Sparkassenakademie
Nordrhein-Westfalen

FORTBILDUNGSPROGRAMM 2026

IT-Sicherheit

INHALTSVERZEICHNIS

SEITE

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

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.

BCM praxisnah: Basis und Grundlagen

Die Bankenaufsicht stellt hohe Anforderungen an das BCM der Sparkassen. Doch was sind die grundlegenden und wesentlichen Prozesse des Notfallmanagements? Wann ist ein Ereignis ein Störfall, ein Notfall oder eine Katastrophe? Antworten auf diese und weitere Fragen erhalten Sie in diesem Seminar.

ZIELGRUPPE

Notfallbeauftragte und Vertretungen, die erst kurz im Amt sind oder das Amt übernehmen

Informationssicherheitsbeauftragte, die die Grundlagen der Prozesse zum Business Continuity Management (BCM) kennenlernen möchten

Umsetzungsverantwortliche für ein BCM-Projekt (auch Aktualisierungsprojekte)

Vertretung des/der Notfallbeauftragten (qualifizierte/r Vertreter/-in wird benötigt)

Revisorinnen und Revisoren der Innenrevision für einen Überblick, z. B. vor und während der Prüfung

IHR NUTZEN

- Sie kennen die grundlegenden und wesentlichen Prozesse des Notfallmanagements /Business Continuity Management (BCM) sowie die jeweils aktuellen externen Anforderungen (DORA, KWG, MaRisk) an das BCM und verstehen diese.
- Sie wissen, wie konkrete Fallbeispiele in der Praxis lösungsorientiert umgesetzt werden.

VORAUSSETZUNG(EN)

Grundsätzlich sind keine speziellen Voraussetzungen erforderlich. Eine Affinität zum Thema wäre allerdings hilfreich.
Hinweis: Für alle „Neueinsteiger“ in das Thema ist dieses Grundlagen-Seminar bestens geeignet oder zur Auffrischung empfohlen, sowie um sich auf das nachfolgende 2-tägige Seminar „BCM Praxisnah - Aufbauseminar" (Angebotsnummer 46.755) vorzubereiten.

IHR REFERENT

Moritz Schumann, S-Management Services GmbH

HINWEISE ZUM LERNMATERIAL

Im Rahmen des Seminars werden viele Informationsquellen bereitgestellt.

TERMIN(E)

Auf Anfrage

DAUER

2 Tage

PREIS

470,00 €

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 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.

Überblick über alle Begriffe zum Business Continuity Management

Gesetzliche und regulatorische Anforderungen

IKT-Geschäftsfortführungsleitlinie und Ziele im Kontext der eigenen und externen Anforderungen

Initiierung der Aufbauorganisation, Rollen und Aufgaben des ganzheitlichen Business Continuity Managements

Business Impact Analyse (BIA) Prozess definieren und durchführen

Risiko Impact Analyse (RIA) Prozess definieren und durchführen

Relevante Szenarien für kritische oder wichtige Funktionen (Prozesse)

Relevante Szenarien für IKT-Reaktion-/Wiederherstellungspläne einschließlich schwerer Betriebsunterbrechungen

Geschäftsfortführungs- sowie Wiederanlaufpläne und Wiederherstellungspläne

Übungsplanung und Notfallübungen für Geschäftsfortführungspläne und IKT-Reaktion-/Wiederherstellungspläne

Schulung- und Sensibilisierung von BCM-Themen

Berichtswesen definieren und Berichte erstellen

Erfahrungsaustausch Notfallmanagement (BCM) (online)

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 und Kenntnisse von BCM-Prozessen als Notfallbeauftragte/-r oder Vertreter/-in sowie IT-Revisor/-in.

Die Affinität zum Thema BCM und Notfallplanung ist hilfreich.

IHR REFERENT

Peter Schwarz, S-Management Services GmbH

HINWEIS(E)

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

TERMIN(E)

Auf Anfrage

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) sowie 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)

13.10.2026 | 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, Leiter/-innen IT, Leiter/-innen Organisation, IT-Revisoren/-innen

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)

28.09.2026 | 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:

- IT-Strategie
- IT-Governance
- Informationsrisikomanagement
- Informationssicherheitsmanagement
- Benutzerberechtigungsmanagement
- IT-Projekte und Anwendungsentwicklung
- IT-Betrieb
- Auslagerung und sonstiger Fremdbezug von IT- Dienstleistungen
- Notfallmanagement
- Cybersicherheit

BCM-Notfallmanagement: Grundlagen für Notfallbeauftragte

In diesem Seminar werden grundlegende und wesentliche Prozesse des Notfallmanagements (BCM) sowie die externen Anforderungen an das BCM beleuchtet. Durch Diskussion der einzelnen Themen werden weitere Umsetzungen aus der Praxis aufgezeigt.

ZIELGRUPPE

Notfallbeauftragte (BC-Beauftragte), die mehr über die Methoden zur Aufrechterhaltung des BCM sowie die Anforderungen erfahren möchten

Notfallbeauftragte, die erst kurz im Amt sind oder das Amt übernehmen (Hinweis: Das Seminar „BCM praxisnah: Basis und Grundlagen“ ist vorab zu empfehlen)

Vertretungen des/der Notfallbeauftragten: In der Praxis wird eine qualifizierte Vertretung benötigt

Etablierte Notfallbeauftragte, die die Möglichkeit zur Verbesserung der eigenen BCM-Prozesse, Aufgaben und etablierten BCM-Prozesse zur Aufrechterhaltung des BCM suchen (schlanke Prozesse)

Umsetzungsverantwortliche für ein BCM-Projekt (auch Aktualisierungsprojekte)

Innenrevisorinnen und -revisoren zur Vertiefung der BCM-Themenfelder vor und während der Prüfung. (Es werden viele Hinweise aus Prüfungen gegeben.)

IHR NUTZEN

- Sie sind über die externen Anforderungen (DORA, KWG, MaRisk) und Standards (u.a. Bundesamt für Sicherheit in der Informationstechnik und ISO-Normen) informiert.
- Sie kennen Methoden zur Aufrechterhaltung eines Business Continuity Managements und können eigene BCM-Prozesse und Abläufe verbessern.
- Sie können die Nachvollziehbarkeit der Notfallplanung und des BCM sicherstellen.

VORAUSSETZUNG(EN)

Grundsätzlich sind keine speziellen Voraussetzungen erforderlich. Eine Affinität zum Thema wäre allerdings hilfreich.
Hinweis: Für alle „Neueinsteiger“ in das Thema und zur Auffrischung des Themas ist das Seminar "BCM - Notfallmanagement: Basis und Grundlagen (online)" (**Angebotsnummer 46.754**) vorab empfohlen.

IHR REFERENT

Moritz Schumann, S-Management Services GmbH

HINWEIS(E)

Im Seminar werden Tools zum BCM nicht explizit behandelt.

HINWEISE ZUM LERNMATERIAL

TERMIN(E)

Auf Anfrage

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

Im Rahmen des Seminars werden aktuelle und wertvolle Informationsquellen für das BCM bereitgestellt. Eine bereitgestellte Checkliste ermöglicht die Durchführung eines vertiefenden Audits oder einer Prüfung des BCM / Notfallmanagements.

Programm/Inhalt

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.

Externe Anforderungen (DORA, KWG, MaRisk) und Standards (u.a. Bundesamt für Sicherheit in der Informationstechnik und ISO-Normen)

Notfalldefinitionen, Abgrenzung Störung, Notfall, Krise anhand von Praxisbeispielen

IKT-Geschäftsfortführungsleitlinie, Ziele sowie Kennzahlen im Kontext der eigenen und externen Anforderungen auf Basis von Praxisbeispielen

Aufbauorganisation, Rollen und Aufgaben des ganzheitlichen Business Continuity Managements

Business Impact Analyse (BIA) Prozess definieren, durchführen und Praxisbeispiele aus Sparkassen

Risiko Impact Analyse (RIA) Prozess definieren, durchführen und Praxisbeispiele, u.a. RTO vs. RTA im Kontext des IKT-Risikomanagements

Relevante Szenarien für kritische oder wichtige Funktionen (Prozesse)

Relevante Szenarien für IKT-Reaktion-/Wiederherstellungspläne einschließlich schwerer Betriebsunterbrechungen

Geschäftsfortführungs- sowie Wiederanlaufpläne und Wiederherstellungspläne

Übungsplanung und Notfallübungen für Geschäftsfortführungspläne und IKT-Reaktion-/Wiederherstellungspläne (u.a. IT-Notfall, Cyber-Angriff)

Maßnahmen zur Aufrechterhaltung der Informationssicherheit im Notfall (Praxisbeispiele)

Praxisbeispiele für Übungen, relevante Übungsarten und Szenarien für kritische oder wichtige Funktionen (Prozesse) sowie für Mindestszenarien (DORA) planen, vorbereiten, durchführen, dokumentieren, bewerten und berichten

Schulung- und Sensibilisierung von BCM-Themen

Unabhängige Auditierung des BCM und Umgang mit Schwachstellen / Risiken sowie Schnittstelle zum IKT-Risikomanagement

Relevante Schnittstellen zur erforderlichen Abstimmung

Krisenkommunikation, Kommunikations- und Krisenmanagementmaßnahmen

Praxisbeispiel für eine Sitzung des Krisenstabs und Möglichkeiten für eine Alarmierungsübung

Berichtswesen zum BCM definieren, Berichte erstellen, Schnittstelle zum IKT-Risikomanagement

Mindestinhalte des Notfallmanagements / Notfallhandbuchs definieren, aktualisieren, bereitstellen etc.

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)

08.09.2026 | virtueller Seminarraum

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.

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 neue Protokollauswertungskonzepte zur Verfügung gestellt, unter anderem gemäß K110 des Rahmenwerks "Sicherer IT-Betrieb".

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)

Auf Anfrage

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)

03.09.2026 – 04.09.2026 |
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.

IT-Compliance für die 1st-Line (inkl. DORA)

IT-Compliance stellt Sparkassen vor große Herausforderungen. Als Prozessverantwortliche/-r sind Sie unter anderem für die Einhaltung der IT-Compliance verantwortlich. In unserem Seminar lernen Sie alles, um der Verantwortung und den Aufgaben von Prozessverantwortlichen gerecht zu werden. Dabei werden die Hintergründe in Verbindung mit der IT-Compliance und den operationellen Risiken vertieft.

ZIELGRUPPE

Prozess- und Fachverantwortliche, die für Schutzbedarfsfeststellung, Business Impact Analysen, Risikoanalysen, Kontrollen etc. verantwortlich sind, Beauftragte der 2. Verteidigungslinie, die selbst die Prozessverantwortlichen zu diesen Themen schulen möchten bzw. sensibilisieren möchten und Innenrevisorinnen und Innenrevisoren, die sich zu diesem Thema informieren möchten, z. B. im Vorfeld von Prüfungen

IHR NUTZEN

- Sie sind über die relevanten gesetzlichen und regulatorischen Anforderungen informiert.
- Sie sind vertraut mit den Aufgaben und der Verantwortung einer/eines Prozessverantwortlichen.
- Sie kennen die aktuellen Hilfsmittel.

IHR REFERENT

Rainer Autenrieth, S-Management Services GmbH

TERMIN(E)

Auf Anfrage

DAUER

1 Tag

PREIS

510,00 €

KONTAKT

ANMELDUNG

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

INHALTE

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

Programm/Inhalt

Vorstellung und Erläuterung der relevanten gesetzlichen, regulatorischen und normativen Anforderungen

Rollen und Funktionen aus dem 3 Linienmodell des DIIR (Deutsches Institut für Interne Revision e.V.)

Zusammenspiel von (operationellem) Risikomanagement und IKS

Schnittstellen und Aufgaben im kontinuierlichen Verbesserungsprozess

Vorstellung der aktuellen Hilfsmittel

Im Rahmen der Veranstaltung werden individuelle Fragestellungen der Teilnehmenden beantwortet.

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 – 23.11.2026 | Sparkassenakademie NRW

Präsenz-Seminar (12.10. - 16.10.2026)
Erfahrungsaustausch (23.11.2026)

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)

Auf Anfrage

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)

15.10.2026 – 16.10.2026 |
Sparkassenakademie NRW

DAUER

1,5 Tage

PREIS

840,00 €

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)

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

Erfahren Sie, welche neuen Herausforderungen und Aufgaben auf Sie als Informationssicherheitsbeauftragte/-r im Bereich der IKT-Risikokontrollfunktion zukommen. Das Seminar bietet Ihnen eine umfassende Darstellung der DORA-Anforderungen an den IKT-Risikomanagementrahmen sowie der neuen Aufgaben der/des Informationssicherheitsbeauftragten (ISB+) im Bereich der IKT-Risikokontrollfunktion. Sie erhalten Lösungsansätze auf Basis der zentral bereitgestellten Arbeitshilfen.

ZIELGRUPPE

Informationssicherheitsbeauftragte, IT-Revisorinnen und -Revisoren und deren Stellvertretungen

IHR NUTZEN

- Sie können Lösungsansätze für die IKT-Risikokontrollfunktion auf Basis zentral bereitgestellter Arbeitshilfen umsetzen.
- Sie sind vertraut mit den Schnittstellen des IKT-Risikomanagements.
- Sie kennen Schulungspflichten sowie Kommunikationsstrategien.

IHR REFERENT

Peter Schwarz, S-Management Services 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)

Auf Anfrage

DAUER

0,5 Tage
09:00 - 12:30 Uhr bzw. 13:30 - 17:00 Uhr

PREIS

325,00 €

KONTAKT

ANMELDUNG

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

INHALTE

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

Programm/Inhalt

Darstellung der neuen Anforderungen und Aufgaben des ISB+ mit IKT-Risikokontrollfunktion

Lösungsansätze zur IKT-Risikokontrollfunktion

Schnittstellen des IKT-Risikomanagements

Schulungspflichten sowie Kommunikationsstrategien

Neue Überwachungs- und Analyseanforderungen zu IKT-Risiken, neue Technologien, Altsystemen, Vorfälle und Tests

Definition und Überwachung von Kennzahlen

Jährliche oder anlassbezogene Überprüfung des IKT-Risikomanagementrahmens sowie Berichte an den Vorstand und an die Aufsicht

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)

01.09.2026 | virtueller Seminarraum
09:30 – 13:00 Uhr
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

Ermittlung kritischer oder wichtiger 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. Dieses Seminar vermittelt einen strukturierten, aktualisierten Ansatz zur Ermittlung kritischer oder wichtiger Funktionen und legt den Fokus auf die praktische Herleitung einer belastbaren Bewertungslogik, nachvollziehbarer Dokumentation, Governance und Folgeaktivitäten.

ZIELGRUPPE

Mitarbeiter/-innen mit IKT-Risikokontrollfunktion, Informationssicherheitsbeauftragte, Notfall-/BCM-Beauftragte, Leiter/-innen Organisation, Prozessverantwortliche

IHR NUTZEN

- Sie kennen einen strukturierten und aktuellen Ansatz zur Ermittlung kritischer oder wichtiger Funktionen gemäß DORA und weiterer Regulatorik.
- Sie können durch das reproduzierbare Verfahren eine belastbare Bewertungslogik ableiten, dokumentieren und begründen.
- Sie erhalten praktische Hinweise zur organisatorischen Einbindung, Governance und zu Folgeaktivitäten für die Umsetzung.

REFERENTINNEN UND REFERENTEN

Mitarbeiter/-in der SIZ GmbH

TERMIN(E)

Auf Anfrage

DAUER

2,5 Stunden

PREIS

189,00 €

KONTAKT

ANMELDUNG

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

INHALTE

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

Programm/Inhalt

Praktische Umsetzung der Methodik

- Einblick in die Methodik
- Typische Herausforderungen bei der Umsetzung in Instituten der Sparkassen-Finanzgruppe
- Organisatorische Einbindung und praktische Hinweise zur Umsetzung

Wissensvermittlung zur Dokumentation und den nötigen Folgeaktivitäten

- Anforderungen an eine nachvollziehbare Dokumentation
- Hinweise zu Governance, Review und Folgetätigkeiten
- Erwartungshaltungen aus Prüfungs- und Aufsichtsperspektive

Offene Fragerunde

Diskussion praxisbezogener Fragestellungen und institutsindividueller Aspekte

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