



KURZPROFIL · INTERIM MANAGEMENT

# Michael Schwendemann

Interim CIO, CRO / Head of Compliance & Risk / Head of Governance

Compliance · Risk · DORA · MaRisk · VAG/MaGo · NIS2

m.schwendemann@sifor.eu · +49 171 4453 822 · www.sifor.eu · Hamburg / europaweit

## PROFIL

Interim Manager mit über 25 Jahren Führungserfahrung in Banken, Versicherungen, Zahlungsverkehr, Kapitalanlagegesellschaften, Dienstleistern und Industrie — davon neun Jahre Linienverantwortung als CIO und COO einer großen Auslandsbank in Frankfurt mit Führung von 60 Mitarbeitenden und Gesamtverantwortung für IT, Operations und Budget. Als Interim CIO, CRO, Head of Compliance & Risk oder Head of Governance verantworte ich — auf Projektbasis oder in Linienverantwortung — den Aufbau und die Transformation von IT-, Compliance- und Risk-Organisationen: von Strukturanalyse und Prozessoptimierung über prüfungssichere Governance-Strukturen bis zur operativen Umsetzung regulatorischer und technischer Großprogramme (z. B. Digitalisierung, KI). Nachweisbare Erfolge in der Begleitung aufsichtsrechtlicher Prüfungen (§44 KWG, PS 951, EZB, WP) und der nachhaltigen Abarbeitung der Feststellungen. Führung interdisziplinärer Teams aus IT, Compliance, Risk und Legal — hands-on, in der Linie, mit geordneter Übergabe.

## FOKUSTHEMEN

### — DORA-Umsetzung

Informationsregister, Auslagerungs- & Dienstleistermanagement, IKT-Risiko- und IKT-Vorfallmanagement, Vertragsanpassungen, BCM, Prüfungsbegleitung.

### — MaRisk- & MaGo/VAG-Umsetzung

Gap-Analyse, schriftlich fixierte Ordnung, IKS, Auslagerung/Ausgliederung (AT 9 / § 32 VAG), Governance nach §§ 23 ff. VAG.

### — NIS2-Umsetzung

Betroffenheitsanalyse, Governance der Leitungsorgane, Lieferkettensicherheit, Meldeprozesse (24h/72h), Audit-Readiness.

### — Interim IT-Management & IT-Steuerung

Interimistische IT-Leitung/CIO-Verantwortung (9 Jahre Linienerfahrung, 60 Mitarbeitende), IT-Budget- und Kostensteuerung, Dienstleistersteuerung (SLA/KPI), Stabilisierung des IT-Betriebs, Personalaufbau und Übergabe.

### — Audit-Readiness & §44-KWG-Prüfungen

Vorbereitung, Begleitung während der Prüfung, ursachenbasierte Abarbeitung der Feststellungen — auf Instituts- wie Prüferseite erfahren.

### — IAM & PAM

Prüfungsfeste Berechtigungskonzepte (RBAC/ABAC), Rezertifizierung, SoD, privilegierte Zugriffe; Tools: Garancy, One Identity, Omada, FSP, CyberArk, SailPoint u. a. — AD, Entra ID, RACF.

### — KI in Compliance & Risk

KI-Governance nach EU AI Act und DORA; produktive KI-Agenten für Due-Diligence-Auswertung und Vertragsanalyse bereits umgesetzt.

## SCHWERPUNKTE IN REGULATORIK, GOVERNANCE & STANDARDS

DORA, MaRisk, BAIT, VAIT, NIS2 sowie Informationssicherheits- und Resilienzstandards nach ISO/IEC 27001, 27002, 27005 und ISO 22301; ergänzend Datenschutz-Governance und Privacy-Anforderungen im Kontext DSGVO / ISO 27701 sowie Prüfungs- und Attestierungsstandards nach SOC 2.

## SPRACHEN & VERFÜGBARKEIT

Deutsch (Muttersprache) · Englisch (verhandlungssicher) · Italienisch (Grundkenntnisse)  
Einsätze europaweit & remote · kurzfristig verfügbar

## AUSGEWÄHLTE MANDATE (ANONYMISIERT)

### **Große Auslandsbank, Frankfurt**

#### CIO & COO — Gesamtverantwortung IT & Operations

Neun Jahre Linienverantwortung mit Führung von 60 Mitarbeitenden. IT-Budgetplanung und Kostensteuerung im zweistelligen Millionenbereich, Auswahl und Steuerung externer IT-Dienstleister inkl. Vertrags- und SLA-Verhandlungen, Personalaufbau sowie Stabilisierung des laufenden IT-Betriebs.

### **Versicherungsunternehmen**

#### Aufbau Compliance-Organisation & DORA-Operationalisierung

Gesamtverantwortung für den Aufbau einer Compliance-, Governance- und Risk-Organisation. Integriertes GRC-Modell, Executive-Reporting für den Vorstand, KI-gestützte Automatisierung von Due-Diligence-Auswertung und Vertragsanalyse.

### **IT- & Mediendienstleister der Banken (KRITIS)**

#### Auslagerungsmanagement & zentraler Einkauf unter DORA, NIS2, PSD2

Vollständiges Informations- und Auslagerungsregister, Dienstleistermanagement mit SLA/KPI-Modell, BCM für einen KRITIS-Dienstleister, Übergabe der Abteilung an die Linie.

### **Versicherungsgruppe**

#### DORA-Umsetzung im Dienstleistermanagement

Informationsregister, Definition kritischer Funktionen und Dienstleister, Due-Diligence-Prozesse, Vertragsanpassungen gemäß DORA, Exit-Planung und -Strategie.

### **Internationaler Versicherungskonzern**

#### Strategieberatung VAIT / DORA

Schriftlich fixierte Ordnung für alle VAIT/DORA-Themen, Richtlinien für IAM und Informationssicherheit, Einführung eines GRC-Tools, Informationsregister mit Erstbewertung.

### **IT-Dienstleister für Banken**

#### IKS, IAM & Begleitung regulatorischer Prüfungen

Einführung Garancy, SoD-Konfliktmanagement inkl. Ausnahmeprozessen, prüfungsfeste Berechtigungskonzepte. Begleitung von §44-KWG-, PS-951-, WP- und Datenschutzprüfungen sowie Umsetzung der Findings.

### **Depotbank / Fondsplattform**

#### Projektleitung & IAM-Architektur

Fachliche Führung eines 10-köpfigen Projektteams, Transformation der IAM-Lösung in die Cloud, Aufbau IT-Notfallmanagement und Auslagerungsprozesse, Informationssicherheit.

Weitere Stationen (Auswahl): Big-Four-Wirtschaftsprüfung · Direktbank · Landesbank · Genossenschaftliche Zentralbank · Europäische Energiebörse · IT-Dienstleister einer Großbank · Wertpapierhaus der Sparkassen

## PARTNERNETZWERK

Seit 25 Jahren gewachsene Partnerschaft mit rund 50 selbstständigen Spezialistinnen und Spezialisten — auf Abruf verfügbar, als eingespielte Teams kurzfristig einsatzbereit. Abgedeckte Fachbereiche u. a.: Einkauf, Backoffice Wertpapiere, Geld-, Devisen- und Derivatehandel, Fondsabwicklung, Treasury, Zahlungsverkehr, Kredite, Rechnungswesen, Meldewesen, Recht & Vertragswesen, Geldwäscheprävention, Interne Revision, Datenschutz, Informationssicherheit, BCM, Notfallplanung, IKT-Vorfallsmanagement, Projektmanagement/PMO. Ein Ansprechpartner für den Kunden — auch bei größeren Programmen.