



ZIELGRUPPE:
Informationssicherheitsbeauftragte,
Stellvertretende Informations-
sicherheitsbeauftragte, IT-Revisoren

Ausbildung zum geprüften Informationssicherheitsbeauftragten

Pflichtmodule

(Aufsichts-) rechtliche

Grundlagen (2 Tage)

- Rechtliche Anforderungen an die Informationssicherheit, Strafrecht, BDSG, Arbeitsschutz, Haftungsrisiken, HGB / AO (Archivierung), MaRisk / BAIT / SOIT, IT-Strategie und Informationssicherheitsleitlinie (AT 4, AT 7.2), Softwaretest und -freigabe (AT 7.2), Notfallmanagement (AT 7.3), Bewertung von Änderungen (AT 8.2), Auslagerungsmanagement (AT 9), Planung und Vorbereitung auf (externe) IT-Prüfungen

IT-Risikomanagement (2 Tage)

- Vorgehensweise, Organisation in der Bank, Risikoberichterstattung

Grundlagen der IT für Informationssicherheitsbeauftragte (2 Tage)

- Sicherheit von Infrastruktur und Netzwerken (z. B. WLAN / VoIP), Virenschutz und Firewalls, Sicherheit im Internet / Social Media, Datensicherung, Archivierung, Hardware-Software Management, Incidentmanagement, Einsatz mobiler Endgeräte, Serversicherheit, Notfallvorsorge, Elektronische Kommunikation (E-Mail etc.), kryptografische Verfahren, PKI, Signaturen, Hashes, VPN

Managen Sie die Informationssicherheit in Ihrem Haus – kosteneffizient und anforderungsgerecht

Die fortschreitende Informationstechnologie und der zunehmende Wettbewerb machen es für Unternehmen unerlässlich, das Management kontinuierlich zu modernisieren und den Informationssicherheitsprozess konsequent umzusetzen. Denn die Einführung eines Informationssicherheits-Managementsystems (ISMS) ist für jedes Unternehmen immer auch eine wichtige strategische Entscheidung. Eine besondere Rolle spielt dabei die Qualifizierung von Mitarbeitern, Fachverantwortlichen (Risikoeigentümer) sowie Informationssicherheitsbeauftragten. Sie ist nicht nur die Grundlage für einen bewussten und konsequenten Informationssicherheitsprozess, sondern auch eine gesetzliche Anforderung, die jedes Unternehmen erfüllen muss.

Prozesse und Verfahren kennen und Maßnahmen umsetzen

Die Seminarreihe, die die GenoAkademie in Kooperation mit der Geno Bank Consult GmbH konzipiert hat, erfüllt diese Anforderungen umfassend und kosteneffizient – vom Informationssicherheitsbeauftragten über die Fachverantwortlichen bis hin zu IT-fremden Mitarbeitern. In unseren Pflichtmodulen erhalten Informationssicherheitsbeauftragte einen Überblick über die IT-Prozesse und Verfahren und werden sensibilisiert für die Gefahren und die daraus abzuleitenden Maßnahmen. In den Wahlmodulen gilt der Blick den Spezialthemen. Und in den Webinaren finden sowohl Fachverantwortliche als auch IT-fremde Mitarbeiter Module, die sie im Bereich der Informationssicherheit sensibilisieren.

Geprüfter Informationssicherheitsbeauftragter

Der Informationssicherheitsbeauftragte ist die Basis für ein konsequentes Informationssicherheitsmanagement. Grundlegende Kompetenzen gehen hier einher mit speziellen IT-fachlichen Aufgaben. Mit unserer Modulreihe wollen wir genau diesem Anspruch gerecht werden, d.h. Qualifikationen aufbauen und vertiefen. Optional ist auch eine Prüfung durch die GenoAkademie möglich – mit dem Abschluss zum „Geprüften Informationssicherheitsbeauftragten“. Den Aufbau und die Inhalte der einzelnen Module sowie die Voraussetzungen für die Teilnahme an der optionalen Prüfung finden Sie in der nachfolgenden Detailübersicht.

Informationssicherheit für Fachverantwortliche (Risikoeigentümer)

Die Bankenaufsicht fordert, dass die Fachverantwortlichen in die Erhebung und Bewertung der Daten, Prozesse und IT-Schutzobjekte eingebunden werden. Diese Aufgaben können nur dann wahrgenommen werden, wenn grundlegende Kenntnisse insbesondere des IT-Risikomanagementprozesses vorhanden sind. Wählen Sie aus unterschiedlichen Webinaren für die Fachverantwortlichen Ihrer Institute die passenden aus – und das Ganze durch die Wahl des Formats auch noch wirtschaftlich attraktiv.

Wahlmodule

- Praxisworkshop IT-Risikomanagement mit ForumISM (2 Tage)
- Praxisworkshop Test- und Freigabeverfahren anhand ausgewählter Beispielanwendungen (1 Tag)
- Praxisworkshop IT-Berechtigungs-Sollkonzept (1 Tag)
- Ausgewählte Inhalte von ITIL & COBIT als Referenzmodelle für IT-Prozesse in einer Genossenschaftsbank (1 Tag)
- Praxisworkshop Notfallmanagement inkl. Notfalltestplanung für ausgewählte zeitkritische Geschäftsprozesse (1 Tag)

Voraussetzungen für die Zulassung zur Prüfung zum Geprüften Informationssicherheitsbeauftragten

- Teilnahme an allen Pflichtmodulen
- Teilnahme an mind. 2 Wahlmodultagen
- Fristgerechte Abgabe einer Projektarbeit
- Fristgerechte Anmeldung zur Prüfung

Alle Teilnehmer erhalten eine Teilnahmebescheinigung. Teilnehmer, die zusätzlich die Projektarbeit und das Colloquium absolvieren, erhalten bei Bestehen den Titel „Geprüfter Informationssicherheitsbeauftragter.“



GenoAkademie

FORSBACH

Raiffeisenstraße 10-16
51503 Rösrath
Fax 02205 803-9260

KUNDEN-SERVICE-CENTER

Telefon 02205 803-9292

© 2018 GenoAkademie

Informationssicherheit am Arbeitsplatz

Jeder Mitarbeiter Ihres Hauses trägt als Anwender von IT-Systemen eine nicht unerhebliche Verantwortung für die Aufrechterhaltung der Informationssicherheit. Hierzu ist es wichtig, grundsätzliche Gefährdungspotentiale zu erkennen und sich in den jeweiligen Situationen richtig zu verhalten. Hierzu bieten wir Ihnen Webinare an, mit denen Sie Ihre Mitarbeiter für aktuelle Themen sensibilisieren können.



Webinare

INFORMATIONSSICHERHEIT FÜR FACHBEREICHsverANTWORTLICHE UND RISIKOEIGENTÜMER

Zielgruppe: Bereichsleiter, Fachbereichsverantwortliche, Stabsstellenleiter, Prozessmanager, Interne Revision

Ihr Nutzen: Die Teilnehmer erfüllen die Anforderungen im Rahmen des Informationssicherheitsmanagements.

Exemplarische Themen: Erhebung und Bewertung von Geschäftsprozessen am Beispiel von ForumISM (60 Minuten), Erhebung und Bewertung von IT-Schutzobjekten am Beispiel von Forum ISM (90 Minuten), Planung, Durchführung und Dokumentation von Notfalltests (45 Minuten), Anforderungen an die Einführung und Nutzung von Software, insbesondere Eigenentwicklungen (60 Minuten), Rezertifizierung des IT-Berechtigungs-Sollkonzepts (45 Minuten), Beurteilung von Auslagerungsunternehmen (Risiko & Leistung) (45 Minuten)

INFORMATIONSSICHERHEIT AM ARBEITSPLATZ

Zielgruppe: Alle Mitarbeiter der Bank und dauerhafte externe Mitarbeiter

Ihr Nutzen: IT-fremde Mitarbeiter werden zum sicheren Umgang mit der IT sensibilisiert.

Exemplarische Themen: Sicherheit im Internet / Social media (30 Min.), Einsatz mobiler Endgeräte (30 Min.), Hinweise zur Nutzung der IT in einer Genossenschaftsbank (30 Minuten), Aktuelle Gefährdungen (30 Min.), Elektronische Kommunikation (E-Mail etc.) (30 Min.)

Wir haben Ihr Interesse geweckt? Sie haben weitere Fragen zu unseren Angeboten? Dann rufen Sie uns an oder schreiben eine E-Mail.

Wir helfen Ihnen gerne weiter!



DIRK MERTENS

Telefon: 0151 15312317
Dirk.Mertens@GenoBC.de

MICHAEL FENSKE

Telefon: 02205 803-9273
Michael.Fenske@genossenschaftsverband.de



BJÖRN SCHERER

Telefon: 0151 14827873
Bjoern.Scherer@GenoBC.de

