Sparkassenakademie
Nordrhein-Westfalen



FORTBILDUNGSPROGRAMM 2027

IT-Sicherheit

INHALTSVERZEICHNIS

SEITE

IT-Sicherheit **3**

46.750 Vertiefung technischer Grundlagen für Informationssicherheitsbeauftragte (ISB) 4

46.754 Kompaktseminar Business Continuity Beauftragte/-r (BCB) - Theoretische Grundlagen (Modul 1) 6

46.756 Erfahrungsaustausch Notfallmanagement (BCM) 8

46.757 Erfahrungsaustausch Informationssicherheits-Management (ISMS) (online) 10

46.758 Workshop zur Vorbereitung auf eine IT-Prüfung nach § 44 KWG 12

46.755 Kompaktseminar Business Continuity Beauftragte/-r (BCB) - Umsetzung in der Praxis (Modul 2) . 14

46.725 Cyberkriminalität: Sensibilisierung durch Hacking-Techniken und Pentests (online) 16

46.745 Grundlagen ISO 27001:2022 (online) 18

46.742 Physische Konzepte im IKT-Risikomanagement und Informationssicherheitsmanagement (online) 20

46.749 ITM-Radar - Protokollierung und Protokollauswertung (online) 22

46.753 Operative Informationssicherheit für die 1st-Line 24

46.120 Grundlagen für neue Informationssicherheitsbeauftragte 26

46.762 Erfolgreiche Auditierung in der Praxis (online) 28

46.763 Methoden im IKT-Risiko- und Informationssicherheitsmanagement erfolgreich umsetzen 30

46.765 Vorfallmanagement - Umgang mit IKT-Vorfällen gemäß DORA (online) 32

46.804 Maßnahmen für kritische oder wichtige Funktionen in der Praxis (online) 34

46.805 Praxis-Workshop - Methodik zur Ermittlung kritischer oder wichtiger Funktionen (kowF) (online) 36

46.767 Business-Impact-Analyse (BIA): Grundlagen verstehen, Praxis beherrschen und erfolgreich implementieren (online) 38

46.768 Praxis-Workshop: Effektive Notfallübungen – Wissen und Handwerkszeug für Notfälle (online) .. 40

46 ORGANISATION UND IT-BETRIEB

IT-Sicherheit

Vertiefung technischer Grundlagen für Informationssicherheitsbeauftragte (ISB)

In diesem Seminar erhalten Sie vertiefende Kenntnisse in ausgewählten Bereichen der logisch, technischen Konzepte (SITB). Durch die systematische Vermittlung und Aktualisierung ausgewählter Themenschwerpunkte werden Sie in die Lage versetzt, Schutzmaßnahmen für technische orientierte Bedrohungen zu bewerten.

ZIELGRUPPE

Informationssicherheitsbeauftragte, Informationssicherheitskoordinatorinnen und -koordinatoren, Datenschutzbeauftragte, IT-Revisorinnen und -Revisoren und IT-Verantwortliche

IHR NUTZEN

- Sie vertiefen Ihre Kenntnisse in ausgewählten Bereichen der logisch, technischen Konzepte.
- Sie sind vertraut mit aktuellen Angriffsvektoren von Cyberkriminellen.
- Sie sind in der Lage, Schutzmaßnahmen für technisch orientierte Bedrohungen zu bewerten.

VORAUSSETZUNG(EN)

Besuch des Seminars **„Grundlagen für neue Informationssicherheitsbeauftragte“ (Angebotsnummer 46.120)** oder erste Erfahrungen im Umgang mit den logisch, technischen Konzepten des SITB

Dieses Seminar richtet sich an Teilnehmerinnen und Teilnehmer ohne oder mit ersten Kenntnissen im Bereich technische Informationssicherheit.

IHR REFERENT

Peter Zwack, S-Management Services GmbH

TERMIN(E)

04.11.2026 – 05.11.2026 |
Sparkassenakademie NRW

09.11.2027 – 10.11.2027 |
Sparkassenakademie NRW

DAUER

2 Tage

PREIS

940,00 €

KONTAKT

ANMELDUNG



Kristina Barbknecht
0231 22240-728
kristina.barbknecht@ska.nrw

INHALTE



Sabine Berens
0231 22240-740
sabine.berens@ska.nrw

Programm/Inhalt

In folgenden Bereichen wird u.a. eine fachliche Vertiefung vermittelt:

Nutzerverwaltung und Passwortsicherheit

Schadsoftware, schadhafte Inhalte sowie Arten von Malware und Funktionsweise: Cross-Site-Scripting, Trojaner, Würmer, Viren, Exploits

Netzstruktur, -sicherheit inkl. WLAN-Absicherung, Portsecurity, Authentifizierung, Pentests, Netzwerkpläne

Datenaustausch, -ablage sowie Grundlagen der Kryptografie, Praxistipps zu Druckern und Multifunktionsgeräten, Vorbeugung gegen APT's

Bei Relevanz wird auf die Lösungen und Produkte der Finanz Informatik zu ausgewählten Themen eingegangen.

Kompaktseminar Business Continuity Beauftragte/-r (BCB) - Theoretische Grundlagen (Modul 1)

Die Bankenaufsicht stellt hohe Anforderungen an das Business Continuity Management (BCM) der Sparkassen. In diesem Seminar erwerben Sie praxisorientiertes Wissen und anwendbare Methoden, um Notfallmanagement und BCM ganzheitlich, regulatorisch konform und auditfähig zu gestalten. Sie erhalten Antworten auf zentrale Fragen wie: Was sind die wesentlichen Prozesse des Notfallmanagements? Wann handelt es sich um einen Störfall, einen Notfall oder eine Katastrophe?

ZIELGRUPPE

Notfallbeauftragte (BC-Beauftragte) und Vertretungen, Einsteiger bis Fortgeschrittene
Umsetzungsverantwortliche für BCM-Projekte (Neuaufbau oder Aktualisierung)
Informationssicherheitsbeauftragte mit BCM-Schnittstellen

IHR NUTZEN

- Sie können souverän ein ganzheitliches BCM inkl. Notfallmanagement gemäß DORA, KWG, MaRisk und den relevanten Standards (u. a. BSI,ISO) umsetzen.
- Sie kennen praxiserprobte Methoden (BIA, RIA, Szenarioplanung, Übungsdesign, Krisenkommunikation, Berichts- und Auditfähigkeit) und können diese umsetzen.
- Sie wissen, wie konkrete Fallbeispiele in der Praxis lösungsorientiert umgesetzt werden.

VORAUSSETZUNG(EN)

Das Kompaktseminar ist modular aufgebaut:

Modul 1: Theoretische Grundlagen - keine Voraussetzungen

Modul 2: Umsetzung in der Praxis - Vorkenntnisse auf dem Niveau von Modul 1 erforderlich (Angebotsnummer 46.755)

IHR REFERENT

Moritz Schumann, S-Management Services GmbH

HINWEIS(E)

Im Seminar erfolgt keine Abbildung oder Schulung der Inhalte in RiMaGo.

Bitte bringen Sie ihren eigenen Laptop mit, um sich in das sparkasseneigene System (z.B. RiMaGo etc.) einloggen zu können.

TERMIN(E)

05.04.2027 – 06.04.2027 |
Sparkassenakademie NRW

DAUER

2 Tage

PREIS

1.150,00 €

KONTAKT

ANMELDUNG



Kristina Barbknecht
0231 22240-728
kristina.barbknecht@ska.nrw

INHALTE



Sabine Berens
0231 22240-740
sabine.berens@ska.nrw

Programm/Inhalt

Begriffe, Aufbauorganisation, Rollen im BCM

Regulatorik: DORA, KWG, MaRisk; Leitlinien/Standards (BSI, ISO)

IKT-Geschäftsfortführungsleitlinie, Ziele und Kennzahlen

Einführung in BIA und RIA; RTO vs. RTA; Schnittstelle IKT-Risikomanagement

Überblick zu Geschäftsfortführungs-, Wiederanlauf- und Wiederherstellungsplänen

Berichtswesen, Schulung/Sensibilisierung

Erfahrungsaustausch Notfallmanagement (BCM)

Die Bankenaufsicht stellt hohe Anforderungen an das Notfallmanagement (BCM) der Sparkassen. Vernetzen Sie sich in unserem Erfahrungsaustausch mit anderen Sparkassen zu aktuellen Themen des Notfallmanagements. Profitieren Sie vom Wissenstransfer zwischen den Sparkassen und dem Referenten und vertiefen Sie Ihre methodische Vorgehensweise anhand von Praxisbeispielen.

Neben den aktuellen Themen haben Sie die Chance, dass Ihre individuellen Themen ebenfalls Berücksichtigung finden. Diese werden durch den Referenten vorbereitet und etwaige Lösungsansätze sowie methodische Vorgehensweisen vorgestellt.

ZIELGRUPPE

Notfallbeauftragte sowie deren Vertreter/-innen, IT-Revisoren und -Revisorinnen

IHR NUTZEN

- Sie profitieren vom Informationsaustausch und Wissenstransfer mit anderen Sparkassen.
- Sie erhalten neue Impulse und Lösungsansätze zur Fortschreibung des eigenen Notfallmanagements (BCM).
- Sie lernen methodische Vorgehensweisen kennen und vertiefen diese.

VORAUSSETZUNG(EN)

Erfahrungen mit und Kenntnisse von BCM-Prozessen als Notfallbeauftragte/r, als Vertretung oder als Mitarbeiter/-in der IT-Revision

REFERENTINNEN UND REFERENTEN

- Moritz Schumann, S-Management Services GmbH
- Peter Schwarz, S-Management Services GmbH

HINWEIS(E)

Bitte reichen Sie Ihre Fragen und Themen bis **zwei Wochen** vor der Veranstaltung per Mail an sabine.berens@ska.nrw ein. Alle Anfragen zu Themen werden selbstverständlich anonymisiert behandelt.

TERMIN(E)

14.04.2027 | Sparkassenakademie NRW

DAUER

1 Tag

PREIS

580,00 €

KONTAKT

ANMELDUNG



Kristina Barbknecht
0231 22240-728
kristina.barbknecht@ska.nrw

INHALTE



Sabine Berens
0231 22240-740
sabine.berens@ska.nrw

Programm/Inhalt

Die jeweils aktuellen Inhalte richten sich nach den Anfragen und Themenwünschen der Teilnehmer/-innen und betreffen erfahrungsgemäß alle BCM-Prozesse sowie Aufgaben, die zum Betrieb und zur Aufrechterhaltung des BCM erforderlich sind. Zudem können Sparkassen eigene Themen oder Umsetzungen vorstellen.

Des Weiteren werden vom Dozenten aktuelle Themen zum Zeitpunkt des Erfahrungsaustauschs sowie Herausforderungen und Hinweise aus Prüfungen behandelt.

Die Inhalte berücksichtigen stets Anforderungen aus der DORA-Verordnung, dem Gesetz über das Kreditwesen (KWG) sowie aus den Mindestanforderungen an das Risikomanagement (MaRisk) und Hinweise aus Prüfungen.

Erfahrungsaustausch Informationssicherheits-Management (ISMS) (online)

Vernetzen Sie sich in unserem Erfahrungsaustausch mit anderen Sparkassen zu aktuellen Themen des Informationssicherheits-Management (ISMS). Profitieren Sie vom Wissenstransfer zwischen den Sparkassen und dem Referenten und vertiefen Sie Ihre methodischen Vorgehensweisen und Prozesse (Aktivitäten). Neben den aktuellen Themen haben Sie die Chance, dass Ihre individuellen Themenvorschläge und Fragen ebenfalls Berücksichtigung finden. Diese werden durch den Referenten vorbereitet. Lösungsansätze, methodische Vorgehensweisen und Best-Practice-Ansätze werden vorgestellt.

ZIELGRUPPE

Informationssicherheitsbeauftragte sowie deren Vertreter/-innen, IT-Verantwortliche und dezentrale Informationssicherheits-Koordinatorinnen und -Koordinatoren, IT-Revisorinnen und -Revisoren

IHR NUTZEN

- Sie profitieren vom Informationsaustausch und Wissenstransfer.
- Sie erhalten neue Impulse und Lösungsansätze zur Fortschreibung des eigenen Informationssicherheits-Managements (ISMS).
- Sie vertiefen methodische Vorgehensweisen und Prozesse (Aktivitäten).
- Sie sind informiert über aktuelle Entwicklungen sowie Erkenntnisse im Kontext der Informationssicherheit.

VORAUSSETZUNG(EN)

Erfahrungen und Kenntnisse in Aktivitäten und Prozessen im Informationssicherheits-Managements.

IHRE REFERENTIN

Maxim Sartison, S-Management Services GmbH

HINWEIS(E)

Bitte senden Sie Ihre individuellen Themenvorschläge und Fragen **bis drei Wochen vor der Veranstaltung** per Mail an: sabine.berens@ska.nrw.

TERMIN(E)

12.10.2027 | virtueller Seminarraum

DAUER

1 Tag

PREIS

580,00 €

KONTAKT

ANMELDUNG



Kristina Barbknecht
0231 22240-728
kristina.barbknecht@ska.nrw

INHALTE



Sabine Berens
0231 22240-740
sabine.berens@ska.nrw

Programm/Inhalt

Die jeweils aktuellen Inhalte richten sich nach den Anfragen und Themenwünschen der Teilnehmenden und betreffen erfahrungsgemäß alle ISM-Prozesse sowie Aufgaben, die zum Betrieb und Aufrechterhaltung des ISM erforderlich sind. Zudem können Sparkassen eigene Themen oder Umsetzungen vorstellen.

Des Weiteren werden vom Dozenten aktuelle Themen zum Zeitpunkt des Erfahrungsaustauschs sowie Herausforderungen und Hinweise aus Prüfungen behandelt.

Die Inhalte berücksichtigen stets Anforderungen aus der DORA-Verordnung, dem Gesetz über das Kreditwesen (KWG) sowie aus den Mindestanforderungen an das Risikomanagement (MaRisk) sowie Hinweise aus Prüfungen.

Workshop zur Vorbereitung auf eine IT-Prüfung nach § 44 KWG

Die Umsetzung und Einhaltung der aufsichtlichen Anforderungen sowie der eigentliche Aufsichtsprozess sind deutlich aufwendiger geworden. Insbesondere die Prüfungen der BaFin gemäß § 44 KWG konfrontieren die Sparkassen mit besonderen Herausforderungen. Die Ergebnisse können weitreichende wirtschaftliche und persönliche Konsequenzen haben. In unserem neuen Workshop erwerben Sie das notwendige Wissen, um gut vorbereitet auf eine 44er-Prüfung zu sein.

ZIELGRUPPE

Informationssicherheitsbeauftragte/IKT-Risikokontrollfunktion, Leiter/-innen IT, Leiter/-innen Organisation, IT-Revisoren/-innen, Mitarbeiter/-innen IT-Regulatorik

IHR NUTZEN

- Sie kennen die bisher geprüften Anforderungen und die Vorgehensweise in einer IT-Prüfung gem. § 44 KWG.
- Sie sind in der Lage, Feststellungen zu vermeiden bzw. zu reduzieren.

VORAUSSETZUNG(EN)

Grundlegende Kenntnisse von Aktivitäten und Prozessen im Informationssicherheits-Management

IHR REFERENT

Matthias Doll, S-Management Services GmbH

TERMIN(E)

17.09.2027 | Sparkassenakademie NRW

DAUER

1 Tag

PREIS

580,00 €

KONTAKT

ANMELDUNG



Kristina Barbknecht
0231 22240-728
kristina.barbknecht@ska.nrw

INHALTE



Sabine Berens
0231 22240-740
sabine.berens@ska.nrw

Programm/Inhalt

Finanzdienstleistungsaufsicht in Deutschland und Europa

Gesetze und Standards als Basis für die IT-Prüfung nach §44 KWG

Grundlagen zur IT-Prüfung nach §44 KWG

Organisatorische Vorbereitungen zur IT-Prüfung

Zeitlicher Ablauf einer Prüfung

Verhaltensregeln für die Prüfung

Prüfungsfelder

Bekannte Feststellungen

Für die IT-Prüfung relevante Themen sind:

- **IKT-Strategie**
- **IKT-Governance & Kontrollrahmen**
- **Risikomanagementrahmen & IKT-Risikomanagement**
- **Informationssicherheitsmanagement**
- **Benutzerberechtigungsmanagement**
- **IKT-Projekte und Anwendungsentwicklung**
- **IT-Betrieb**
- **Auslagerung und sonstiger Fremdbezug von IKT-Dienstleistungen**
- **Notfallmanagement**
- **Cybersicherheit**
- **Operative Informationssicherheit**

Kompaktseminar Business Continuity Beauftragte/-r (BCB) - Umsetzung in der Praxis (Modul 2)

Die Bankenaufsicht stellt hohe Anforderungen an das Business Continuity Management (BCM) der Sparkassen. In diesem Seminar erwerben Sie praxisorientiertes Wissen und anwendbare Methoden, um Notfallmanagement und BCM ganzheitlich, regulatorisch konform und auditfähig zu gestalten. Sie erhalten Antworten auf zentrale Fragen wie: Was sind die wesentlichen Prozesse des Notfallmanagements? Wann handelt es sich um einen Störfall, einen Notfall oder eine Katastrophe?

ZIELGRUPPE

Notfallbeauftragte (BC-Beauftragte) und Vertretungen, Einsteiger bis Fortgeschrittene
Umsetzungsverantwortliche für BCM-Projekte (Neuaufbau oder Aktualisierung)
Informationssicherheitsbeauftragte mit BCM-Schnittstellen

IHR NUTZEN

- Sie können souverän ein ganzheitliches BCM inkl. Notfallmanagement gemäß DORA, KWG, MaRisk und den relevanten Standards (u. a. BSI,ISO) umsetzen.
- Sie kennen praxiserprobte Methoden (BIA, RIA, Szenarioplanung, Übungsdesign, Krisenkommunikation, Berichts- und Auditfähigkeit) und können diese umsetzen.
- Sie wissen, wie konkrete Fallbeispiele in der Praxis lösungsorientiert umgesetzt werden.

VORAUSSETZUNG(EN)

Das Kompaktseminar ist modular aufgebaut:

Modul 1: Theoretische Grundlagen - keine Voraussetzungen (**Angebotsnummer 46.754**)

Modul 2: Umsetzung in der Praxis - Vorkenntnisse auf dem Niveau von Modul 1 erforderlich

IHR REFERENT

Moritz Schumann, S-Management Services GmbH

HINWEIS(E)

Bitte bringen Sie ihren eigenen Laptop mit, um sich in das sparkasseneigene System (z.B. RiMaGo etc.) einloggen zu können.

TERMIN(E)

07.04.2027 – 08.04.2027 |
Sparkassenakademie NRW

DAUER

2 Tage

PREIS

1.150,00 €

KONTAKT

ANMELDUNG



Kristina Barbknecht
0231 22240-728
kristina.barbknecht@ska.nrw

INHALTE



Sabine Berens
0231 22240-740
sabine.berens@ska.nrw

Programm/Inhalt

Vertiefung: BIA/RIA-End-to-End, Szenarien für k/w-Funktionen und Mindestszenarien (DORA)

Erstellung und Härtung von GfP/WAP/IKT-Reaktions- und Wiederherstellungsplänen

Übungsplanung und -durchführung (z. B. IT-Notfall, Cyberangriff), Bewertung und Reporting

Krisenkommunikation, Krisenstabsarbeit inkl. Alarmierungsübung

Auditfähigkeit, Umgang mit Schwachstellen, Schnittstellen zum IKT-Risikomanagement

Nutzung institutseigener Tools/Prozesse im Rahmen der Praxisübungen (keine Tool-Schulung)

Möglichkeit, eigene Fallbeispiele einzubringen.

Cyberkriminalität: Sensibilisierung durch Hacking-Techniken und Pentests (online)

In den letzten Jahren haben sich die Vorgehensweisen und Motive von Cyberkriminellen deutlich verändert. Ziel dieses zweitägigen Seminars ist es, die Methoden der Cyberkriminellen zu verstehen, um mit diesem Wissen geeignete IT-Sicherheitsmaßnahmen zu implementieren und IT-Risiken besser einschätzen zu können. Zudem lernen Sie, wie einfache Sicherheitsprüfungen in Form von Penetrationstests im Netzwerk der Sparkasse durchgeführt werden können.

ZIELGRUPPE

Mitarbeiter/-innen aus den Bereichen IT-Organisation, IT-Revision sowie IT-Administratoren und Informationssicherheitsbeauftragte

IHR NUTZEN

- Sie sind vertraut mit aktuellen Angriffsmethoden auf IT-Systeme und IT-Anwendungen.
- Sie sind in der Lage, geeignete IT-Sicherheitsmaßnahmen zu implementieren.
- Sie vertiefen das erlernte Wissen in Form von Praxisübungen.

VORAUSSETZUNG(EN)

Bei der Online-Veranstaltung wird ein virtuelles Trainingslabor in der Cloud bereitgestellt. Erfahrungsgemäß ist die Geschwindigkeit auf dieses Labor aus dem Sparkassennetz heraus sehr langsam und daher das Labor fast nicht zu gebrauchen. Deshalb wird empfohlen, an dem Online-Veranstaltung aus einem anderen Netz heraus teilzunehmen. Dies kann z. B. das DSL-Netz in der Sparkasse oder im Home-Office sein. Zudem wird die Verwendung der Labor-Umgebung der Web-Browser Firefox empfohlen

IHR REFERENT

Marc Heinzmann, plan42 GmbH

HINWEIS(E)

Die Veranstaltung findet im virtuellen Seminarraum der Sparkassenakademie statt. Ihre Zugangsdaten und weitere technische Infos erhalten Sie mit der Einladung zum Online-Seminar.

TERMIN(E)

16.03.2027 – 17.03.2027 | virtueller Seminarraum

DAUER

2 Tage

PREIS

940,00 €

KONTAKT

ANMELDUNG



Kristina Barbknecht
0231 22240-728
kristina.barbknecht@ska.nrw

INHALTE



Sabine Berens
0231 22240-740
sabine.berens@ska.nrw

Programm/Inhalt

Arbeitsweise von Cyberkriminellen

- **Cyberangriffe**
- **Social Engineering**

Ablauf von Angriffen

- **Beispiele anhand der MITRE ATT@CK Matrix**

Angriffe auf das Netzwerk

- **Portscanning**
- **OS Fingerprinting**
- **ARP#Spoofing**
- **DNS#Spoofing**
- **Man#in#the#Middle Angriffe**
- **Netzwerk Sniffing**
- **WLAN Hacking**

Angriffe auf Server#Systeme

- **Schwachstellenscanning mit Nessus**
- **Wörterbuch / Brute Force Angriffe auf Passwörter**
- **Angriffe auf Passwort#Hashes**
- **Angriffe mit dem Exploit Framework "Metasploit"**

Angriffe auf Arbeitsplatzsysteme

- **Drive#by#Downloads**
- **Kodierung von Malware**

Angriffe auf Webanwendungen

- **SQL#Injection**
- **Manipulation von URL#Parametern**
- **Cross#Site#Scripting**

Social Engineering

- **Mögliche Szenarien**
- **Einsatz des "Social Engineering Toolkits"**

Grundlagen ISO 27001:2022 (online)

ISO 27001 spezifiziert die Anforderungen für die Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines Informationssicherheitsmanagements. Machen Sie sich vertraut mit den Grundlagen der ISO 27001:2022.

ZIELGRUPPE

Informationssicherheitsbeauftragte, Mitarbeiter/-innen bzw. Verantwortliche der Fachbereiche, die für Umsetzung, Pflege und Dokumentation der operativen Informationssicherheitsmaßnahmen zuständig sind (dies sind hauptsächlich die Bereiche IT, Betriebsorganisation und Gebäudemanagement [Haustechnik]) und Innenrevisorinnen und -revisoren, die sich zu diesem Thema informieren möchten, z. B. im Vorfeld von Prüfungen

IHR NUTZEN

- Sie verstehen das Zusammenspiel der ISO 2700x Normenreihe,
- Sie haben einen Überblick über die Anforderungen der ISO 27001 an ein Informationssicherheitsmanagementsystem.
- Sie kennen die Planung und die Durchführung von Audits und Kontrollen.

VORAUSSETZUNG(EN)

Dieses Seminar richtet sich an Teilnehmerinnen und Teilnehmer ohne oder mit geringen Vorkenntnissen.

IHR REFERENT

Dr. Detlef Reich, S-Management Services GmbH

HINWEIS(E)

Die Veranstaltung findet im virtuellen Seminarraum der Sparkassenakademie stattfinden. Ihre Zugangsdaten und weitere technische Infos erhalten Sie mit der Einladung zur Veranstaltung.

TERMIN(E)

Auf Anfrage

DAUER

1 Tag

PREIS

490,00 €

KONTAKT

ANMELDUNG



Kristina Barbknecht
0231 22240-728
kristina.barbknecht@ska.nrw

INHALTE



Sabine Berens
0231 22240-740
sabine.berens@ska.nrw

Programm/Inhalt

Verstehen der Organisation und ihres Kontextes

Verstehen der Erfordernisse und Erwartungen interessierter Parteien, um daraus den Anwendungsbereich des ISMS abzuleiten

Aufgaben und Zuständigkeiten des Vorstandes

Informationssicherheitsrisikomanagement

Erforderliche Ressourcen, Kompetenzen, Dokumentation sowie Kommunikation

Betrieb des Informationssicherheitsmanagementsystems

Bewertung und Auditierung des Informationssicherheitsmanagementsystems

Kontinuierliche Verbesserung

Im Rahmen des Seminars wird auf individuelle Fragestellungen der Teilnehmenden eingegangen. Eigene Fallbeispiele können von den Teilnehmenden gerne mit eingebracht werden.

Physische Konzepte im IKT-Risikomanagement und Informationssicherheitsmanagement (online)

Der Geltungsbereich des IKT-Risikomanagementrahmens (IKT-RMR) gemäß dem Digital Operational Resilience Act (DORA) sowie des Informationssicherheits-Managements (ISM) gemäß der ISO 27001 erstreckt sich auf die Gebäude und Standorte der Sparkassen. Alle SITB-Anforderungen müssen im Rahmen des dreijährigen Auditprogramms berücksichtigt werden. Das Seminar gibt einen praxisnahen Überblick über die physischen Konzepte aus der Perspektive des IKT-Risikomanagements sowie der Informationssicherheit.

ZIELGRUPPE

Verantwortliche (Bau-Organisation) von Gebäuden/Räumen (IT-Assets), die sich über die aktuellen regulatorischen Anforderungen informieren wollen, Informationssicherheits-Beauftragte, IKT-Risikokontrollfunktion sowie dezentrale Informationssicherheitskoordinatorinnen und -koordinatoren, die mehr über die physische Sicherheit (gemäß der Physischen Konzepte des SIZ-Produkts "Sicherer IT-Betrieb" im Rahmen des IKT-Risikomanagements und Informationssicherheits-Managements) erfahren möchten, Informationssicherheitsbeauftragte und BC-Beauftragte (Notfallmanagement), die erst seit Kurzem die neue Aufgabe übernommen haben und einen praxisnahen Einstieg und Überblick in das Thema suchen, Auditorinnen und Auditoren, die die physischen Konzepte auditieren und/oder eine IT-Sicherheitsbegehung planen und Revisorinnen und Revisoren vor der Prüfung der physischen Konzepte.

IHR NUTZEN

- Sie lernen die physischen Konzepte sowie interne und externe Anforderungen kennen und können aus den generischen Anforderungen des SIZ-Produkts „Sicherer IT-Betrieb“ wirksame Maßnahmen für die operative Informationssicherheit im Kontext der physischen Konzepte und des IKT-Risikomanagements ableiten.
- Sie werden in die Lage versetzt, die praxisnahe Kontrollen (1st Line) und die Auditierung (2nd Line) oder Prüfungen (3rd Line) der physischen Konzepte durchzuführen.
- Sie profitieren von den Praxiserfahrungen aus zahlreichen sicherheitstechnischen Begehungen in Sparkasse im Zuge szenariobasierter oder vertiefender Audits und kennen viele Impulse für die eigenen Aufgaben.

IHRE REFERENTIN

Mandy Nieke, S-Management Services GmbH

TERMIN(E)

21.10.2027 | virtueller Seminarraum

DAUER

1 Tag

PREIS

520,00 €

KONTAKT

ANMELDUNG



Kristina Barbknecht
0231 22240-728
kristina.barbknecht@ska.nrw

INHALTE



Sabine Berens
0231 22240-740
sabine.berens@ska.nrw

Programm/Inhalt

Die Anforderungen aus dem Digital Operational Resilience Act (DORA) gemäß Artikel 18 RTS RMF für die „physische Sicherheit und Sicherheit vor Umweltereignissen“ sowie aus den Mindestanforderungen an das Risikomanagement (MaRisk) und aktuelle Hinweise aus Prüfungen werden berücksichtigt.

Die Inhalte sind auf die jeweils aktuellen Konzepte des SIZ-Produkts ”Sicherer IT-Betrieb" Module abgestimmt:

- K201 Standort, Gebäude, Räume
- K207 Überschwemmungsschutz
- K202 Schutz gegen Stromausfall
- K203 Blitz-/Überspannungsschutz
- K206 Klimatisierung
- K205 Brandschutz
- K208 Überwachung
- K209 Zutrittsschutz

Zu den Konzepten werden jeweils Lösungsvorschläge aus der Praxis vorgestellt, u. a.

- Berücksichtigung der physischen Konzepte im Auditprogramm
- Abbildung im IKT-Assetmanagement und des Schutzbedarfs
- Fachliche Begründungen zur Schutzbedarfsfeststellung
- Anwendung der generischen SITB-Anforderungen bei unterschiedlichen Arten von Gebäuden und Räumen
- Risikoanalysen von Standorten, Gebäuden und Räumen
- IT-Sicherheitstechnische Begehungen im Rahmen szenariobasierter oder vertiefender Audits, inklusive Bereitstellung von Checklisten etc.

Bonus für die Teilnehmenden

- Hochladen eines individuellen Profils im SITB inkl. Handout
- Checkliste Umsetzung Konzept K209 Zutrittsschutz
- Praxistipps – Brandschutz E-Batterien
- K201 Standortbezogene Risikoermittlung inkl. Anlage
- DORA-Risikoanalyse Art. 26 Abs. 2 c - Ausfall Raum-Gebäude - Beispiel

und vieles mehr (je nach Aktualität der Themen)

ITM-Radar - Protokollierung und Protokollauswertung (online)

Mit dem ITM-Radar lassen sich regulatorische Anforderungen der Bankenaufsicht bewerten und die Prüfungssicherheit durch entsprechende Maßnahmen erhöhen. Im September 2022 wurden über ITM-Radar Protokollauswertungskonzepte unter K110 des Rahmenwerks "Sicherer IT-Betrieb" zur Verfügung gestellt, die auch heute unter der DORA noch aktuell und anwendbar sind.

Hierzu bieten wir dieses halbtägige Seminar an, in dem das Vorgehen erläutert wird.

ZIELGRUPPE

Informationssicherheitsbeauftragte, Mitarbeiter/-innen aus den Bereichen Organisation und IT, IT-Revisorinnen und IT-Revisoren

IHR NUTZEN

- Sie sind über die neu zur Verfügung gestellten Protokollauswertungskonzepte informiert.
- Sie können das Vorgehen der Sicherheitsüberwachung methodisch einordnen.
- Sie kennen den Regelungsbedarf in der Sparkasse.

IHR REFERENT

Sven Lammers, ETL consit GmbH

HINWEIS(E)

Die Veranstaltung findet im virtuellen Seminarraum der Sparkassenakademie statt. Ihre Zugangsdaten und weitere technische Infos erhalten Sie mit der Einladung zum Online-Seminar.

TERMIN(E)

17.02.2027 | virtueller Seminarraum
09:00 – 13:30 Uhr

DAUER

0,5 Tage
0,5 Tage

PREIS

285,00 €

KONTAKT

ANMELDUNG



Kristina Barbknecht
0231 22240-728
kristina.barbknecht@ska.nrw

INHALTE



Sabine Berens
0231 22240-740
sabine.berens@ska.nrw

Programm/Inhalt

Die Unterlagen (Leitfaden, Richtlinie, Tool, Beispiele) werden vorgestellt.

Das Vorgehen der Sicherheitsüberwachung wird methodisch eingeordnet.

Es wird anhand von Beispielen das Vorgehen zur Erstellung der Protokollauswertungskonzepte erläutert.

Der Regelungsbedarf in der Sparkasse wird besprochen.

Operative Informationssicherheit für die 1st-Line

Operative Informationssicherheitsmaßnahmen (operative IS-Maßnahmen) der 1. Verteidigungslinie gewährleisten die grundlegende Sicherheit von Kundeninformationen und finanziellen Transaktionen. Vertiefen Sie Ihr Wissen über den aufsichtsrechtlichen Rahmen, der für die Wahrnehmung Ihrer Aufgaben relevant ist und erhalten Sie praxisnahe Hinweise zur Integration der erforderlichen Tätigkeiten in die Betriebsprozesse für IT und Infrastruktur. Dabei erwerben Sie Kenntnisse im Umgang mit den aktuellen Hilfsmitteln aus dem SIZ-Produkt "Sicherer IT-Betrieb" und dem Wiki IT-Consulting der S-Management-Services GmbH.

ZIELGRUPPE

Mitarbeiter/-innen aus den Bereichen IT, Betriebsorganisation und Gebäudemanagement (Haustechnik), die für die Umsetzung, Pflege und Dokumentation der operativen IS-Maßnahmen (auf Basis der vom Informationssicherheitsmanagement vorgegebenen Sollmaßnahmen) zuständig sind. Informationssicherheitsbeauftragte, die selbst die internen Bereiche bzgl. der Verantwortung schulen und informieren möchten. Dienstleistersteuerer für ausgelagerte Informationssicherheitsbeauftragte. Datenschutzbeauftragte, Innenrevisorinnen und Innenrevisoren, die sich zu diesem Thema informieren möchten, z. B. im Vorfeld von Prüfungen.

IHR NUTZEN

- Sie haben einen Überblick über die Aufgaben und Verantwortlichkeiten der 1st-Line im Rahmen der operativen Informationssicherheit.
- Sie kennen den gesetzlichen und aufsichtsrechtlichen Rahmen zur Umsetzung der operativen Informationssicherheit.
- Sie haben ein Verständnis für die grundsätzlichen Verfahren des SIZ-Produkts „Sicherer IT-Betrieb“ im Bereich der operativen Informationssicherheit.
- Sie sind informiert über die aktuell in der Sparkassenorganisation erarbeiteten und empfohlenen Verfahren zur operativen Informationssicherheit.
- Sie sind vertraut mit praxisnahen Hinweisen zur Integration der Tätigkeiten in Zusammenhang mit der operativen Informationssicherheit in die Betriebsprozesse für IT und Infrastruktur.

REFERENTINNEN UND REFERENTEN

- Gundolf Jahn, S-Management Services GmbH IT-Consultant mit langjährigen Erfahrungen in Sparkassen
- Birgit Heykamps, S-Management Services GmbH

HINWEISE ZUM LERNMATERIAL

Die verwendeten Hilfsmittel und gezeigten Praxisbeispiele werden den Teilnehmenden im Rahmen des Seminars zur Verfügung gestellt.

TERMIN(E)

18.02.2027 – 19.02.2027 |
Sparkassenakademie NRW

22.09.2027 – 23.09.2027 |
Sparkassenakademie NRW

DAUER

2 Tage

PREIS

940,00 €

KONTAKT

ANMELDUNG



Kristina Barbknecht
0231 22240-728
kristina.barbknecht@ska.nrw

INHALTE



Sabine Berens
0231 22240-740
sabine.berens@ska.nrw

Programm/Inhalt

Einordnung/Abgrenzung der operativen Informationssicherheit im Rahmen eines Informationssicherheits-Managementsystems auf Basis der ISO-Norm 27001

Gesetzlicher und aufsichtsrechtlicher Rahmen zur Gewährleistung der Informationssicherheit aus Sicht der 1st lod (MaRisk, DORA)

Verfahren zur Umsetzung operativen Informationssicherheit auf Basis des SIZ Produktes „Sicherer IT-Betrieb“, z.B.

- **Erstellung/Pflege Informationsverbund**
- **Schutzbedarfsfeststellung**
- **Definition und wirksame Umsetzung angemessener operativer IS-Maßnahmen zum Schutz der Elemente des Informationsverbundes**
- **Erkennen und Behandeln von Risiken im Informationsverbund (inkl. Risikoanalyse)**
- **Methoden zum Testen der operativen Informationssicherheit/Sicherheitsüberwachung**
- **Schwachstellenmanagement**
- **Aufgaben der 1st lod bei der Erkennung und Behandlung von IS-Vorfällen**

Vorstellung der aktuellen Hilfsmittel aus dem SITB und dem Wiki IT-Consulting der S-MS

Praxisorientierte Hinweise zur Umsetzung der Aufgaben zur operativen Informationssicherheit im Rahmen der Verfahren des IT-Betriebes

Im Rahmen der Veranstaltung werden individuelle Fragestellungen der Teilnehmer/-innen beantwortet

HINWEISE ZUM INHOUSE-TRAINING

Bei Bedarf kann die Wissensvermittlung auch als Inhouse-Seminar gebucht werden. In diesem Fall können die Referentinnen und Referenten noch besser auf die konkreten Herausforderungen in der Sparkasse eingehen und die jeweiligen Ablaufprozesse zielgerichtet betrachten.

Grundlagen für neue Informationssicherheitsbeauftragte

Für die erfolgreiche Übernahme der wichtigen und komplexen Funktion als Informationssicherheitsbeauftragte/-r sind einige fachliche Inhalte und Kompetenzen erforderlich. Mit diesem Schulungsangebot für Einsteiger/-innen werden dazu die fachlichen, organisatorischen und methodischen Grundlagen vermittelt, damit die erfolgreiche Übernahme und Ausführung der komplexen Funktion "Informationssicherheitsbeauftragte/-r" gemeistert werden kann.

ZIELGRUPPE

Mitarbeiter/-innen, die die Funktion als Informationssicherheitsbeauftragte/-r oder als deren Vertreter/-in neu übernehmen oder übernommen haben

Mitarbeiter/-innen, die einen umfassenden Einblick in das Aufgabengebiet "Informationssicherheitsbeauftragte/-r" erwerben wollen (z. B. Leiter Compliance)

IHR NUTZEN

- Sie wissen, welche verschiedenen Aufgabenbereiche die Funktion des/der Informationssicherheitsbeauftragten beinhalten.
- Sie sind vertraut mit den fachlichen, organisatorischen und methodischen Grundlagen.
- Sie kennen wichtige Bausteine Ihrer Ausbildung.

VORAUSSETZUNG(EN)

Dieses Schulungsangebot richtet sich an Teilnehmer/-innen ohne oder mit geringen Vorkenntnissen.

REFERENTINNEN UND REFERENTEN

- Jürgen Nordmann, S-Management Services GmbH
- Peter Zwack, S-Management Services GmbH

HINWEIS(E)

Teilnehmer/-innen erwerben ein Abschlusszertifikat, welches zum Nachweis der fachlichen Qualifikation verwendet werden kann. Es erfolgt keine Prüfung.

Hinweis auf weiterführende Seminare:

Technische Vertiefung für Informationssicherheitsbeauftragte (Angebotsnummer 46.750)

DORA - Informationssicherheitsbeauftragte (ISB+) im Kontext der IKT-Risikokontrollfunktion (Angebotsnummer 46.763)

TERMIN(E)

12.10.2026 – 01.12.2026 |
Sparkassenakademie NRW

Präsenz-Seminar (12.10. - 16.10.2026)
Erfahrungsaustausch (01.12.2026)

DAUER

6 Tage

PREIS

2.725,00 €

KONTAKT

ANMELDUNG



Kristina Barbknecht
0231 22240-728
kristina.barbknecht@ska.nrw

INHALTE



Sabine Berens
0231 22240-740
sabine.berens@ska.nrw

Programm/Inhalt

Organisatorische Grundlagen der Informationssicherheit

Einordnung in die Regulatorik, wichtige Anforderungen an die Informationssicherheit

Inhalt eines Informationssicherheitsmanagementsystems

Informationsklassifizierung

Strukturanalyse & Schutzbedarfsfeststellung

Sollmaßnahmenkataloge

Planung und Durchführung von Audits

Überblick zum Business Continuity Management

Überblick über die Anforderungen aus dem Auslagerungs- und Vertragsmanagement

Detaillierte Durchsprache aller notwendigen Konzepte des SIZ-Produkts „Sicherer IT-Betrieb" (SITB), u. a. Betriebskonzepte, logisch-technischen Konzepte, physischen Konzepte

Vorstellung weiterer Konzepte aus dem SITB

Informationen zum Ablauf von Prüfungen nach §44 KWG

Vermittlung von erforderlichen, persönlichen Kompetenzen, z.B. Umgang mit schwierigen Situationen und Gesprächspartnern

Aufzeigen von Möglichkeiten zum effizienteren Arbeiten

Im Rahmen des Seminars wird auf individuelle Fragestellungen der Teilnehmenden eingegangen. Eigene Fallbeispiele können von den Teilnehmenden gerne mit eingebracht werden.

Erfolgreiche Auditierung in der Praxis (online)

Wie verlaufen die Planung und die Organisation eines Audits? Welche Anforderungen gibt es? Und wie wird ein Audit durchgeführt? Antworten auf diese Fragen finden Sie in unserem Seminar. Lernen Sie, wie Sie eine erfolgreiche Auditierung umsetzen können.

ZIELGRUPPE

Informationssicherheitsbeauftragte, IT-Revisorinnen und -Revisoren sowie andere Mitarbeiter/-innen, die sich mit der Planung und Durchführung von Audits befassen

IHR NUTZEN

- Sie wissen, wie eine Auditierung von der Planung bis hin zur erfolgreichen Durchführung gelingen kann.
- Sie kennen lösungsorientierte Umsetzungen aus der Praxis.
- Sie haben einen Überblick über die Dokumentationsgrundlagen.

VORAUSSETZUNG(EN)

Grundsätzlich sind keine speziellen Voraussetzungen erforderlich. Eine Affinität zum Thema ist hilfreich.

IHRE REFERENTIN

Maxim Sartison, S-Management Services GmbH

HINWEISE ZUM LERNMATERIAL

Im Rahmen des Seminars werden viele Informationsquellen bereitgestellt.

TERMIN(E)

12.04.2027 | virtueller Seminarraum

DAUER

1 Tag

PREIS

580,00 €

KONTAKT

ANMELDUNG



Kristina Barbknecht
0231 22240-728
kristina.barbknecht@ska.nrw

INHALTE



Sabine Berens
0231 22240-740
sabine.berens@ska.nrw

Programm/Inhalt

Anforderungen an eine Auditierung

Planung und Organisation eines Audits

Wie gestalte ich das Audit?

Wie führe ich ein Audit als ISB durch?

Welche Dokumentationsgrundlagen gibt es?

In welchem Umfang müssen Stichproben gezogen werden und wo dokumentiere ich diese?

Methoden im IKT-Risiko- und Informationssicherheitsmanagement erfolgreich umsetzen

Das Seminar vermittelt Ihnen einen umfassenden Überblick über die Methoden und Verfahren im IKT-Risikomanagement gemäß DORA. Sie lernen die aktuellen Anforderungen an die Verfahren in den ISMS, ISRM, BCM und ITSCM kennen und erhalten konkrete Umsetzungshinweise. Zudem werden Ihnen die relevanten Themen wie IKT-Assetmanagement, Risikoanalyse, Digital Resilience Testing und IKT-Vorfallmanagement praxisnah vermittelt.

ZIELGRUPPE

Informationssicherheitsbeauftragte, Notfallbeauftragte, IKT-Risikomanager/-innen, Revisoren/-innen sowie Methoden-/Prozessverantwortliche der 1st-Line (bei Bedarf)

IHR NUTZEN

- Sie kennen die Anforderungen und Entwicklungen im IKT-Risikomanagement.
- Sie können die Methoden und Verfahren in der Praxis erfolgreich umsetzen.
- Sie sind vertraut mit den aktuellen Hilfsmitteln und Instrumenten (DSGV, PPS und SITB).
- Sie gewinnen einen Überblick über die Änderungen und können diese in Ihrer Sparkasse anwenden.

VORAUSSETZUNG(EN)

Kenntnisse der Verfahren, der in den Sparkassen eingesetzten Managementsysteme (ISM, IKT-Risikomanagement, BCM), Kenntnisse über die Anforderungen als ISB+

REFERENTINNEN UND REFERENTEN

- Gundolf Jahn, S-Management Services GmbH IT-Consultant mit langjährigen Erfahrungen in Sparkassen
- Birgit Heykamps, S-Management Services GmbH

HINWEIS(E)

Abgrenzung: Auf die Umsetzung in den gängigen Tools wird vereinzelt Bezug genommen. Es erfolgt keine Detailschulung. IKT-Drittparteienrisikomanagement wird in diesem Seminar nicht behandelt.

TERMIN(E)

04.05.2027 – 05.05.2027 |
Sparkassenakademie NRW

18.10.2027 – 19.10.2027 |
Sparkassenakademie NRW

DAUER

1,5 Tage

PREIS

940,00 €

KONTAKT

ANMELDUNG



Kristina Barbknecht
0231 22240-728
kristina.barbknecht@ska.nrw

INHALTE



Sabine Berens
0231 22240-740
sabine.berens@ska.nrw

Programm/Inhalt

Die Inhalte werden an die weiteren Entwicklungen des DSGV-DORA-Projektes, die Ergebnisse aus PPS 2.0 sowie die Fortschreibung des Rahmenwerkes SITB angepasst.

DORA bringt neue geänderte Anforderungen an die Verfahren in den ISMS, ISRM, BCM, ITSCM, zum Beispiel:

- Strategieprozess
- Klassifizierung kritischer und wichtiger Funktionen
- Überwachung der Ziele anhand von Kennzahlen
- Überprüfung IKT-Risikomanagementrahmen
- IKT-Assetmanagement
- Risikoanalyse und -behandlung
- Testen der digitalen Resilienz
- Berichtswesen: Bericht zur Überprüfung des IKT-Managementrahmens, IKT- Risikobericht etc.
- IKT-Vorfallmanagement
- Schulung und Sensibilisierung
- Kommunikationsstrategie

Überblick über Änderungen

Darstellung der Verfahren

Umsetzungshinweise, aktuelle Hilfsmittel (DSGV-Instrumente, PPS, SITB)

Vorfallmanagement - Umgang mit IKT-Vorfällen gemäß DORA (online)

In einer zunehmend digitalisierten Welt ist der richtige Umgang mit IKT-Vorfällen von zentraler Bedeutung. Unser Online-Seminar vermittelt ein vertiefendes Verständnis der Anforderungen des Digital Operational Resilience Acts (DORA) sowie der einschlägigen Vorgaben der BaFin im Hinblick auf den sachgerechten Umgang mit IKT-Störungen bzw. (schwerwiegenden) IKT-bezogenen Vorfällen und zahlungsbezogenen Betriebs- oder Sicherheitsvorfälle sowie Cyberbedrohungen. Im Mittelpunkt stehen Definition, Klassifikation, Erkennung, Behandlung und Meldung der schwerwiegenden IKT-bezogenen Vorfälle sowie die Ausgestaltung wirksamer Prozesse (PPS-PLK) in Übereinstimmung mit den regulatorischen Erwartungen.

ZIELGRUPPE

Informationssicherheitsbeauftragte, Mitarbeitende mit IKT-Risikokontrollfunktion, Informationssicherheitskoordinatorinnen und -koordinatoren, IT-Revisorinnen und -revisoren sowie IT-Verantwortliche (operative Informationssicherheit)

IHR NUTZEN

- Sie kennen die wesentlichen Anforderungen des Digital Operational Resilience Acts (DORA) und deren praktische Umsetzung im Umgang mit IKT-Vorfällen.
- Sie können Vorfälle nach DORA-Kriterien definieren, klassifizieren und gezielt überwachend erkennen.
- Sie sind vertraut mit effektiven Prozessen sowie den relevanten Berichtspflichten und verstehen die Schnittstellen zu anderen Bereichen wie dem Notfallmanagement.

IHRE REFERENTIN

Mandy Nieke, S-Management Services GmbH

HINWEIS(E)

Die Veranstaltung findet im virtuellen Seminarraum der Akademie statt. Ihre Zugangsdaten und weitere Informationen erhalten Sie ca. 2 Wochen vor dem Termin mit der Einladung.

TERMIN(E)

25.11.2026 | virtueller Seminarraum
13:30 – 17:00 Uhr

DAUER

0,5 Tage

PREIS

380,00 €

KONTAKT

ANMELDUNG



Kristina Barbknecht
0231 22240-728
kristina.barbknecht@ska.nrw

INHALTE



Sabine Berens
0231 22240-740
sabine.berens@ska.nrw

Programm/Inhalt

Einführung und regulatorische Rahmenbedingungen (DORA, BaFin)

Definitionen und Klassifikation von Vorfällen (DORA-Kriterien)

Erkennung und Überwachung von Vorfällen (IKT-bezogene Vorfälle und Informationssicherheitsvorfälle)

Abstimmung mit IKT-Dienstleistern, u. a. FI-aggregierte Meldungen

Incident-Management und Problem-Management (Prozesse, Verantwortlichkeiten)

Meldewesen und Berichtspflichten (Meldeportale: MVP-Portal, DMA-Anwendung der FI)

Meldung nach der Anzeigenverordnung

Schnittstelle Notfallmanagement (z. B. Cyberangriff, Krisenkommunikation)

Praxisbeispiele, Umsetzungshilfen

Maßnahmen für kritische oder wichtige Funktionen in der Praxis (online)

Die Anforderungen zur Identifikation „kritischer oder wichtiger Funktionen", welche aufgrund der Art, des Umfangs und der Komplexität ihrer Tätigkeit kritisch oder wichtig sind (gemäß Art. 3 Abs. 22 DORA), stellen die Sparkassen vor erhebliche fachliche und organisatorische Herausforderungen. Das Seminar behandelt die anstehenden kurz- bis mittelfristigen Maßnahmen zur Umsetzung der Anforderungen an kritische oder wichtige Funktionen im Kontext von DORA.

ZIELGRUPPE

Mitarbeiter/-innen mit IKT-Risikokontrollfunktion, Informationssicherheitsbeauftragte, Notfall-/BCM-Beauftragte, Leiter/-innen Beauftragtenwesen, Leiter/-innen (IT-) Organisation, zentrales Auslagerungsmanagement, Revision

IHR NUTZEN

- Sie haben ein methodisches Wissen zur Identifikation kritischer oder wichtiger Funktionen (kowF).
- Sie können quantitative und qualitative Kriterien praxisorientiert verbinden und in bestehende Prozesse integrieren.
- Sie sind vertraut mit den notwendigen Anpassungen im GRC-Tool, der Dokumentation und den Folgeaktivitäten.

REFERENTINNEN UND REFERENTEN

Mitarbeiter/-in der SIZ GmbH

TERMIN(E)

Auf Anfrage

DAUER

1 Tag

PREIS

355,00 €

KONTAKT

ANMELDUNG



Kristina Barbknecht
0231 22240-728
kristina.barbknecht@ska.nrw

INHALTE



Sabine Berens
0231 22240-740
sabine.berens@ska.nrw

Programm/Inhalt

Überblick der Weiterentwicklung der Methodik

Wissensvermittlung in der Informationssicherheit und IKT-Risikomanagement zu den Themen

- Anpassung im GRC-Tool (Kennzeichnung kowF)
- Identifikation aller relevanten Assets und IKT-Dienstleistungen
- Kommunikation der Änderungen im Quartals- und Jahresbericht zum IKT-Risikomanagementrahmen
- Anpassung des Testprogramms/Schwachstellenscans
- Diskussion praxisbezogener Fragestellungen

Wissensvermittlung in dem Business Continuity Management/Notfallmanagement zu den Themen

- Fachliche Herausforderungen bei der anlassbezogenen Business Impact Analyse (BIA)
- IKT-Notfallpläne für jede neue identifizierte kowF
- Anlassbezogene Überprüfung und Anpassung der Notfallübungsplanung
- Diskussion praxisbezogener Fragestellungen

Wissensvermittlung im IKT-Drittparteienmanagement zu den Themen

- Neubewertung gem. Risikoermittlung DLB u. a. daraus folgend Anpassung vertraglicher Regelungen (IKT-Sicherheitsanforderungen), Erstellung Exitstrategien, Aufnahme Unterauftragnehmer ins Informationsregister
- Übermittlung der neuen kowF sowie daraus abgeleiteten IKT-DL an die BaFin (Anzeigepflicht)
- Diskussion praxisbezogener Fragestellungen

Praxis-Workshop - Methodik zur Ermittlung kritischer oder wichtiger Funktionen (kowF) (online)

Dieser praxisorientierte Workshop vermittelt Ihnen die bewährte Methodik zur Identifikation und Bewertung kritischer oder wichtiger Funktionen (kowF) gemäß dem SIZ-Leitfaden. Durch die Kombination aus theoretischem Wissen und praktischen Übungen erlangen Sie die Fähigkeiten, diese Methodik effektiv und nachvollziehbar in Ihrer Sparkasse anzuwenden.

ZIELGRUPPE

Notfallbeauftragte/Business-Continuity-Beauftragte, Prozessverantwortliche, Mitarbeiter/-innen mit IKT-Risikokontrollfunktion

IHR NUTZEN

- Sie sind vertraut mit der Bedeutung von kritischen oder wichtigen Funktionen im Kontext des Business Continuity Management (BCM) und können deren Rolle im BCM klar einordnen.
- Sie können kritische oder wichtige Funktionen eindeutig kennzeichnen, nachvollziehbar dokumentieren und in bestehende BCM-Prozesse integrieren.
- Sie sind in der Lage, aktuelle Anforderungen aus DORA, KWG und MaRisk (inkl. relevanter Prüfungshinweise) in Ihre Vorgehensweise einzubeziehen.

IHR REFERENT

Moritz Schumann, S-Management Services GmbH

HINWEIS(E)

Der Workshop berücksichtigt stets die aktuellen Anforderungen aus der DORA-Verordnung, dem Gesetz über das Kreditwesen (KWG) sowie den Mindestanforderungen an das Risikomanagement (MaRisk) und integriert wertvolle Hinweise aus aktuellen Prüfungen. Dabei werden die Inhalte kontinuierlich an aktuelle regulatorische Entwicklungen und Praxiserfahrungen angepasst.

Die Veranstaltung findet im virtuellen Seminarraum der Sparkassenakademie statt. Ihre Zugangsdaten und weitere technische Infos erhalten Sie mit der Einladung zum Online-Seminar.

TERMIN(E)

05.03.2027 | virtueller Seminarraum
09:00 – 12:30 Uhr

03.09.2027 | virtueller Seminarraum
09:00 – 12:30 Uhr

DAUER

0,5 Tage

PREIS

340,00 €

KONTAKT

ANMELDUNG



Kristina Barbknecht
0231 22240-728
kristina.barbknecht@ska.nrw

INHALTE



Sabine Berens
0231 22240-740
sabine.berens@ska.nrw

Programm/Inhalt

Einführung und Grundlagen der Methode zur Ermittlung von kowF

- Verständnis der Bedeutung von kowF im Kontext des Business Continuity Managements
- Grundlagen und Rahmenwerke der kowF-Ermittlung

Datenquellen und die 3-Phasen-Methode zur Ermittlung der kowF

- Identifikation relevanter Datenquellen für die kowF-Analyse
- Detaillierte Erläuterung und Anwendung der dreistufigen Methodik zur Ermittlung

Kennzeichnung und Implementierung der kowF

- Methoden zur eindeutigen Kennzeichnung und Dokumentation von kowF
- Strategien zur Integration der ermittelten kowF in bestehende BCM-Prozesse

Praktische Übungen

- Fallstudien und Gruppenarbeiten zur direkten Anwendung der gelernten Methodik
- Austausch von Best Practices und Lösungsansätzen

Fragen und Antworten/Zusammenfassung

- Individuelle Klärung von Fragen und Herausforderungen
- Zusammenfassung der wichtigsten Erkenntnisse und Handlungsempfehlungen

Business-Impact-Analyse (BIA): Grundlagen verstehen, Praxis beherrschen und erfolgreich implementieren (online)

Sie entwickeln ein fundiertes Verständnis der Business-Impact-Analyse (BIA) und erwerben die Fähigkeiten, diese eigenständig durchzuführen sowie erste Implementierungsschritte in Ihrer Organisation einzuleiten. Das Seminar vermittelt praxisnahes Wissen zur Business-Impact-Analyse unter Berücksichtigung aktueller regulatorischer Anforderungen und bewährter Praktiken.

ZIELGRUPPE

Notfallbeauftragte/Business-Continuity-Beauftragte, Prozessverantwortliche, Mitarbeiter/-innen mit IKT-Risikokontrollfunktion

IHR NUTZEN

- Sie kennen Zweck, Stellenwert und Einsatzfelder der Business-Impact-Analyse im Rahmen des Business Continuity Managements (BCM).
- Sie können eine Business-Impact-Analyse nach einem klaren Vorgehensmodell planen, Daten erheben und kritische Geschäftsprozesse systematisch analysieren.
- Sie sind vertraut mit der Interpretation von BIA-Ergebnissen und deren Nutzung für Wiederherstellungsziele sowie geeignete Wiederherstellungsstrategien.

VORAUSSETZUNG(EN)

Erfahrungen mit und Kenntnisse von BCM-Prozessen

IHR REFERENT

Moritz Schumann, S-Management Services GmbH

HINWEIS(E)

Die Inhalte spiegeln stets die Anforderungen der DORA-Verordnung, des Gesetzes über das Kreditwesen (KWG) und der Mindestanforderungen an das Risikomanagement (MaRisk) wider, ergänzt durch relevante Hinweise aus Prüfungen.

Die Veranstaltung findet im virtuellen Seminarraum der Sparkassenakademie statt. Ihre Zugangsdaten und weitere technische Infos erhalten Sie mit der Einladung zum Online-Seminar.

TERMIN(E)

15.10.2027 | virtueller Seminarraum
09:00 – 12:30 Uhr

DAUER

0,5 Tage

PREIS

320,00 €

KONTAKT

ANMELDUNG



Kristina Barbknecht
0231 22240-728
kristina.barbknecht@ska.nrw

INHALTE



Sabine Berens
0231 22240-740
sabine.berens@ska.nrw

Programm/Inhalt

Einführung in die Grundlagen der BIA
Verständnis der Bedeutung und des Zwecks der BIA im Rahmen des Business Continuity Managements

Methodik und Durchführung einer BIA
Schritt-für-Schritt-Anleitung zur Planung, Datenerhebung und Analyse kritischer Geschäftsprozesse

Ergebnisse und Nutzung der BIA
Interpretation der BIA-Ergebnisse und deren Anwendung zur Festlegung von Wiederherstellungszielen und -strategien

Praktische Übung
Anwendung des Gelernten anhand eines realitätsnahen Fallbeispiels

Fragen/Antworten/Zusammenfassung
Klärung offener Punkte und Konsolidierung der wichtigsten Erkenntnisse

Praxis-Workshop: Effektive Notfallübungen – Wissen und Handwerkszeug für Notfälle (online)

Nach Abschluss dieses Workshops sind Sie in der Lage, Notfallübungen professionell zu konzipieren, umzusetzen und systematisch auszuwerten. Sie erlangen die Kompetenz, Übungsergebnisse für die nachhaltige Weiterentwicklung und Optimierung ihrer BCM-Prozesse zu nutzen und somit die Widerstandsfähigkeit ihrer Organisation signifikant zu stärken.

ZIELGRUPPE

Notfallbeauftragte/Business-Continuity-Beauftragte, Krisenstabsmitglieder, Prozessverantwortliche, Ressourcenverantwortliche

IHR NUTZEN

- Sie können Notfallübungen zielgerichtet konzipieren – inklusive Szenarienentwicklung, Rollenklärung und Erstellung der Übungsunterlagen.
- Sie sind vertraut mit einer professionellen Durchführung und Beobachtung sowie einer belastbaren Dokumentation von Ereignissen und Entscheidungen.
- Sie können Ergebnisse strukturiert auswerten und konkrete Maßnahmen ableiten, um Ihre Notfallvorsorge kontinuierlich zu verbessern.

VORAUSSETZUNG(EN)

Erfahrungen mit und Kenntnisse von BCM-Prozessen

HINWEIS(E)

Die Veranstaltung findet im virtuellen Seminarraum der Sparkassenakademie statt. Ihre Zugangsdaten und weitere technische Infos erhalten Sie mit der Einladung zum Online-Seminar.

HINWEISE ZUM LERNMATERIAL

Dieser interaktive Praxis-Workshop vermittelt Ihnen das notwendige Wissen und das praktische Handwerkszeug, um Notfallübungen im Business Continuity Management (BCM) effektiv zu planen, durchzuführen und die gewonnenen Erkenntnisse für eine kontinuierliche Verbesserung Ihrer Notfallvorsorge zu nutzen. Die Inhalte sind stets auf dem neuesten Stand und berücksichtigen relevante Anforderungen aus der DORA-Verordnung, dem Gesetz über das Kreditwesen (KWG) sowie den Mindestanforderungen an das Risikomanagement (MaRisk) und aktuelle Hinweise aus Prüfungen.

TERMIN(E)

04.10.2027 | virtueller Seminarraum
09:00 – 12:30 Uhr

DAUER

0,5 Tage

PREIS

340,00 €

KONTAKT

ANMELDUNG



Kristina Barbknecht
0231 22240-728
kristina.barbknecht@ska.nrw

INHALTE



Sabine Berens
0231 22240-740
sabine.berens@ska.nrw

Programm/Inhalt

Einführung und Grundlagen für Notfallübungen
Bedeutung und Arten von Notfallübungen, regulatorische Anforderungen und Best Practices

Planung und Vorbereitung einer Notfallübung
Definition von Übungszielen, Szenarienentwicklung, Rollen und Verantwortlichkeiten, Erstellung von Übungsunterlagen

Durchführung und Beobachtung der Notfallübung
Steuerung des Übungsverlaufs, Rolle des Beobachters, Dokumentation von Ereignissen und Entscheidungen

Auswertung und "Lessons Learned"
Systematische Analyse der Übungsergebnisse, Identifizierung von Stärken und Schwächen, Entwicklung konkreter Maßnahmen zur Verbesserung

Fragen/Antworten/Zusammenfassung
Raum für individuelle Fragen und Diskussionen, Festigung der wichtigsten Erkenntnisse



DIE BUSINESS SCHOOL

Zertifizierte Weiterbildung zum Fach- oder Betriebswirt

Die Business School bietet zertifizierte Weiterbildungen zu Fach- oder Betriebswirten an. 100 % online und gleichzeitig persönlich betreut. Flexibel nach Deinen Wünschen, berufsbegleitend und europaweit auf Bachelor- und Master-Programme anrechenbar. Als Label der Sparkassenakademien Nordrhein-Westfalen verfügen wir über fundierte Erfahrungen in der Aus- und Weiterbildung – über 5.000 zufriedene Teilnehmerinnen und Teilnehmer haben mit uns schon ihre beruflichen Perspektiven verbessert.

Informiere Dich über unsere berufsbegleitenden Weiterbildungsangebote.

IHRE ANSPRECHPARTNER/-INNEN



Rabea Hesse
Bildungsberaterin Business School

0231 22240-712
bs@ska.nrw



Nathalie Mädje
Bildungsberaterin Business School

0231 22240-757
bs@ska.nrw



Liane Stach
Bildungsberaterin Business School

0231 22240-792
bs@ska.nrw



Laura Freiin von Eerde
Bildungsberaterin Business School

0231 22240-795
bs@ska.nrw



TAGUNGSZENTRUM HÖRDER BURG

Ob in Präsenz, digital oder hybrid: Mieten Sie unsere Räume für Ihre Veranstaltung

Kongress, Besprechung, Seminar, Workshop oder eigene Schulung für die Mitarbeitenden? Wir bieten Ihnen den passenden Raum für Ihre Veranstaltung.

Sie planen eine Online-Veranstaltung durchzuführen? Mit uns haben Sie den richtigen Partner an Ihrer Seite: Unsere digitalen Räume und hausinternes Studio bieten Ihnen die optimale Basis für Ihre digitale Veranstaltung. On top übernehmen wir für Sie auf Wunsch die professionelle Begleitung Ihrer Veranstaltung durch „Co-Moderatoren“, die Schulung Ihrer Dozenten, das gesamte Teilnehmermanagement, die inhaltliche Konzeption Ihrer Veranstaltung und vieles mehr.

Für Veranstaltungen in Präsenz erwarten Sie in dem exklusiven Gebäudeensemble der Hörder Burg mit direktem Seeblick über 40 hochmoderne Seminar- und Tagungsräume mit einmaligem Flair. Ein auf Ihre Bedürfnisse abgestimmtes Catering sowie hochprofessionelle Organisationsabläufe und maßgeschneiderte Rahmenprogramme runden unser Angebot perfekt ab.

Gern kombinieren wir auch das Raumangebot für Sie und führen Ihre Veranstaltung hybrid durch. Dabei ist ein Teil des Publikums physisch vor Ort, die weiteren Teilnehmer sind digital hinzugeschaltet. Der Vorteil: Das Online-Publikum wird aktiv in die Präsenz-Veranstaltung mit einbezogen und alle Teilnehmenden können in Echtzeit miteinander interagieren und in Kontakt treten.

Haben wir Ihr Interesse geweckt?

Unser Veranstaltungsmanagement berät Sie gern persönlich zu Ihrem individuellen Angebot.

IHRE ANSPRECHPARTNER/-INNEN



Antonia König
Veranstaltungsmanagement

0231 22240-744
antonia.koenig@ska.nrw



Andreas Gaida
Veranstaltungsmanagement

0231 22240-722
andreas.gaida@ska.nrw



MITTELSTANDSCAMPUS NRW

Der Mittelstand bildet das Herz der deutschen Wirtschaft

Der MittelstandsCampus NRW, eine Marke der Sparkassenakademie NRW, bietet mittelständischen Unternehmen vielfältige Bildungsangebote und Inhouse-Beratungen für zentrale Themen an, wie zum Beispiel:

· Nachhaltigkeit,
· Digitalisierung und
· Arbeitgeberattraktivität – Führung.

Ein exklusives Kooperationsnetzwerk, beispielsweise mit der Universität Witten/Herdecke oder der Hochschule für Finanzwirtschaft und Management, sichert zusammen mit unserer fundierten Erfahrung die Qualität der hochwertigen sowie einzigartigen Workshops, Bildungsformate und Beratungsleistungen.

Neben unseren digitalen Veranstaltungen begrüßen wir Sie und Ihre Mitarbeiter/-innen zudem in unserem Tagungszentrum Hörder Burg in einem einmaligen Ambiente. Von unserer rund 700 Jahre alten „Burg“ haben Sie einen direkten Blick auf den Phoenix See in Dortmund. Ein Ort, der wie kein anderer für Transformation und Zukunftsfähigkeit steht.

IHR ANSPRECHPARTNER



Christian Overhage
Projektleiter Mittelstandscampus NRW

0231 22240-717
christian.
overhage@mittelstandscampus-
nrw.de

Lern- und Buchungsportal

Informieren Sie sich über unser Bildungsangebot.

Digitale Transformation