FORFA
CONSULTING

# COURSE / EVENT PROFILE


Rolf von Roessing
Hon. Prof., CISA, CISM, CGEIT, CISSP,
CDPSE, FBCI, CABCF

## Overview

**Rolf von Roessing**

**CISA, CISM, CGEIT, CDPSE, CISSP, CABCF, FBCI**

*Past Global Vice Chair, Past International Vice President, ISACA Board of Directors, Past Chairman of the Audit Committee, The Business Continuity Institute*

Rolf von Roessing is a partner and CEO at FORFA Consulting AG, an international consultancy firm specialising in GRC, security and related disciplines. He brings 30 years of experience in governance, risk management and compliance; security and business continuity; and crisis management in a range of sectors, including banking and finance, insurance, wholesale and retail, automotive, and healthcare.

He has also been teaching as a senior lecturer in M. Sc. courses at Donau-Universität Krems since 2005 and is a member of the Academic Council for M. Sc. Management and IT, M. Sc. Information Security Management, and M. Sc. Cybersecurity.

He is a former International Vice President and Global Vice Chairman of ISACA (2009-2011; 2019-2021) Since 2021, Rolf has been lead developer within the core team developing the ISACA Digital Trust Ecosystem and Framework (DTEF), and a principal reviewer of the related AI white paper by ISACA.

From 2001 to 2008, Rolf was a member of the BCI Board of Directors, and Chairman of the Audit Committee from 2003 to 2008.

Rolf has published extensively on BCM, resilience and cyber topics since 2001. A list of works is available on scholar.google.com and academia.edu. He frequently provides contributions to leading journals and magazines such as Computer Weekly. In 2023, he was nominated as one of three worldwide ISACA Global Evangelists.

| Expertise |
| --- |
| • Digital Trust, AI, digital transformation<br>• Governance, Risk Management, Compliance (GRC)<br>• Information security, cybersecurity<br>• BCM, ITSCM, crisis and incident management, resilience<br>• Outsourcing, vendor management<br>• Data protection and privacy<br>• Regulatory<br>• Interim C-level |

| Sectors |
| --- |
| • Banking and finance<br>• Insurance<br>• Wholesale and retail<br>• Automotive<br>• Industry (various)<br>• Healthcare<br>• Institutional |

## IIA Iceland & ISACA Group

Workshop Description

This series of short workshops provides a learning journey for internal auditors, with insights on IT audit and how to apply it to new European Union legislation. It consists of three half day sessions covering

- Session 1: IT Audit and Assurance Fundamentals
- Session 2: EU-NIS2 and Related Regulations in Critical Infrastructure Protection
- Session 3: EU-DORA and Related Financial Sector Regulations

The workshops are designed for practitioners with audit and assurance roles in IT, cyber resilience and cyber risk. Session 3 provides a deep dive into the Digital Operational Resilience Act, including its delegated Regulatory Technical Standards (RTS) and Implementing Technical Standards (ITS).

After attending Session 1, participants will:

- Have a solid understanding of the general IT audit practice and approach
- Understand the Topical IIA Requirements
- Know how to scope the IT audit in a risk-based manner, answering the question "how much is enough to obtain reasonable assurance?"
- Master the art of efficient auditing under limited time and budgets

The session will award 4 CPE and will be followed by a general Q&A for the group attending.

After attending Session 2, participants will:

- Understand the scope and requirements of the EU-NIS2 Directive
- Be able to audit and review the detailed requirements of the Directive
- Know how to leverage recognized audit programs and external frameworks to obtain assurance over critical infrastructure protection
- Understand the EU and national arrangements for supervisory review, certification and reporting

The session will award 4 CPE and will be followed by a general Q&A for the group attending.

After attending Session 3, participants will:

- Understand the scope and requirements of the EU-DORA Regulation
- Be able to audit and review the detailed requirements of the Regulation, including the RTS and ITS
- Know how to leverage recognized frameworks such as NIST CSF 2.0 to support the audit
- Understand the role of the national and EU supervisory mechanisms around DORA

The session will award 4 CEP and will be followed by a general Q&A for the group attending.

## Mentoring Program Offering

In many instances, professional practitioners attending the course may not have the bandwidth to personally manage and supervise the key learnings, due to day-to-day pressures and a lack of time in distributing the knowledge across their organizations. As a direct follow-up to the two-day cyber resilience course, a Mentoring Program is available that ensures sustainable and deep implementation in organizations. The program is tailored to the individual needs and objectives of each organization, taking into account the "as is" as well as the target states of cyber resilience. The mentoring approach has been proven in practice, providing several key advantages:

- Enabling people: instead of presenting "turnkey" consulting solutions, internal resources are actively involved from the beginning, in line with the time they can afford
- Fast and efficient knowledge transfer: Mentors share their experience directly and maintain regular dialogue with their mentees
- Superior, senior experience and knowledge: Mentors are industry veterans with 30+ years of experience, with a mission to empower the next generation
- High multiplier: mentees stay together in groups and maintain a regular exchange of thoughts and practical results, forming a growing network of "in the know" people
- Small but scalable footprint: Mentors can draw on a vast network of specialist or consultant help if additional manpower is needed, but they will always seek the internal solution first
- Tone from the top: Mentors can support the cases for top management, external audit, certification, and control of external advisory work

In a typical mentoring setting, an initial analysis of the "as is" and target state will be conducted in a defined and efficient way. Based on the results, internal leadership and the mentor will develop the structure for internal workshops to be held with the target group. The agreed concept will be deployed (typically in the course of 3 to 5 days), and regular touch points and reviews will be set for the following months. The regular contact ensures that cyber resilience projects and initiatives stay on course, and helps identify any red flags that may arise. Mentors and mentee groups achieve success together, creating a climate of step-by-step success and confidence.

## Contact Details

LinkedIn profile: https://www.linkedin.com/in/rolf-von-roessing-7b519b/

Corporate: FORFA Consulting AG, Dammstrasse 16, 6300 Zug ZG, Switzerland

Land: +41 41 511 4603

Mobile / WhatsApp / Signal / Telegram: +49 172 671 2322

Mail: rvr@forfa.ch