1. Juli 2024 · 12:30–16:00 Uhr
Online-Veranstaltung

AKADEMIE HEIDELBERG

# Aktuelle Aufsichts-Anforderungen an die operative Informationssicherheit

## Banken-Aufsicht-Seminar · 4,5 CPE-Punkte

Aktuelle Anforderungen an Schwachstellenmanagement, Penetrationstests und SIEM!

- **Konkrete Aufsichts-Erwartungen aus MaRisk, BAIT und EBA-ICT-Leitlinien**
- **Häufige Fragestellungen und identifizierte Schwachstellen in der Praxis**
- **Anforderungen an das (toolunterstützte) Identifizieren und die Behandlung von Schwachstellen**
- **Anforderungen an die Durchführung regelmäßiger Penetrationstests**
- **Anforderungen an die SIEM-Administration, Loganbindung, Use Cases und die Behandlung von SIEM-Meldungen innerhalb eines SOC**
- **Anforderungen an den Malwareschutz, den Schutz vor Datenabfluss und die Verwaltung und das Management zulässiger Software und IDV**

**Referent**

Alexander Lohr
Ehem. Bankgeschäftliche IT-Prüfungen, SAP Systemservices
Architektur, Zentrale IT-Plattformmanagement Drittprodukte
Deutsche Bundesbank, Düsseldorf

# Aktuelle Aufsichts-Anforderungen an die operative Informationssicherheit

## Programm

**Alexander Lohr, Bundesbank** · 12:30 – 16:00 Uhr

Vorstellung der konkreten Erwartungen der Aufsicht an ausgewählte Themen der operativen Informationssicherheit aus MaRisk, BAIT, DORA und EBA-ICT-Leitlinien

- Konkretisierung der Anforderungen an die operative Informationssicherheit durch MaRisk und BAIT – Neuerungen und Verschärfungen durch DORA
- Identifikation, Bewertung und Behandlung von Schwachstellen. Anforderungen an die Nutzung eines Schwachstellenscanners (Netzwerkscan/ authentifizierter Scan)
- Umgang mit Schwachstellen im Schwachstellen-management, Bündelung und Priorisierung, Reporting und Übertragung in das Risikomanagement
- Notwendigkeit von regelmäßigen Penetrationstests, Inhalte, Angriffsszenarien, Root-Cause-Analyse, Bewertung der Ergebnisse
- Einsatz eines SIEM-Systems, notwendige Loganbin-dungen, Anforderungen an die Qualität der Logs und Speicherfristen, Entwicklung von Use Cases
- Security Operations Center (SOC), 24/7 Überwachung, Reporting von SIEM-Alarmen
- Schutz vor Schadsoftware: Web-Proxy, lokale Client- und Serverinstallationen (Windows/Unix/Mainframe), möglicher Verzicht auf lokalen Virenschutz
- Schutz vor Datenabfluss, Verschlüsselung, Vorstellung klassischer Datenabflusskanäle
- Management zulässiger Software und IDV, Entwickler-Clients, administrative Benutzer, Skriptausführung und Überwachung
- Einbezug von IT-Dienstleistern – Prozesstransparenz und Steuerbarkeit
- Häufige Fragestellungen
- Praxisbericht: Identifizierte Schwachstellen aus aktuellen Prüfungen

## Gute Gründe für Ihre Teilnahme

- Sie erarbeiten sich aktuelles Know-how zu spezifischen Aufsichts-Anforderungen an die operative Informationssicherheit
- Sie erhalten sofort anwendbare Umsetzungstipps für Ihr Institut und Ihren Bereich
- Sie klären offene Fragen für Ihren Bereich oder Ihr Institut mit dem Referenten
- Sie erhalten wertvolle Praxistipps im Erfahrungsaustausch mit anderen Praktikern*innen

## Seminarziel

Der Bereich der operativen Informationssicherheit ist facettenreich und entwickelt sich, dem Stand der Technik entsprechend, stetig weiter. So konnte beispielsweise in den letzten Jahren beobachtet werden, dass der Einsatz eines Security Information and Event Management (SIEM)-System sowie eines Schwachstellenscanners unabdingbar für die Erfüllung eines hohen Schutzbedarfes für sicherheitskritische IT-Systeme sind. Dementsprechend wachsen auch die aufsichtlichen Anforderungen an die von den Instituten verantworteten IT-Systemen.

Wesentliche Feststellungen in dem Bereich der operativen Informationssicherheit zeigen, dass für viele Institute ein Nachholbedarf zur Erfüllung der aufsichtlichen Anforderungen und zur Erfüllung des eigenen Sollmaßnahmenkataloges erforderlich ist, um die sicherheitsrelevante Systeme auch tatsächlich vor Schwachstellen zu schützen.

Nicht nur die reine Identifikation möglicher Schwachstellen, sondern auch deren Behebung setzt die Informationssicherheit, nicht zuletzt auch aufgrund der stetig wachsenden IT-Landschaft, vor große Herausforderungen, die mit dem Informationsrisikomanagement in Einklang gebracht werden müssen.

Sofern das Institut Dienstleister (zum Beispiel zur Administration eines SIEM) beauftragt, müssen die Anforderungen dennoch eingehalten und von der Informationssicherheit überwacht werden.

Die (IT-)Revision hat die Einhaltung der in den MaRisk und BAIT verankerten Anforderungen entsprechend zu prüfen.

## Wissenswertes

Aus der Praxis für die Praxis!
Wir wenden uns insbesondere an die Mitarbeitenden der Bereiche

- IT-Sicherheitsmanagement und IT-Architekten
- Informationssicherheit (ISB) und Informationsrisikomanagement (IRM)
- Interne Revision und IT-Revision
- IT-Organisation, IT-Notfallmanagement und ITSCM
- IT-Compliance und IT-Governance
- IT-Grundsatz und IT-Regulatorik
- sowie andere interessierte Fachbereiche bzw. Vorstands- und Geschäftsleitungsmitglieder, externe Prüferinnen und Prüfer sowie Bankdienstleister

## Unser Referent

**Alexander Lohr**
Ehem. Bankgeschäftliche IT-Prüfungen, SAP Systemservices Architektur, Zentrale IT-Plattformmanagement Drittprodukte
Deutsche Bundesbank, Düsseldorf

*Alexander Lohr ist studierter Wirtschaftsinformatiker und arbeitet seit über 12 Jahren bei der Deutschen Bundesbank. Mehrere Jahre war er als Prüfer im Rahmen von bankgeschäftlichen IT-Prüfungen bei Banken und Sparkassen im Einsatz. Zuvor war er als Programmierer sowie als IT- und Cloud-Architekt für die Bundesbank tätig. Zudem war er projektbezogen für die Europäische Zentralbank (EZB) tätig.*

IT-Auslagerungen & IT-Notfallmanagement
im Fokus der Aufsicht
15./16. Mai 2024, Online-Veranstaltung

DORA, MaRisk & NIS-2-Richtlinie in der Dienstleistersteuerung
4. Juni 2024, Online-Veranstaltung

BAIT Spezial:
Informationssicherheit & Informationsrisikomanagement
4. Juni 2024, Online-Veranstaltung

Auslagerungsmanagement Spezial: Steuerung von »Software as a Service« (SaaS) und Cloud-Diensten
6. Juni 2024, Online-Veranstaltung

Agile Revisionsprüfungen & Prüfungsplanungen
10. Juni 2024, Online-Veranstaltung

Fachtagung IT-Aufsicht
17./18. Juni 2024, Online-Veranstaltung

BAIT Spezial für Compliance & Governance
26. Juni 2024, Online-Veranstaltung

DORA-konforme Auslagerungsverträge & SLA
1. Juli 2024, Online-Veranstaltung

Basis-Seminar »IKT-Risikomanagement«
10./11. Juli 2024, Online-Veranstaltung

▶ Diese und weitere Seminar-Angebote finden Sie bei uns online unter *www.akademie-heidelberg.de/online-seminare*

## Zusätzliche Informationen

Fragen zu diesen Schulungen oder unserem gesamten Seminar-Programm beantworte ich Ihnen sehr gerne.

Björn Wehling
Telefon 06221/65033-44
b.wehling@akademie-heidelberg.de

# Anmeldeformular

Aktuelle Aufsichts-Anforderungen an die operative Informationssicherheit

Name

Vorname

Position

Firma

Straße

PLZ / Ort

Tel./Fax

E-Mail

Name der Assistenz

Datum Unterschrift

An **anmeldung@akademie-heidelberg.de** oder per Fax an: **06221/65033-29**

### Termin + Seminarzeiten

Montag, 1. Juli 2024
12:30–16:00 Uhr
Online-Zugang ab 12:15 Uhr

Seminar-Nr. 24 07 BA111 W

### Teilnahmegebühr

€ 320,– (zzgl. gesetzl. USt)

Die Gebühr beinhaltet die Teilnahme am Online-Seminar sowie die Präsentation als PDF-Datei.
Im Anschluss an das Seminar erhalten Sie ein Zertifikat, das Ihnen die Teilnahme an der Fortbildung bestätigt.

### Allgemeine Geschäftsbedingungen

Es gelten unsere Allgemeinen Geschäftsbedingungen (Stand: 01.01.2010), die wir Ihnen, wenn gewünscht, gerne zusenden. Diese können Sie jederzeit auch auf unserer Hompage einsehen: *www.akademie-heidelberg.de/agb*

### Zum Ablauf

- Vor dem Seminartag erhalten Sie von uns eine E-Mail mit einem Link, über den Sie sich direkt in die Online-Veranstaltung einwählen können.
- Für Ihre Teilnahme ist es nicht notwendig, ein Programm herunterzuladen. Sie können am Seminar direkt per *Zoom* im Internet-Browser teilnehmen.
- Über Ihr Mikrofon und Ihre Kamera können Sie jederzeit Fragen stellen und mit den Referierenden und weiteren Teilnehmenden diskutieren. Alternativ steht auch ein Chat zur Verfügung.

**AH Akademie für Fortbildung Heidelberg GmbH**
Maaßstraße 28 · 69123 Heidelberg
Telefon 06221/65033-0 · Fax 06221/65033-69
info@akademie-heidelberg.de
www.akademie-heidelberg.de

04.24/2407BA111