



Wissen online

Informationssicherheitsbeauftragter kompakt

Die neue Rolle sicher bewältigen

Alles im Griff –

Aufgaben und Rolle des Informationssicherheitsbeauftragten

Die BaFin wird mit den „Bankaufsichtlichen Anforderungen an die IT (BAIT)“, die Funktion des Informationssicherheitsbeauftragten konkretisieren.

Das Institut hat die Funktion des Informationssicherheitsbeauftragten zur Wahrnehmung aller Belange der Informationssicherheit innerhalb des Instituts und gegenüber externen IT-Dienstleistern einzurichten. Eine Auslagerung ist unter bestimmten Voraussetzungen zwar möglich, in diesem Fall ist jedoch eine zuständige Ansprechperson im Institut zu benennen.

Da Informationen und deren Verarbeitung in IT-Systemen in den Instituten essentiell für den Geschäftsbetrieb sind, müssen deren Integrität, Verfügbarkeit, Authentizität und Vertraulichkeit stets sichergestellt sein. Damit ist das Informationssicherheitsmanagement integraler Bestandteil einer ordnungsgemäßen Geschäftsorganisation gem. § 25a Abs. 1 KWG i. V. m. AT 7.2 MaRisk. Die Geschäftsleitung trägt dabei die Gesamtverantwortung für das Informationssicherheitsmanagement und muss somit den Sicherheitsprozess initiieren, steuern und kontrollieren. Explizit benennt die BaFin bei den Aufgaben der Geschäftsleitung das Treffen strategischer Leitaussagen im Rahmen der IT-Strategie, das Erstellen einer Informationssicherheitsleitlinie und das Schaffen der notwendigen organisatorischen Rahmenbedingungen. Umgesetzt werden die genannten Vorgaben in einem Informationssicherheitskonzept, welches wiederum selbst auch geplant, umgesetzt, kontrolliert und weiter verbessert werden muss. Dies wird in den Banken ein „Informationssicherheitsbeauftragter“ übernehmen. Dieser nimmt die Belange der Informationssicherheit innerhalb des Instituts und gegenüber externen Erbringern von IT-Services wahr.

Der interne Informationssicherheitsbeauftragte muss dafür über ausreichend Sachkompetenz und IT-Sachverstand verfügen, damit die Geschäftsleitung jederzeit ihrer Verantwortung für das Informationssicherheitsmanagement gerecht werden kann, und externen Partnern ein kompetenter Ansprechpartner für Fragen zur Verfügung steht. Die dafür notwendige Sachkunde und organisatorische Einbindung wird von der BaFin in den BAIT konkretisiert. Die derzeitige Fassung besagt, dass der Informationssicherheitsbeauftragte nicht in die Hierarchie der internen operativen IT eingebunden sein darf. In kleineren Instituten könne die Funktion mit anderen Beauftragten (z.B. Risikocontrolling, Compliance)

gebündelt oder von der Geschäftsleitung selbst übernommen werden. In jedem Fall ist bei dem Informationssicherheitsbeauftragten und dessen Vertreter eine ausreichende Kenntnis zu den Themen erforderlich.

Die erforderlichen Grundlagenkenntnisse erlangen Sie in unserem Online-Kurs zum Informationssicherheitsbeauftragten kompakt. Tiefergehende Kenntnisse vermitteln wir den Fachverantwortlichen in unseren Programmen zum „Informationssicherheitsmanager ADG“.

In dem Online-Kurs aktualisieren und erweitern Informationssicherheitsbeauftragte ihre Kenntnisse in folgenden Themenfeldern:

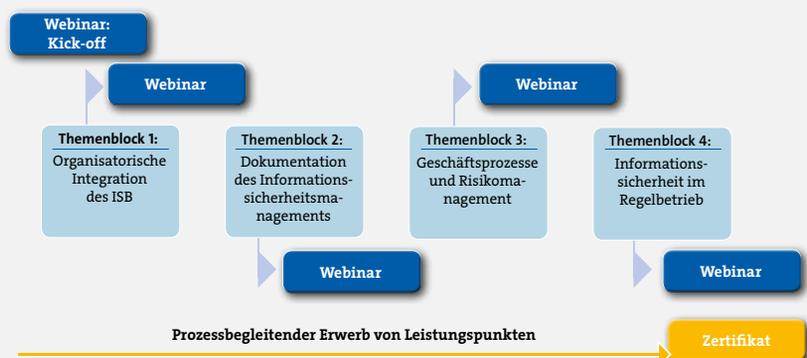
- Organisatorische Integration des Informationssicherheitsbeauftragten
- Dokumentation des Informationssicherheitsmanagements
- Geschäftsprozesse und Risikomanagement
- Informationssicherheit im Regelbetrieb

Sie erhalten darüber hinaus methodische Hilfestellungen für den Transfer und die Umsetzung in ihren Häusern.

Das Konzept:

Der Online-Kurs ist als Blended-Learning – Kombination von Selbstlerneinheiten, Gruppenaustausch und Meetings via Webinaren – konzipiert. Nach einem medialen Informationsinput (Videos, WBT etc.) beschäftigen sich die Teilnehmer mit konkreten, abgegrenzten Fragestellungen, die sich auf ihre eigenen Häuser beziehen. Ihre Ergebnisse und Lösungsansätze stellen sie in Form von Forumseinträgen und Kommentaren zur Diskussion. Das Forum wird von Fachexperten und Prozessmoderatoren begleitet. Die Teilnehmer haben so die Möglichkeit, inhaltlich sowie methodisch ihre Lösungsansätze zu reflektieren und sich gegenseitig zu unterstützen. Dies dient dem Anwendungstransfer und der Netzwerkbildung in der Gruppe. Zum Abschluss jedes Themenblocks erfolgt eine moderierte Diskussion (Webinar) zu den jeweiligen Fachfragen und Lernerfahrungen der Woche. Die Qualifizierung erfolgt „in der Bank“, d.h. arbeitsplatznah ohne zusätzliche Reise- und Abwesenheitszeiten. Der Zeitbedarf beträgt ca. 4 Stunden pro Woche. Jeder Themenblock schließt mit einem Wissensquiz ab. Weitere zertifikatsrelevante Punkte werden über Aufgaben erworben.

Programm- ablauf



Die Veranstaltung richtet sich an:

- Vorstände, Führungskräfte und Spezialisten in den Banken, die die Aufgabe des Informationssicherheitsbeauftragten in Zukunft übernehmen.

Ihr Nutzen als Teilnehmer:

- Sie können sich die für die Funktion des Informationssicherheitsbeauftragten erforderlichen Grundlagenkenntnisse in einem 4-Wochen-Online-Kurs aneignen.
- Sie lernen die erforderlichen Grundlagen kompakt kennen. Danach können Sie für sich beurteilen, welche weiteren Vertiefungen für Sie in Ihrem Haus relevant sind.
- Der Online-Kurs ermöglicht Ihnen ein selbständiges Einteilen Ihrer Lernzeit.
- Sie profitieren von den begleitenden Reflektionsaufgaben und lernen die Umsetzung der Informationssicherheit in Ihrem Haus hautnah kennen.
- Sie sammeln während des Programms erste Umsetzungserfahrungen und können weitere Umsetzungsschritte konkret angehen.
- Das Zertifikat dokumentiert Ihre Themenkompetenz.

Der Nutzen für Ihre Bank:

- Die Inhalte sind mit den Kenntnisanforderungen der BaFin gem. aktuellem Stand der BAIT abgestimmt.
- Ihr Informationssicherheitsbeauftragter erwirbt die Grundlagenkenntnisse, um in seiner neuen Funktion zu starten.
- Die Wissensvermittlung erfolgt rein online – sie sparen damit Abwesenheitszeit und Fahrtkosten.
- Die bankinternen ersten Umsetzungsschritte des Teilnehmers werden von unseren Fachexperten aktiv mitbegleitet.
- Mit dem Zertifikat können Sie die IT-Kompetenz Ihrer Verantwortlichen dokumentieren.

Zeitplan und Inhalte

Einführungswebinar: Zielsetzung, Struktur und Ablauf des Kurses

Webinartermin: 07.11.2019 | 09:00 Uhr

Themenblock 1: Organisatorische Integration des Informationssicherheitsbeauftragten

- Auswahl des Informationssicherheitsbeauftragten
- Aufgabenprofil und Ziele
- Organisatorische Einbindung
- Zusammenarbeit im Informationssicherheitsteam
- Rechtliche und aussichtsrechtliche Anforderungen (MaSI, IT-Sig, BDSG)

Webinartermin: 14.11.2019 | 09:00 Uhr

Themenblock 2: Dokumentation des Informationssicherheitsmanagements

- IT-Strategie
- Informationssicherheitsleitlinie
- Richtlinie zum Informationsrisikomanagement
- Informationssicherheitskonzept
- Notfallvorsorge und Notfallhandbuch

Webinartermin: 21.11.2019 | 09:00 Uhr

Themenblock 3: Geschäftsprozesse und Risikomanagement

- Einbindung der Geschäftsprozessverantwortlichen
- Bewertung der Wesentlichkeit von Geschäftsprozessen
- Business-Impact-Analyse und Schutzbedarfsbewertung
- Risiko- und Restrisikoanalyse
- Aufbereitung und Dokumentation des Risikoberichts

Webinartermin: 28.11.2019 | 09:00 Uhr

Themenblock 4: Informationssicherheit im Regelbetrieb

- Überwachung der Sicherheitsmaßnahmen
- Durchführung von Mitarbeiterschulungen
- Auslagerungscontrolling
- Wirtschaftlichkeit kontra Informationssicherheit
- IT-Prüfungsgebiete, Vorbereitung und notwendige Dokumentation

Webinartermin: 05.12.2019 | 09:00 Uhr



Ihre Fachexperten:

[Dr. Haiko Timm](#), Forum Gesellschaft für Informationssicherheit GmbH, unterstützt und berät Banken rund um das Thema IT-Sicherheit – speziell in den Themen IT-Sicherheitsmanagement und IT-technische Umsetzung der MaRisk – und führt System-, Prozess- sowie vor allem Sicherheitsanalysen durch.

[Martin Wiesenmaier](#) ist bei der FORUM Gesellschaft für Informationssicherheit mbH als Leiter IT-Prüfung/IT-Beratung tätig. Seine beruflichen Schwerpunkte liegen auf der IT-Revision sowie Beratungen rund um die Themen Informationssicherheitsmanagement, Notfallkonzept, Outsourcing sowie Benutzerberechtigungsmanagement.

[Frank Stiegler](#) ist Rechtsanwalt mit Schwerpunkt im IT-Recht in Frankfurt, bewegt sich im Umfeld des Chaos Computer Club. Er berät und begleitet Unternehmen auf Deutsch und Englisch als Berater und externer Datenschutzbeauftragter mit Fokus auf Praktikabilität und Verständlichkeit.

Prozessbegleitung und Moderation:

[Andreas Siemes](#) war Projektleiter Online-Bildung bei der Konrad-Adenauer-Stiftung. Er verfügt über jahrelange Erfahrung bei der Gestaltung und Begleitung von online-Kursen.

Prozessbegleitung VR-Bildung:

[Thorsten Ewertowski](#) ist bei der ADG als Spezialist für E-Learning und Lernsysteme tätig. Der studierte Wirtschaftsinformatiker hat über 5 Jahre Erfahrung im E-Learning-Bereich und ist für die Administration der Lernplattform VR-Bildung verantwortlich.

Leitung und Koordination des Programms:

[Philipp Diel](#) ist bei der ADG im Produktmanagement für die Themen IT, Organisation und Immobilienwertermittlung zuständig. Dabei hat er bereits vielseitige Online-Lernformate konzipiert und begleitet.

Fax Anmeldung 02602 14 95-500

Informationssicherheitsbeauftragter kompakt

Termin:	Anmelde-Nummer:	Preis:
07.11.2019 09:00 Uhr 21.11.2019 09:00 Uhr	SRB119-063	EUR 499,- für Mitglieder der ADG/des Fördervereins
14.11.2019 09:00 Uhr 28.11.2019 09:00 Uhr		EUR 625,- für Nicht-Mitglieder
05.12.2019 09:00 Uhr		

Name/Vorname

Position

E-Mail Teilnehmer

E-Mail Hauptansprechpartner

Institut

Telefon Teilnehmer

Straße/Postfach

Zugangskennung VR-Bildung

PLZ/Ort

Datum Unterschrift und Stempel