QUEST
Professional Center

PROFESSIONAL TRAINING COURSE

Course No. 1084

Cybersecurity & Digital Risk for Banks

DIGITAL BANKING, FINTECH & AI
FINANCE, INVESTMENT & BANKING

DURATION **5 Days**	DELIVERY **Classroom**
LOCATION **Munich, Germany**	DATES **21 – 25 Dec 2026**

Scheduled Event Details

CITY	Munich, Germany
DATE	21 – 25 Dec 2026
DELIVERY TYPE	Classroom
COURSE FEE	€5,400

Course Overview

Cybersecurity & Digital Risk for Banks is a comprehensive professional training course designed to equip banking executives, cybersecurity professionals, risk managers, IT specialists, compliance officers, and decision-makers with the strategic knowledge and practical skills required to protect financial institutions against evolving cyber threats and digital risks. As banks accelerate digital transformation through online banking, cloud computing, artificial intelligence, mobile financial services, and interconnected digital ecosystems, cybersecurity has become a critical business priority for protecting assets, maintaining customer trust, ensuring operational resilience, and supporting regulatory compliance.

This course provides participants with a comprehensive understanding of cybersecurity principles within the banking sector, digital risk management frameworks, cyber governance, identity and access management, network security, cloud security, data protection, cyber threat intelligence, incident response, business continuity, disaster recovery, third-party risk management, and security operations. Participants will explore how modern cybersecurity strategies safeguard banking infrastructure, digital channels, payment systems, customer information, and critical financial services while strengthening organizational resilience against increasingly sophisticated cyber threats.

The program also examines the relationship between Cybersecurity & Digital Risk for Banks and Digital Banking Transformation, Financial Technology (FinTech), Open Banking, Banking-as-a-Service (BaaS), Enterprise Risk Management, Regulatory Compliance, Anti-Money Laundering (AML), Data Governance, Operational Risk Management, Privacy Protection, Business Continuity Management, and Digital Innovation. Participants will gain practical insights into assessing cyber risks, implementing security controls, managing security incidents, strengthening governance frameworks, and developing enterprise cybersecurity strategies aligned with business objectives and regulatory expectations.

Through interactive workshops, cyber incident simulations, banking case studies, risk assessment exercises, threat analysis, and real-world financial services scenarios, participants will strengthen their ability to evaluate cybersecurity risks, improve digital resilience, protect critical banking operations, respond effectively to cyber incidents, and support secure digital transformation initiatives. By the end of the course, participants will be equipped to develop practical cybersecurity and digital risk strategies that enhance governance, improve operational resilience, strengthen regulatory compliance, and support sustainable growth across financial institutions.

Objectives

- Analyze Cybersecurity & Digital Risk concepts and evaluate their impact on banking operations, digital resilience, and organizational performance by the end of the course.
- Develop strategic approaches for managing cybersecurity and digital risks within financial institutions.
- Evaluate cyber threats, vulnerabilities, and digital risks using structured risk assessment methodologies.
- Apply cybersecurity principles to protect banking infrastructure, digital channels, customer data, and critical financial services.
- Design security controls and resilience strategies that support secure banking operations and business continuity.
- Improve incident detection, cyber response capabilities, and organizational crisis management.
- Strengthen governance through regulatory compliance, cybersecurity frameworks, data governance, privacy protection, and enterprise risk management.
- Implement Key Performance Indicators (KPIs), cybersecurity maturity metrics, risk indicators, and operational resilience measures to evaluate security performance.
- Assess the cybersecurity implications of cloud computing, artificial intelligence, digital banking platforms, third-party services, and emerging technologies.
- Align cybersecurity initiatives with enterprise strategy, Digital Banking Transformation, operational resilience, regulatory expectations, and sustainable organizational growth before course completion.

Who Should Attend

This course is designed for banking executives, Chief Information Security Officers (CISOs), Chief Information Officers (CIOs), cybersecurity managers, information security professionals, IT managers, digital transformation managers, banking operations managers, risk managers, compliance officers, AML professionals, business continuity managers, internal auditors, infrastructure specialists, security analysts, project managers, and professionals responsible for cybersecurity and digital risk management within financial institutions.

The program is equally valuable for central bank professionals, financial regulators, government financial institution leaders, FinTech professionals, cybersecurity consultants, technology architects, cloud security specialists, data governance professionals, operational risk specialists, legal and regulatory professionals, and decision-makers responsible for digital resilience, regulatory compliance, secure digital transformation, and technology governance across the financial sector.

Learning Outcomes

- By the end of this course, participants will be able to:
- Develop comprehensive cybersecurity and digital risk management strategies for financial institutions.
- Evaluate cyber threats, vulnerabilities, and digital risks affecting banking operations.
- Apply cybersecurity controls to protect banking systems, digital platforms, and sensitive financial information.
- Design incident response, business continuity, and disaster recovery plans for cyber resilience.
- Assess cybersecurity risks associated with cloud computing, digital banking services, third-party providers, and emerging technologies.
- Strengthen governance through regulatory compliance, cybersecurity frameworks, enterprise risk management, data governance, and privacy protection.
- Prepare executive dashboards using cybersecurity KPIs, digital risk indicators, operational resilience metrics, and security performance measures.
- Integrate cybersecurity initiatives with Digital Banking Transformation, Enterprise Risk Management, Operational Excellence, and Strategic Planning.
- Evaluate the impact of emerging technologies on cybersecurity risks and banking resilience.
- Develop a practical implementation roadmap that strengthens cybersecurity governance, reduces digital risks, improves operational resilience, supports regulatory compliance, protects

critical banking assets, and accelerates secure digital transformation.

Course Outline

DAY 01

Foundations of Cybersecurity in Banking

- The evolving cybersecurity threat landscape in financial services
- Cybersecurity principles and international security frameworks
- Banking technology infrastructure and digital ecosystems
- Cybersecurity governance and enterprise security strategy

> **PRACTICAL APPLICATION OR DISCUSSION**
> Assessing cybersecurity readiness within financial institutions

DAY 02

Digital Risk Management and Infrastructure Protection

- Digital risk identification and assessment methodologies
- Identity and access management
- Data protection, privacy, and information security
- Network security and infrastructure resilience

> **PRACTICAL APPLICATION OR DISCUSSION**
> Conducting a digital risk assessment and designing security controls

DAY 03

Protecting Digital Banking Operations

- Security of digital banking platforms and payment systems
- Cloud security and third-party risk management
- Cyber threat intelligence and vulnerability management
- Security operations and continuous monitoring

DAY 03 — CONTINUED

PRACTICAL APPLICATION OR DISCUSSION

Designing cybersecurity controls for banking operations

DAY 04

Incident Response, Compliance, and Operational Resilience

- Cyber incident response and crisis management
- Business continuity and disaster recovery planning
- Regulatory compliance and cybersecurity governance
- Measuring cybersecurity performance using KPIs and resilience metrics

PRACTICAL APPLICATION OR DISCUSSION

Developing a cyber incident response plan

DAY 05

Building a Cyber-Resilient Financial Institution

- Enterprise cybersecurity strategy and implementation planning
- Organizational change management and cybersecurity culture
- Emerging trends in cybersecurity and digital risk management
- Continuous improvement and operational resilience

FINAL WORKSHOP

Develop a comprehensive Cybersecurity & Digital Risk implementation roadmap that includes cybersecurity strategy, enterprise governance, digital risk assessment, regulatory compliance, cybersecurity controls, data protection, identity and access management, cloud security, third-party risk management, business continuity, incident response, performance measurement, organizational change management, and continuous improvement initiatives to strengthen operational resilience, protect critical banking assets, support secure digital transformation, and achieve sustainable organizational growth.

QUEST
Professional Center

Register or Request More Information

Course page: https://quest-training.com/courses/cybersecurity-digital-risk-for-banks
Website: https://quest-training.com
Email: info@quest-training.com
Phone: +905016771440