



SHORT PROFILE · 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 / across Europe

## PROFILE

Interim manager with more than 25 years of leadership experience in banks, insurance companies, payments, asset management companies, service providers and industry — including nine years of line responsibility as CIO and COO of a major foreign bank in Frankfurt, leading 60 staff with overall responsibility for IT, operations and budget. As interim CIO, CRO, Head of Compliance & Risk or Head of Governance I take responsibility — on a project basis or in line responsibility — for building and transforming IT, compliance and risk organisations: from structural analysis and process optimisation through audit-proof governance structures to the hands-on implementation of major regulatory and technical programmes (e.g. digitalisation, AI). Proven track record in supporting supervisory examinations (Sec. 44 KWG, PS 951, ECB, external audit) and in the sustainable remediation of findings. Leading interdisciplinary teams from IT, compliance, risk and legal — hands-on, in the line, with an orderly handover.

## FOCUS AREAS

### — DORA implementation

Register of information, outsourcing & third-party management, ICT risk and ICT incident management, contract amendments, BCM, audit support.

### — MaRisk & MaGo/VAG implementation

Gap analysis, written rules of procedure, internal control system, outsourcing (AT 9 / Sec. 32 VAG), governance under Sec. 23 et seq. VAG.

### — NIS2 implementation

Scoping analysis, governance of management bodies, supply chain security, reporting processes (24h/72h), audit readiness.

### — Interim IT management & IT steering

Interim IT leadership/CIO responsibility (9 years of line experience, 60 staff), IT budget and cost management, vendor steering (SLA/KPI), stabilisation of IT operations, staff build-up and handover.

### — Audit readiness & Sec. 44 KWG examinations

Preparation, support during the examination, root-cause-based remediation of findings — experienced on both the institution's and the auditor's side.

### — IAM & PAM

Audit-proof authorisation concepts (RBAC/ABAC), recertification, SoD, privileged access; tools: Garancy, One Identity, Omada, FSP, CyberArk, SailPoint and others — AD, Entra ID, RACF.

### — AI in compliance & risk

AI governance under the EU AI Act and DORA; productive AI agents for due diligence evaluation and contract analysis already delivered.

## FOCUS IN REGULATION, GOVERNANCE & STANDARDS

DORA, MaRisk, BAIT, VAIT, NIS2 as well as information security and resilience standards under ISO/IEC 27001, 27002, 27005 and ISO 22301; complemented by data protection governance and privacy requirements in the context of GDPR / ISO 27701 as well as audit and attestation standards under SOC 2.

## LANGUAGES & AVAILABILITY

German (native) · English (business fluent) · Italian (basic)

Assignments across Europe & remote · available at short notice

# Michael Schwendemann — Selected mandates & network

## SELECTED MANDATES (ANONYMISED)

### **Major foreign bank, Frankfurt**

#### CIO & COO — overall responsibility for IT & operations

Nine years of line responsibility leading 60 staff. IT budget planning and cost management in the double-digit millions, selection and management of external IT service providers including contract and SLA negotiations, staff build-up, and stabilisation of day-to-day IT operations.

### **Insurance company**

#### Building a compliance organisation & operationalising DORA

Overall responsibility for building a compliance, governance and risk organisation. Integrated GRC model, executive reporting for the board, AI-supported automation of due diligence evaluation and contract analysis.

### **IT & media service provider for banks (critical infrastructure)**

#### Outsourcing management & central procurement under DORA, NIS2, PSD2

Complete register of information and outsourcing register, third-party management with an SLA/KPI model, BCM for a critical-infrastructure service provider, handover of the department to the line.

### **Insurance group**

#### DORA implementation in third-party management

Register of information, definition of critical functions and providers, due diligence processes, DORA-compliant contract amendments, exit planning and strategy.

### **International insurance group**

#### Strategic advisory VAIT / DORA

Written rules of procedure for all VAIT/DORA topics, policies for IAM and information security, roll-out of a GRC tool, register of information with initial assessment.

### **IT service provider for banks**

#### ICS, IAM & support of regulatory examinations

Roll-out of Garancy, SoD conflict management incl. exception processes, audit-proof authorisation concepts. Support of Sec. 44 KWG, PS 951, external and data protection audits and remediation of the findings.

### **Custodian bank / fund platform**

#### Project lead & IAM architecture

Leading a ten-person project team, transforming the IAM solution to the cloud, building IT contingency management and outsourcing processes, information security.

Further roles (selection): Big Four audit firm · Direct bank · Landesbank · Central institution of the cooperative banks · European energy exchange · IT subsidiary of a major bank · Securities house of the German savings banks

## PARTNER NETWORK

A partnership grown over 25 years with around 50 independent specialists — available on call, deployable at short notice as well-rehearsed teams. Covered functional areas include: procurement, securities back office, money market, FX and derivatives trading, fund settlement, treasury, payments, lending, accounting, regulatory reporting, legal & contract management, AML, internal audit, data protection, information security, BCM, contingency planning, ICT incident management and project management/PMO. One point of contact for the client — even on larger programmes.