, die Anforderungen aus MaRisk und BAIT effizient und revisionssicher umzusetzen.

Zielgruppe:

- Risikomanager und Controller in den Banken und Finanzinstitutionen
- Informationssicherheitsbeauftragte und Datenschutzbeauftragte
- Auslagerungsmanager
- Compliance Officers
- Mitarbeiter aus den Bereichen IT-Controlling und Electronic Banking
- IT-Revisoren
- IT-Prozessmanager
- IT-Manager

Voraussetzungen:

Grundkenntnisse in der IT-Sicherheit bzw. Informationssicherheit

Sonstiges:

Dauer: 3 Tage

Preis: 1850 Euro plus Mwst.

Ziele:

- Sie lernen die Informationssicherheit und Risikomanagement im Bankenumfeld unter Berücksichtigung aufsichtsrechtlicher Pflichten umzusetzen und aufrechtzuerhalten. Sie kennen die Anforderungen und Regularien aus MaRisk und BAIT.

- Sie sind in der Lage, die Anforderungen aus MaRisk und BAIT effizient und revisionssicher umzusetzen.

- Sie sind bestens mit den Voraussetzungen, den Ablauf und der erfolgreichen Durchführung eine Revision vertraut.

Inhalte/Agenda:

- **Einleitung & Grundlagen**
  - ◊ IT-Sicherheit vs. Informationssicherheit
  - ◊ Etablierte Standards & Kriterien-Werke

- **Business Impact Analyse / Schutzbedarfsfeststellung**
  - ◊ Einordnung & Abgrenzung sowie Anwendung im Kontext der BA-IT
  - ◊ Beispielhafte Durchführung einer BIA

- **IT-Strategie und IT-Governance**
  - ◊ Anforderungen an die Steuerung der IT-Risiken (OpRisk) –Ableitung, Formulierung, Messung und Kontrolle von Zielen im Rahmen eines gut dokumentierten IT-Strategieprozesses
  - ◊ Konsistenzschwächen zwischen IT-, Risiko- und Ressourcenstrategie vermeiden – Anforderungen an das Monitoring und Erfolgskontrolle abgeleiteter Maßnahmen
  - ◊ Analyse der IT-Struktur (fachbereichsübergreifend) – Basis für Schutzbedarfsfeststellungen und Steuerungen von IT-OpRisk

- **Anforderungen an das Informationsrisikomanagement**
  - ◊ Anforderungen an die Datenqualität
  - ◊ Zusammenspiel zwischen BIA und Risikomanagement; Definition einer angemessenen Metrik
  - ◊ Nachvollziehbarkeit und Aussagefähigkeit der Risikoberichte – quantitative vs. qualitative Beurteilungen

- **Informationssicherheitsmanagement(systeme): etablierte Standards und wie diese unterstützend wirken können**
  - ◊ Überblick über etablierte Standards (VdS 10000, BSI IT Grundschutz, DIN EN ISO/IEC 27001, IDW PS et al)
  - ◊ Informationssicherheitsmanagement in der Praxis:
  - ◊ Benutzerberechtigungen: Minimale Rechtevergabe und Funktionstrennung – Wie sieht eine revisionssichere Protokollierung aus?
  - ◊ Sicherheitsseitige Begleitung von IT-Projekten und Umgang mit erkannten Informationssicherheitsrisiken – Auswirkungsanalyse – Wie geht man mit erkannten Risiken um?
  - ◊ Changemanagement und Sicherheitspatches – Wie werden Störungen angemessen dokumentiert/analysiert?
  - ◊ Auslagerungen und sonstiger Fremdbezug im Einklang mit den (IT-) Strategien – Cloud-Dienste im Kontext der BA-IT

- **Benutzerberechtigungsmanagement**
  - ◊ Prozess zur Vergabe, Kontrolle und Löschung – häufige Schwächen und Feststellungsquellen
  - ◊ Einstufung und Protokollierung kritischer Zugriffsrechte – regelmäßiger Abgleich mit dem SOLL-Berechtigungskonzept
  - ◊ Einrichtung angemessener Prozesse zur Protokollierung und Zuordnung der Verantwortung einer unabhängigen Stelle

- **IT-Projekte und Anwendungsentwicklung**
  - ◊ Inventarisierung der IT-Systeme – Abhängigkeiten und daraus resultierende OpRisk (IT)
  - ◊ Identifikation und Bewertung abhängiger IT-Risiken – Gefahr und Vermeidung doppelter Bewertung; geeignetes Clustering und Gruppierung

- **Anforderungen an den sicheren IT-Betrieb, Sicherung von Informationen**
  - ◊ Konkrete Erwartungen an das Datensicherungskonzept
  - ◊ Business Continuity Management vs. Notfallmanagement: Einordung sowie Abgrenzung

- **Outsourcing & Lieferantenbeziehungen**
  - ◊ Konkretisierung durch die BA-IT – Steuerung und Transparenz im Mittelpunkt
  - ◊ Prüfung von Weiterverlagerungen bis zum 3. Weiterverlagerungslevel – Anforderungen an vertragliche Gestaltungen
  - ◊ Prüfung großer IT-Dienstleister – Relevante Auslegungsfragen, Lieferantenaudits und wie Standards angemessene Alternativprüfungsmöglichkeiten darstellen können

- **Einstufung als Betreiber einer kritischen Infrastruktur – was bedeutet das jetzt konkret?**
  - ◊ KRITIS-Sektorstudie Finanz- und Versicherungswesen
  - ◊ B3S – was ist das überhaupt, was gibt es aktuell für die Finanzbranche und wo ist der Haken?

- **Wertvolle Praxistipps & Hinweise**
  - ◊

◊ Häufige Probleme im Informationsverbund: Überblick, Aktivitäten und Ableitungen
◊ Informationssicherheitsmanagement: Handlungsempfehlungen zur Prozessgestaltung, Dokumentation und zum Test des Informationssicherheitsvorfalls
◊ Handlungsempfehlungen und Praxisbeispiele aus aktuellen IT-Prüfungserfahrungen

◊