Management Circle Intensiv-Seminar

DORA – IT-Sicherheit im Fokus der Aufsicht

So setzen Sie den Digital Operational Resilience Act prüfungssicher um

Regulatorik und Umsetzungsmaßnahmen

- IT-Risiken identifizieren und bewerten
- IKT-Drittanbieter prüfen und überwachen

Prüfungsschwerpunkte und Handlungsempfehlungen

- IKS-Governance ausgestalten und Prozesse implementieren
- Berichtspflichten erfüllen und Nachweise dokumentieren

Roadmap zur Betriebsstabilität digitaler Systeme

- Security Operation Center einrichten und kontinuierlich verbessern
- NIS-2-konforme Organisation aufbauen

Bericht der Bundesbank

- ✔ Rolle der Aufsicht unter DORA
- ✔ Bankgeschäftliche Prüfungen unter DORA

Ihre Experten sind u.a.

Klaus Kilvinger
Opexa Advisory GmbH

Dominik Schäfer
Deutsche Bundesbank

Markus Diederichs
Selbstständiger Berater

Thorsten Schulz
Rödl & Partner GmbH

Begeisterte Teilnehmerstimme

„Eine rundherum gelungene Veranstaltung. Ich konnte viel für meine tägliche Arbeit mitnehmen.

Wählen Sie Ihren Termin
29. und **30. Oktober 2024** in **Frankfurt/M.**
Online-Seminar am **03.** und **04. Dezember 2024**

MANAGEMENTCIRCLE®
BILDUNG FÜR DIE BESTEN

Melden Sie sich jetzt an! www.managementcircle.de/M13178

Note 1,9

Digitale Betriebsstabilität sichern und Drittanbieter überprüfen

Empfang mit Kaffee und Tee **ab 9.00 Uhr**

9.30 **Herzlich willkommen**

- Begrüßung durch die Seminarleiter und kurze Vorstellungsrunde
- Überblick über Ziele und Inhalte des Seminars

9.45 **Das Infinite Game der Informationssicherheit – Cybersecurity-Bedrohungen und -Gegenmaßnahmen**

- Infinite Game und Finite Game
- Threat Landscape – globale Marktsicht und lokale Auswirkungen
- Standards und Umsetzungsszenarien
- Best Practices in Branchen und Themen
- Ausblick auf die nächsten Entwicklungen

10.45 Kaffee- und Teepause

11.00 **DORA-VO, DORA-RL, Technical Standards und Guidelines – was muss die Bank über DORA wissen?**

- Was regelt der Digital Operational Resilience Act (DORA) konkret?
- Wissensstand in Banken und regulatorischer „Screening-Prozess"
- Mitarbeiter vs. Führungskräfte, Überblicks- und Expertenwissen
- Weiterbildungsinhalte und Vermittlungswege
- Erwartungsmanagement gegenüber internen und externen Stakeholdern
- Überblick über die Entwürfe von Technical Standards und die Ausarbeitung von Leitlinien zur DORA-Verordnung durch die EU-Finanzaufsichtsbehörden

12.30 Business Lunch

13.45 **DORA in der Finanzbranche – wer ist betroffen und was sind die Auswirkungen?**

- Governance- und Kontrollrahmen für IKT-Risiken
- Anforderungen an das IKT-Risikomanagement
- Bewältigung und Meldung IKT-bezogener Vorfälle an die Aufsichtsbehörden
- Prüfung der digitalen Betriebsstabilität
- Risikomanagement von IKT-Drittanbieter
- Aufsichtsrahmen für kritische IKT-Drittanbieter
- Austausch von Informationen zu Cyberbedrohungen

14.45 **Prüfung der digitalen Betriebsstabilität**

- Anforderung an die Unternehmensführung
- Erwartungen an die Prüfer und Prüfungsmethoden
- Prüfungsplanung

15.45 Kaffee- und Teepause

16.00 **Risikomanagement von IKT-Drittanbietern – kein Hexenwerk!**

- Abgleich mit den aufsichtsrechtlichen Anforderungen (BAIT, VAIT)
- Parallelen zum Datenschutz
- Auslagerung oder sonstiger Fremdbezug
- Roadmap für die Umsetzungsplanung

17.15 Zusammenfassung der Tagesergebnisse, Erfahrungsaustausch im Teilnehmerkreis und Diskussion

Ende des ersten Seminartages **ca. 17.30 Uhr** und anschließendes Get-together

Ihre Seminarleiter

Klaus Kilvinger
Geschäftsführender Gesellschafter,
Opexa Advisory GmbH,
München

Sven Staender
Opexa Advisory GmbH,
München

Integration der DORA-Anforderungen in die IKS-Strukturen und IT-Prüfungen bestehen

9.00 **Es geht weiter**

- Zusammenfassung der Ergebnisse des ersten Seminartages
- Überleitung und Vorstellung der Themen des zweiten Seminartages

9.15 **DORA - Perspektive der Aufsicht**

- Auswirkungen auf die Finanzindustrie
- Schwerpunkt IKT-Risikomanagementrahmen
- Rolle der Aufsicht unter DORA
- Bankgeschäftliche Prüfungen unter DORA

Dominik Schäfer
Prüfungen / Bankinterne Risikomodel,
Deutsche Bundesbank, Zentrale,
Frankfurt/M.

10.45 Kaffee- und Teepause

11.00 **DORA und die IT-Prüfung – wie ist der Ablauf, worauf ist zu achten?**

- Was wird besser?
- Was wird aufwendiger?
- Reporting und Nachweisführung
- Kritik
- Alles wird gut ...

Thorsten Schulz
IT-Prüfer/IT-Berater,
Rödl & Partner GmbH,
Köln

12.30 Business Lunch

13.45 **Wie Security Operation Center Ihre Cyber Resilienz erhöht**

- Einordnung und Leistungscharakteristika
- Auswirkungen auf die Resilienz
- Organisation und operative Einbindung
- Kontinuierliche Verbesserung und Weiterentwicklung

Markus Diederichs
Selbstständiger Berater,
Köln

15.15 Kaffeepause

15.30 **Herausforderung Cybersicherheit für Banken – die neue EU-Richtlinie über Netz- und Informationssysteme (NIS-2)**

- Ziele der NIS-2-Richtlinie
- Erkenntnisse aus der aktuellen Cybersicherheitslage
- Verpflichtungen für Organisationen mit Bezug zu regulatorischen Anforderungen im Finanzbereich (z.B. DORA)
- Das NIS-2-Umsetzungsgesetz für Deutschland
- Herangehensweise und Mehrwert in der Umsetzung im Kontext Managementsystem-Zertifizierung als Lösungsvektor

Klaus Steinkirchner
Managing Consultant,
Opexa Advisory GmbH,
München

17.00 Zusammenfassung der Seminarergebnisse, Zeit für Ihre abschließenden Fragen

Ende des Intensiv-Seminars **ca. 17.15 Uhr**

Get-together
Ausklang des ersten Tages in informeller Runde. **Management Circle** lädt Sie zu einem kommunikativen Umtrunk ein. Entspannen Sie sich in angenehmer Atmosphäre und vertiefen Sie Ihre Gespräche mit den Referenten und den Teilnehmern!

Ihr Seminarleiter

Klaus Kilvinger
Geschäftsführender Gesellschafter,
Opexa Advisory GmbH,
München

Ihr Expertenteam

Markus Diederichs ist seit über zwei Jahrzehnten im Bereich der Informationstechnologie tätig. Dabei liegt sein Schwerpunkt auf dem Thema Cybersicherheit. In diesem Gebiet begleitet er seit mehr als 15 Jahren komplexe Projekte und übt operative, vertriebliche sowie leitende Rollen aus. Neben der kontinuierlichen Anwendung neuer Sicherheitstechnologien und der Behandlung verschiedenster Angriffsvektoren umfasst seine Expertise das Design, den Aufbau und den Betrieb kontinuierlicher Monitoringsysteme.

Klaus Kilvinger ist Experte für Integrierte Managementsysteme der Informationssicherheit nach ISO/IEC 27001 und TISAX®. Er ist seit vielen Jahren in der IT aktiv. Seine beruflichen Stationen lagen im Bereich von IT-Services u.a. bei öffentlichen Unternehmen sowie nationalen und internationalen Unter-nehmen. Dabei hatte er verschiedene Rollen im Vertrieb, im Management und in der Beratung inne. Klaus Kilvinger ist heute als CISO, Interim-Manager, Projektleiter, Co-Auditor, Trainer & Coach und geschäftsführender Gesellschafter der **Opexa Advisory GmbH** tätig. Sein Ziel ist es, Unternehmen zu einer verbesserten Informationssicherheit zu verhelfen und deren Resilienz zu erhöhen.

Dominik Schäfer ist Experte für bankgeschäftliche IT-Prüfungen und IT-Regulatorik bei der **Deutschen Bundesbank**. In dieser Rolle hat er als Vertreter der Bundesbank intensiv an der Erstellung des RTS zum Risikomanagementrahmenwerk unter DORA mitgewirkt. Bereits in der Vergangenheit konnte sich Dominik Schäfer erfolgreich in verschiedenen nationalen und internationalen Projekten einbringen, bspw. bei der Novellierung der BAIT 2021 sowie der Weiterentwicklung der IT-spezifischen Prüfungsmethodik des SSM. Vor seinem Wechsel in die Aufsicht hat Domink Schäfer als Prozessmanager für IT-Security in einer systemrelevanten Bank sowie drei Jahre als Consultant in der Wirtschaftsprüfung gearbeitet.

Thorsten Schulz ist bei **Rödl & Partner** im Bereich Digital Solutions tätig. Seine Tätigkeitsschwerpunkte liegen in der Betreuung und Beratung von Banken und Finanzdienstleistern zur Umsetzung aufsichtsrechtlicher Anforderungen (KWG, BA Guidelines, MaRisk und BAIT). Neben der Durchführung von Revisionsprüfungen berät er auch bei Themen rund um die Entwicklung von IT-internen Kontrollsystemen und Assurance-Prozessen. Er verfügt über 10 Jahre Praxis- und Prüfungserfahrung im Bereich des Prozessmanagements von Finanzdienstleistern, vornehmlich bei kleinen und mittleren Instituten (KMU).

Sven Staender war lange Jahre Leiter der Konzernrevision einer system-relevanten Bank in Deutschland bevor er sich selbständig gemacht hat. Als Certified Internal Auditor (CIA), Certified Fraud Examiner (CFE) und mit der Certification in Risk Management Assurance (CRMA) verfügt er über langjährige Erfahrung in der Organisation und Durchführung von Revisionstätigkeiten in Kredit- und Finanzinstituten. Als Quality Assessor und offiziell registrierter Prüfer für Interne Revisionssysteme ist Sven Staender berechtigt, Revisionsabteilungen zu zertifizieren. Durch seine Tätigkeit in diversen Revisionsarbeitsgruppen verfügt er über ein umfassendes Wissen in aktuellen Revisionsthemen. Als TÜV-zertifizierter Datenschutzbeauftragter und IT Security Manager sowie Datenschutzauditor und IT Security Auditor besitzt er umfassende Kenntnisse, um IT-Sicherheit und Revision sinnvoll miteinander zu verbinden und zu beurteilen.

Klaus Steinkirchner begleitet als Experte seine Kunden seit über 25 Jahren in zahlreichen Projekten mit Schwerpunkt Informationssicherheit, Datenschutz, IT Compliance sowie IT Service Management. Mit seinen langjährigen Erfahrungen als Berater, Coach, Projektleiter, Auditor und Trainer für mittelständische Unternehmen und internationale Großkonzerne steht für ihn die Identifizierung und Umsetzung nachhaltiger Kundenpotentiale im Vordergrund. Weitere Rollen hatte er zudem im Vertrieb sowie als Führungskraft in der Linienorganisation inne. Klaus Steinkirchner ist als Managing Consultant für die **Opexa Advisory GmbH** tätig.

Warum das Seminar wichtig ist

Digitale Attacken stellen für die Finanzindustrie eine enorme Herausforderung dar. Finanzinstitute sind aufgrund ihrer Bedeutung ein bevorzugtes Ziel von Cyber-Angriffen.

Die Europäische Union möchte vor diesem Hintergrund die digitale Widerstandsfähigkeit der Finanzbranche stärken und hat hierfür den Digital Operational Resilience Act (DORA) in Kraft gesetzt. Ziel ist es, die digitale Sicherheit zu erhöhen.

DORA fordert von den Instituten, ihre IT, ihr Business Continuity Management, ihr Krisenmanagement, das Outsourcing sowie das Informationsrisiko- und -sicherheitsmanagement eng zu verzahnen, um auf Angriffe schnell und wirksam zu reagieren.

In unserem Seminar wenden Sie alle Anforderungen, die DORA an Ihr Institut stellt, rechts-, aufsichts- und prüfungskonform an. Damit stellen Sie sicher, dass Ihr Haus im Falle eines digitalen Angriffs bestmöglich vorbereitet und geschützt ist.

Ihr Nutzen

Am ersten Seminartag erfahren Sie,

- ✔ welche **Regelungen DORA** und die zugehörigen **Standards** und **Guidelines** vorgeben.
- ✔ welche **Abteilungen** in der Bank von DORA **betroffen sind** und welche **Auswirkungen** dies hat.
- ✔ wie Sie Ihre **digitale Betriebsstabilität** prüfen.
- ✔ welche **Risiken IKT-Drittanbieter** für die Bank bedeuten.

Am zweiten Seminartag lernen Sie,

- ✔ wie Sie DORA in Ihre **IKS-Strukturen** integrieren.
- ✔ wie die **IT-Prüfung** unter DORA abläuft.
- ✔ wie Sie ein **Security Operations Center** in Ihrer Bank einrichten.
- ✔ wie Sie der **Herausforderung Cybersicherheit** begegnen.

Ihre Vorteile auf einen Blick

Ausgewiesene Experten
Sie werden von anerkannten und erfahrenen Referenten aus der Beratung und Unternehmenspraxis trainiert und begleitet. Umfangreiches Wissen zu DORA und der IT-Sicherheit wird direkt an Sie weitergegeben.

Hohe Praxisrelevanz
Die Seminarinhalte werden durch zahlreiche Beispiele und Erfahrungsberichte aus der Praxis ergänzt. In jedem Seminar ist ausreichend Zeit für Ihre persönlichen Fragestellungen.

Exklusive Praxisbericht
Erfahren Sie mehr über die Etablierung der IKS-Strukturen in der DekaBank.

Interaktive Workshop-Atmosphäre
Der Aufbau des Seminars ermöglicht eine intensive und praxisnahe Wissensvermittlung. Nutzen Sie die Möglichkeit, Ihre Fragen direkt mit unseren Experten zu klären.

Intensives Networking
Nutzen Sie den branchenübergreifenden Erfahrungsaustausch mit Experten und Fachkollegen und knüpfen Sie wertvolle Kontakte. Bauen Sie so Ihr Expertennetzwerk aus.

Kompakte Seminarunterlagen
Nutzen Sie die aktuell erstellten Seminarunterlagen zur Nachbereitung und als hilfreiches Nachschlagewerk in Ihrem Tagesgeschäft.

Ihre Fragen vorab
Sie erhalten zwei Wochen vor dem Seminar einen Fragebogen, in dem Sie uns Ihre Fragen und Themenschwerpunkte mitteilen können. Unser Expertenteam kann sich so besser auf Ihre individuellen Interessen und Bedürfnisse einstellen.

Sie haben noch Fragen? Gerne!

Rufen Sie mich an oder schreiben Sie mir eine E-Mail.

Dr. Thomas Lorenz
Projektmanager
Tel.: +49 6196 4722-570
thomas.lorenz@managementcircle.de

DORA – IT-Sicherheit im Fokus der Aufsicht

Wen Sie auf dieser Veranstaltung treffen

Dieses Intensiv-Seminar richtet sich an **Fach-** und **Führungskräfte** der Bereiche **(IT-)Risikomanagement**, **(IT-)Controlling** (**OpRisk/ Informationsrisiko**), **Informationssicherheit**, **zentrales Auslagerungsmanagement** sowie **Interne Revision** und **Compliance** aus **Banken**, **Sparkassen** und **Genossenschaftsinstituten**. Darüber hinaus wenden wir uns an **Verbandsvertreter** und **Unternehmensberater**, die Banken fit für die IT-Sonderprüfung machen.

Termine und Veranstaltungsorte

29. und **30. Okt. 2024 Eschborn** bei **Frankfurt/M.** 10-93060

Management Circle Campus, Düsseldorfer Straße 36, 65760 Eschborn, Tel.: +49 6196/4722-800

Für Übernachtungsmöglichkeiten in unmittelbarer Nähe fragen Sie bitte unser Team.

03. und **04. Dezember 2024** als **Online-Seminar** 12-93061

Besuchen Sie auch mal unseren Blog!

Dort finden Sie **aktuelle News**, **spannende Tipps** unserer zahlreichen Experten und **exklusive Beiträge** rund um die Themen unserer Veranstaltungen.

www.managementcircle.de/blog

Begrenzte Teilnehmerplätze – jetzt anmelden!

Online-Anmeldung:	**www.managementcircle.de/M13178**
PDF zum Ausdrucken:	**www.managementcircle.de/form**
E-Mail:	**anmeldung@managementcircle.de**
Telefonisch:	**+49 6196 4722-700**
per Post:	**Management Circle AG, Postfach 56 29, 65731 Eschborn/Ts.**

Anmeldebedingungen

Nach Eingang Ihrer Anmeldung erhalten Sie eine Anmeldebestätigung und eine Rechnung. Der Ticketpreis für das zweitägige Seminar beträgt inkl. Business Lunches, Erfrischungsgetränken, Get-together und der Dokumentation € 2.295,–. Der Preis für die Online-Teilnahme beträgt inkl. Dokumentation € 2.095,–. **10% Preisnachlass erhalten Sie** auf den gesamten Rechnungsbetrag bei der Anmeldung von mehr als 2 Teilnehmern aus Ihrem Unternehmen. **Buchen Sie ohne Risiko: Die kostenlose Stornierung ist bis vier Wochen vor dem Veranstaltungstermin möglich.** Danach oder bei Nichterscheinen des Teilnehmers berechnen wir den gesamten Ticketpreis. Die Stornierung bedarf der Schriftform. Selbstverständlich ist eine Vertretung des angemeldeten Teilnehmers möglich. Alle genannten Preise verstehen sich zzgl. der gesetzlichen MwSt.

Werbewiderspruch

Sie können der Verwendung Ihrer Daten für Werbezwecke durch die Management Circle AG selbstverständlich jederzeit widersprechen oder eine erteilte Einwilligung widerrufen. Hierfür genügt eine kurze Nachricht an unseren Datenschutzbeauftragten per Mail an datenschutz@managementcircle.de oder per Post an Management Circle AG, Datenschutz, an die oben genannte Adresse. Weitere Informationen zum Datenschutz erhalten Sie unter www.managementcircle.de/datenschutz.

Über Management Circle

Seit über 30 Jahren bieten wir berufliche Weiterbildung auf höchstem Niveau. Unter dem Motto **Bildung für die Besten** erlangen Sie den Wissensvorsprung, der Sie auf Ihrem Karrierepfad weiterbringt. In Zusammenarbeit mit unseren Experten aus Wirtschaft, Politik und Wissenschaft identifizieren wir für Sie die relevanten Themen und Trends – aktuell und zukunftsweisend. Unser gesamtes Weiterbildungsangebot finden Sie unter **www.managementcircle.de**

Reisen Sie mit der Deutschen Bahn zu attraktiven Sonderkonditionen zum Veranstaltungsort. Infos unter: www.managementcircle.de/bahn

Produziert mit Ökostrom und Biofarben basierend auf nachwachsenden Rohstoffen

FSC www.fsc.org MIX Papier | Fördert gute Waldnutzung FSC® C018996

A/EP