Operational Risk Management For IT Professionals

System and Information technology

SOLVEWORX

Virtual

24 hours

USD 1,300

Registration Deadline
4-May-2025

Course Description:

IT Operational risk is a critical concern for modern banking institutions, especially in the context of IT systems. This course is designed specifically for Bank IT professionals to understand, assess, and mitigate operational risks in the ever-evolving landscape of digital banking. The course covers key concepts, methodologies, and tools and best practises to identify, assess, mitigate, and monitor operational risks faced by banks.

Target Audience:

This course is intended for Business Professionals, IT Professionals, Engineers, Architects, Data Analysts, Report Writers, Educators, Trainers, Graphic Designers, Project Teams, Students and Enthusiasts, Administrative Professionals, Entrepreneurs, Small Business Owners and Anyone Interested in Diagramming.

What does the Course Cover?

Operational Risk Frameworks:

- The fundamental concepts and components of operational risk.
- Explore various operational risk frameworks and regulatory requirements specific to the banking sector.
- Learn how to establish an effective operational risk management framework within a bank.

Risk Identification and Assessment:

- Develop skills to identify and assess operational risks in banking operations.
- Learn various risk assessment techniques, including risk control self-assessment (RCSA), key risk indicators

(KRIs), and scenario analysis.

- Understand how to prioritise operational risks based on their potential impact and likelihood.

Risk Mitigation and Control:

- Learn strategies and best practices for mitigating operational risks in banking.
- Explore risk control techniques, including process controls, segregation of duties, and access controls.
- Understand the importance of implementing effective internal controls to prevent operational failures.

Key Operational Risk Areas:

- Explore key areas of operational risk in banking, such as fraud, cyber risk, compliance risk, and business
- continuity.

Operational Risk Management For IT Professionals

System and Information technology

SOLVEWORX

Virtual

24 hours

USD 1,300

Registration Deadline
4-May-2025

- Understand the specific challenges and mitigation strategies associated with each operational risk area.
- Operational Risk Monitoring and Reporting:
- Learn how to establish effective monitoring and reporting mechanisms for operational risks.
- Understand the role of key risk indicators (KRIs) and risk dashboards in tracking and communicating operational risk exposures.
- Explore best practices for reporting operational risk to stakeholders, including senior management and regulators.

Course Outline:

Module 1: Introduction to Operational Risk Management in Banking (60 minutes)

- Operational Risk Management in Banking
- Operational Risk in the Digital Age
- Effective communication of IT operational risks
- Board and management reporting requirements

Module 2: Regulatory Framework and Compliance (60 minutes)

- Basel III and Operational Risk
- Regulatory Guidelines for IT Security in Banking
- Compliance Challenges and Solutions

Module 3: Identifying Operational Risks in IT Systems (60 minutes)

- Types of Operational Risks in IT
- Risk Identification Techniques
- IT Vulnerabilities and Threats in Banking

Module 4: Key Risk Indicators (KRIs) and Key Control Indicators (KCIs) (60 minutes)

- Key Risk Indicators (KRIs) in IT
- Selection and development of KRIs and KCIs
- Monitoring and reporting on KRIs and KCIs
- Quantitative vs. Qualitative Risk Assessment

Module 5: Technology and Operational Risk (60 minutes)

- Fintech Disruptions and Risks
- Cloud Computing and Cybersecurity
- Managing Risks in Mobile Banking

Operational Risk Management For IT Professionals

System and Information technology

SOLVEWORX

Virtual

24 hours

USD 1,300

Registration Deadline
4-May-2025

Module 6: Incident Response and Crisis Management (60 minutes)
- Developing an Incident Response Plan (60 minutes)
- Crisis Communication Strategies
- Role of IT in Incident Response

Module 7: Vendor Risk Management (60 minutes)
- Evaluating Third-Party IT Risks
- Contractual Agreements and SLAs
- Monitoring and Controlling Vendor Risks

Module 8: Business Continuity Planning (60 minutes)
- IT Disaster Recovery Planning
- Redundancy and Failover Systems
- Ensuring Continuous IT Operations

Module 9: Cybersecurity and Data Protection (60 minutes)
- Cybersecurity Best Practices for Banks
- Data Encryption and Privacy Regulations
- Insider Threats and IT Security

Module 10: Fraud Prevention and Detection (60 minutes)
- IT Systems in Fraud Prevention
- Advanced Fraud Detection Tools
- Case Studies: IT-based Fraud in Banking

Module 11: Risk Culture and Awareness (60 minutes)
- Importance of risk culture in operational risk management
- Strategies for promoting risk awareness
- Behavioural and organisational factors in risk culture

Module 12: Emerging Trends and Future Challenges (60 minutes)
- Emerging Risks in banking and their impact
- Technology-driven changes and challenges
- AI and Machine Learning in Operational Risk Management
- Predictive Analytics for IT Security in Banking

Course Objectives:

Comprehensive Understanding of Operational Risk

Delegates will gain a thorough understanding of what operational risk is, including its key components, causes, and the impact it can have on a banking institution. They will learn how operational risk differs from other types of risks such as credit and market risk.

Operational Risk Management For IT Professionals

System and Information technology

SOLVEWORX

Virtual

24 hours

USD 1,300

Registration Deadline
4-May-2025

Frameworks and Best Practices
The course will provide delegates with knowledge of operational risk management frameworks, such as the Basel guidelines and industry best practices. They will learn how to establish and implement an effective operational risk management framework within their bank.

Risk Identification and Assessment Techniques
Delegates will acquire practical skills to identify and assess operational risks in various banking operations. They will learn how to use techniques such as Risk Control Self- Assessment (RCSA), Key Risk Indicators (KRIs), and scenario analysis to evaluate potential risks.

Risk Mitigation and Control Strategies
The course will cover different strategies for mitigating operational risks, including the design and implementation of internal controls, process improvements, and other risk reduction techniques. Delegates will also learn about the importance of segregation of duties and other control measures.

Effective Use of Loss Data
Delegates will learn how to collect, analyze, and use loss data to identify trends and drive risk mitigation strategies. This will include understanding the importance of tracking and reporting operational losses, as well as learning how to classify and use this data to improve risk management practices

Focus on Key Operational Risk Areas
The course will focus on major operational risk areas, such as fraud, cyber risk, compliance risk, and business continuity. Delegates will learn about the specific challenges each area presents and how to mitigate associated risks

Operational Risk Monitoring and Reporting
Delegates will learn how to develop and use monitoring and reporting tools for operational risk, including the use of KRIs and risk dashboards. They will gain insights into effective communication of risk exposures to senior management and regulatory bodies

Regulatory Compliance and Industry Standards
A significant takeaway will be an understanding of the regulatory landscape for operational risk management, including the Basel III/IV requirements. Delegates will be equipped with the knowledge to ensure their bank remains compliant with these regulations.

Operational Risk Management For IT Professionals

System and Information technology

SOLVEWORX

Virtual

24 hours

USD 1,300

Registration Deadline
4-May-2025

Delegates:

While there are no specific pre-requisites to attend this course, it is designed with those from the Banking and Financial Services sector in mind, and draws on many common banking principles and practise.
In so doing, the course makes reference to and use of terms and concepts in Banking. IT Risk Managers tasked with assessing and mitigating risks related to the bank's IT systems, applications, and processes.

- Risk managers responsible for managing operational risks within the bank and Operational Risk Officers and Professionals specifically focused on IT operational risk management
- IT Security Managers, responsible for overseeing the bank's IT security measures and IT Risk Managers tasked with assessing and mitigating risks related to the bank's IT systems, applications, and processes.
- Information Security Officers responsible for protecting the bank's information
- Cybersecurity Analysts and professionals who focus on safeguarding computer systems and networks need to understand the operational risks associated with cyber threats.
- Network Security Engineers who design, implement, and manage the bank's network security infrastructure, ensuring secure data transmission.
- Operational Staff and Staff members involved in various operational areas, such as fraud prevention, compliance, IT, and business continuity, would benefit from this course
- Compliance officers responsible for ensuring adherence to regulatory requirements related to operational risk management
- Operations managers responsible for overseeing day-to-day IT banking operations
- Business Continuity Managers and those responsible for the development and implementation of plans to ensure IT systems and operations continue in the face of disruptive events.

The applicability of the course extends beyond these roles listed above, and any banking professional involved in IT and risk management across information security, business continuity, or operations would benefit from gaining knowledge and skills in IT operational risk management in banking including Incident Response Team Members, Vendor Management Specialists, Fraud Prevention Analysts, Data Protection Officers and IT Trainers responsible for training bank staff on IT security practices, requiring up-to-date knowledge of operational risks and best practices.

Operational Risk Management For IT Professionals

System and Information technology

SOLVEWORX

Virtual

24 hours

USD 1,300

Registration Deadline
4-May-2025

Instructor Bio:

Vito Giudice has held key c-suite and board leadership roles in financial services institutions and currently holds several Risk-related board and executive roles across the Financial Services Sector in Australia & New Zealand and provides Risk, Governance and Compliance related advisory services to clients in the United States and Asia.
Mr Guidice has lectured Company Law, Banking Law and Corporate Governance and Financial Planning at both undergraduate and postgraduate level at Monash University Melbourne, and presented annual research papers to the Australia Corporate Law Teachers Association for three years running.

Over the course of his career, Vito has led the Australian Financial Services Licence compliance audits of National Australia Bank and Bendigo Bank and has also held key risk, governance and compliance related roles at Ernst & Young, where he first obtained unique insights into retail banking operations and a deep understanding of the unique risk and compliance processes and systems in banking.
His risk advisory experience has also included identifying compliance obligations across Asia Pacific for ANZ's corporate banking division and he was part of a team that addressed the financial advice remediation within the Commonwealth Retail bank's wealth division, in the aftermath of The Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry in Australia.

He has also led risk management and compliance internal audit projects for Bank Australia and other smaller retail banks, reviewing internal control systems across the bank, and has served as an Independent Risk committee member on the boards of a number of government, private and charitable organisations.
Vito has also previously served as the acting Chief Risk Officer (Financial Crime) for the Consumer, Private and Small Banking division of the second largest bank in Australia, and more recently led the Regulatory Compliance function for a leading wealth manager, and now runs a niche Risk Consulting practise with several large corporate clients in the United States, Europe and Asia.

His areas of expertise span Governance, Risk and Compliance and strategic business management across the banking and regulated financial services sector.
Vito Guidice continues to consult in a number of high-profile roles and set up high performance teams to monitor Compliance with Regulatory standards and reduce compliance and reputation risk across Australia & Asia/Pacific, and continues to train and coach Financial Sector employees on Risk, Innovation, Transformation and compliance obligations.

He holds a Bsc. (Hons) in Mathematics and a Masters degree in Risk Management from Monash University and is a graduate member of the Australian Institute of Company directors.