IFF

THE MECHANICS OF OPERATIONAL RISK

POSTGRADUATE CERTIFICATE

DELIVERED BY DISTANCE LEARNING OVER 14 WEEKS

Contact:
www.iff-training.com
Tel: +44(0)20 7017 7190
Email: cs@iff-training.com

Learning partner of RiskMinds

In partnership with Middlesex University London

COURSE INFORMATION

DELIVERED BY DISTANCE LEARNING OVER 14 WEEKS

WHAT YOU WILL LEARN

No longer seen as a back office function, operational risk teams are an increasingly important component in modern risk management. The fallout from the financial crisis and resulting increased regulatory scrutiny combined with significant industry innovation and disruption from things such as FinTech, AI and cryptocurrencies means those working in operational risk need to constantly upgrade their skills and knowledge at a significant pace.

This course aims to provide a framework for operational risk best practice, demystify the complex issues impacting the industry.

On completion of this distance learning course you will have a comprehensive understanding of all the key aspects of successful operational risk management.

COURSE AT A GLANCE

Unit 1 – Big Picture Overview
Unit 2 – People and Conduct
Unit 3 – Software and Model Risk
Unit 4 – Data Security and Business Processes
Unit 5 – Compliance and Regulatory Change
Unit 6 – Quantification, Scenario Analysis and Mitigation
Unit 7 – Risk Culture and Governance

COURSE LEADER

CLIVE CORCORAN

Clive Corcoran has been involved in the finance and investment management sectors, on both sides of the Atlantic, for more than 25 years. After completing his education in the UK, Canada and the US, he co-founded and became the CEO of an investment management company based in the USA. The company provided wealth management and fiduciary services to a variety of international clients. His own responsibilities included personalised business management, international tax planning and providing strategic financial advice to high net worth individuals. Since relocating to the UK in 2000, he has continued, as an FCA registered investment adviser, to be engaged in providing strategic investment advice to private clients and pension funds.

As an author he has written several titles on finance and investment management.

He has delivered tailored training globally on a variety of topics including operational risk. Clive's courses have a strong emphasis on linking theory with real-life practical insights from his many years of experience

HOW YOU WILL LEARN

- A new module is released every two weeks
- You can read the units online, save them to your computer or print them out
- You set the pace for yourself
- No need to travel or take time off work – cost effective
- Apply the knowledge, skills and expertise to your work straight away

POST GRADUATE CERTIFICATE

To make your studies more relevant and valuable, the course is validated by the Business School at Middlesex University at a Postgraduate Certificate level. For those wishing to receive a Postgraduate Certificate from Middlesex University, an additional marked assignment of 5000 words will need to be submitted, based on a continuing case study that runs throughout the duration of the course.

DATES & PRICE

26 February 2020 (FLF4997)
16 September 2020 (FLF5378)

Standard Price – £1999
With Postgraduate Certificate- £2359

* VAT may be payable depending on your location – see online booking page for details

HOW TO APPLY

Tel: +44 (0)20 7017 7190

Email: cs@iff-training.com

APPLY ONLINE HERE

CUSTOMISED TRAINING

IFF's bespoke digital training solutions will help you address your specific key business challenges. The programme is designed for you, with content focusing on the issues you and your teams are facing. The fully branded digital course will be hosted by us, and unlike other online courses, your employees will receive a specialist qualification at the end of the programme from a London University.

- Tailored content - 100% targeted to cover your business needs
- No travel or time out of the office – 100% Distance Learning
- Value for money – train teams of staff at the same time
- Risk free – we've been doing this for 30 years

We will meet you anywhere in the world. If you would like one of our consultants to talk about your needs in more detail or if you would like more information on our customised training solutions, please contact us on +44 (0)20 7017 7190 or email: cs@iff-training.com

COURSE SYLLABUS

UNIT 1
BIG PICTURE OVERVIEW

Unit Learning Aims and Objectives

On completion of this unit, the successful participant will be able to:

- ★ **Distinguish operational risk from other kinds of financial risks**
- ★ **Understand the core concepts involved in risk governance**
- ★ **Recognise the adverse consequences, including reputational damage and penalties, that arise from operational failures**
- ★ **Understanding the distinction between macro and micro level Key Risk Indicators (KRIs)**
- ★ **Understand how Value-at-Risk (VaR) can be applied to operational risk**
- ★ **Recognise how issues related to misconduct will impact the firm**
- ★ **Explore different contingent scenarios relating to potential operational failures**
- ★ **Articulate the key principles of sound corporate governance**

UNIT CONTENT

Overview of Key Operational Risk Issues and Governance

- Distinguishing operational risk from other kinds of risk
- The impact of operational risk on the organisation
- Implementing an organizational structure based on holistic principles – ERM
- Well-resourced internal audit systems, proper risk discovery, measurement and reporting systems
- Overview of how to determine the level of regulatory and loss absorbing capital for op risk
- Determining the direct and indirect effects of adverse operational outcomes
- Estimating probability of adverse outcome and loss to business
- Determining the direct and indirect effects of an adverse outcome
- HR processes designed to screen new employees, conduct regular reviews, motivate and enhance employee morale
- Separation of risk and compliance function from front office/P&L targets

Adverse Consequences from Operational Failures

- Reputational risk - the trustworthiness of businesses
- Extreme reputational damage may lead to business failure – e.g. Arthur Andersen
- Legal risk -enforceability of contracts with counterparties
- Litigation risk - fines and class action law suits
- Breaches of regulation – e.g. BNP Paribas $9 billion fine for violating US rules on dealing with black-listed countries
- Derivatives risks – e.g. swap agreements between Orange County in California and investment banks were declared null and void
- Avoidance of overly complex instruments -use standardised master agreements
- Rogue trading – e.g. Societe Generale, UBS
- IT systems failures and customer dissatisfaction – e.g. TSB systems integration failure

Case Study
The consequences of the Deepwater Horizon oil spill disaster in the Gulf of Mexico for BP

Macro Level KRIs and Op Risk Indicators

- Characteristics of macro or systemic KRIs – stress levels in the banking system
- Understanding the distinction between macro level KRI's and those which are endogenous to the operations of specific institutions
- Market stress indicators – VIX, bid/ask spread, market microstructure measures
- Use of KRIs for operational risk assessments
- Aggregation of KRIs across different business units
- Development of contingency scenarios – what if analysis
- Using ratios and KRIs for trend analysis
- Continued development of quantitative protocols, and reporting systems for detecting causes of risk resulting in financial loss
- Explanation of how Value-at-Risk (VaR) can be applied to operational risk

UNIT 2
PEOPLE AND CONDUCT

Unit Learning Aims and Objectives

On completion of this unit, the successful participant will be able to:

- ★ **Understand the importance of a code of conduct in corporate governance**
- ★ **Appreciate the need for a diversity of perspectives within human resources**
- ★ **Recognise the role of accountability within various episodes of misconduct – including the LIBOR rigging scandal**
- ★ **Understand the reasons that make possible unauthorised transactions (rogue trading) and what steps can be taken to curtail such possibilities**
- ★ **Understand how compensation can be structured in a way that allows for individual accountability**
- ★ **Analyse the circumstances that make institutions vulnerable to fraud**
- ★ **Appreciate how to design business systems with negative feedback which contain the adverse consequences from operational failures**
- ★ **Recognise the possibility of substantial fines, realised losses and damages from lawsuits associated with fraud and misconduct**

UNIT CONTENT

Best Practice in Human Resource Management

- Commitment by all levels of the organization to ethical principles
- Codes of conduct – articulation of the company's philosophy
- Focus on gender discrimination and prevention of sexual harassment
- Screening of the ethical profile of all executives and board members
- Full engagement of human resources personnel in the risk culture
- Enterprise wide support for ongoing professional development
- Diversity of perspectives - ensure status quo is rigorously challenged
- Remuneration of risk and compliance teams must be wholly separated from front office interference, "star traders" and P&L performance?
- Rewards, bonuses should be adjusted for risk and claw backs and deferred compensation structures should be in place for key revenue generators
- Business ethics and corporate social responsibility (CSR)
- A socially responsible firm should be an ethical firm and vice versa - responsibility to all stakeholders and not just shareholders
- How do businesses ensure that directors, managers and employees act ethically?

COURSE SYLLABUS

Case Study
- Circumstances of the HSBC Money Laundering abuse
- Prohibited dealings with "outlaw" regimes
- Record fine paid to the US regulators

Rogue Trading – Low Frequency, High Losses, Reputational Damage

- Unauthorised trading and fraudulent trading - is there a difference
- How did control systems fail to prevent very large losses?
- Concealment of losses – informational asymmetry between risk takers and risk supervisors
- Conditional deferred payments for traders – claw-backs, bonus payments in subordinated debt and restricted equity etc
- Contingency planning related to stress testing
- Design business systems with negative feedback – not amplifying failures
- Deciding on the appropriate capital allocation for unauthorised trading
- Risk estimates should be fully factored into the assessment of viability/profitability from different kinds of operational activities

Case Study
Review the circumstances of the losses at Societe Generale in 2008 by J Kerviel, and at UBS in 2012 by Kweku Adoboli

LIBOR Rigging Scandal – Systematic Market Abuse

- Circumstances surrounding the manipulation of LIBOR
- Market manipulation, fraud and collusion with external third parties
- Evidence collected by Federal Reserve and Bank of England
- Failure of the regulators
- Collusion between traders at different banks
- Impact on trillions of dollars of derivative transactions
- Fines imposed by regulators
- Legal risk – law suits
- Barclays – recent change of business model and re-organisation
- Example of poor risk culture

Case Study
UK Parliamentary Treasury Select Committee Report on LIBOR Rigging

UNIT 3
SOFTWARE AND MODEL RISK

Unit Learning Aims and Objectives

On completion of this unit, the successful participant will be able to:

- ★ **Understand the core concepts in the architecture of enterprise software, especially systems integration and security issues**
- ★ **Understand the key principles of cyber security**
- ★ **Understand the key elements in new software technologies including blockchain, artificial intelligence and cloud computing**
- ★ **Understand the micro-structure of markets, their fragmentation and the nature of automated trading**
- ★ **Explain the risks associated with high frequency trading (HFT)**
- ★ **Explain the liquidity risks in electronic markets**
- ★ **Demonstrate the importance of, and the risks associated with, modelling activities in banks**
- ★ **Explain algorithmic trading and some of the examples where "flash" trading has led to significant disruptions in financial markets**

UNIT CONTENT

Reliance on Robust and Secure Software Systems

- Architecture of enterprise software – integration and security issues
- Cyber risk – how secure are in bound channels?
- How secure are outsourced systems?
- Documentation of home-made and outsourced solutions
- Increasing focus on data collection and aggregation – FRTB issues
- Complexity issues – integration of middleware with back office systems
- New technologies and integration with legacy systems
- Preparation for block chain technologies – impact on business processes
- Adoption of artificial intelligence (AI) based methods
- Use of machine learning and other cognition modelling

Data Aggregation Depends on an Integrated Software Architecture

- Addressing failures of silo approach to risk reporting systems
- Need for integration of risk reporting systems across business lines and geographical regions
- Requirements within BCBS 239 for aggregating risk exposures
- Identifying potential risk concentrations before they manifest into a critical phase
- Implementing appropriate management information systems (MIS)2 at the business and bank-wide level
- Enhancing the infrastructure for reporting key information, particularly that used by the board and senior management to identify, monitor and manage risks
- Accelerating the speed at which information is available and hence decisions can be made
- Risk reports should be easy to understand yet comprehensive enough to facilitate informed decision-making.
- Description of the risk within FRTB regulations if bank loses ability to use IMA approach
- FRTB requires full integration of front and back office systems for assessing trading book exposures

Case Study
Overview of IMA validation testing within FTRB – backtesting P&L attribution testing

Electronic Markets and Algorithmic Trading

- Description of multilateral trading facilities (MTF's), dark pools
- Fines levied for failure to disclose full list of participants in dark pools
- Fragmentation of market venues and technological infrastructure
- Impact of HFT on market micro-structure
- Nature of "flash" trading with increased risk of "flash crashes"
- New role of electronic market makers
- Regulatory surveillance of potential disruptive behaviour from algorithmic trading
- Circuit breakers in equity markets, futures markets

Case Study
The Flash Crash of May 2010 Impact of High Frequency Trading (HFT) on liquidity in US equity market

COURSE SYLLABUS

UNIT 4
DATA SECURITY AND BUSINESS PROCESSES

Unit Learning Aims and Objectives

On completion of this unit, the successful participant will be able to:

- ★ **Identify the principal sources of cyber risk – internal and external**
- ★ **Understand the risks associated with introducing new business systems and how these need to be thoroughly tested before deployment**
- ★ **Analyse the risks associated with introducing new products and how these need to be thoroughly tested before deployment**
- ★ **Understand the nature of business process re-engineering (BPR)**
- ★ **Undertake diagnostics relating to possible operational loss scenarios**
- ★ **Understand how digitisation, FinTech, blockchain are really a challenge to a banks' business model**
- ★ **Undertake root cause analysis for various operational failures Develop an appreciation of how the business identifies and responds to potential and actual operational risks**

UNIT CONTENT

Cyber Risk and Data Security

- Examination of all breaches and near misses
- Objectives, scope and reliability of incident recording
- Risks from external suppliers and clients – outsourcing risks
- Management of contracts with third party suppliers
- Impact of new products, processes, business lines and locations
- Differentiation between prevention and managing negative outcomes
- Addressing the cultural divide between IT "tech" staff and senior management
- Cloud computing and outsourcing - Amazon Web Services
- Risk assessment process – how does the business identify and respond to potential and actual risks?
- Risk governance philosophy needs to be fully integrated into all accounting, surveillance, IT systems and data storage back-up systems
- Change management – implementing new requirements on privacy, GDPR etc

Critical Business Process Diagnostics

- Internal loss data collection – collation to common causes
- Emerging risks identification – new products and processes
- Thorough testing to ensure robustness of all new proposed offerings to clients
- Characteristics of re-engineering business processes (BPR)
- Six Sigma Approach – application of the approach in financial services
- Features and risks of Straight Through Processing
- "Digitisation, FinTech, blockchain" – all these developments are really threatening banks' business models
- Design business systems with negative feedback – not amplifying failures
- No process or activity too large or too complex for risks to be readily understood
- Adopt holistic and enterprise wide surveillance techniques
- Minor losses that may be accepted – cost of remedy vs. toleration

Case Study

- Systems integration failure at TSB Bank
- Role of external consultants
- Middleware malfunction and inadequate testing
- Costs – direct and indirect to the business

Root Cause Analysis

- Identification of underlying causes for operational failures – digging beneath the surface
- Forensic and systematic analysis of large scale failures and near failures
- Data mining approaches and time line sequences – critical nodes in networks
- Transforming from a reactive approach to operational failure to a pro-active approach
- Prioritising amongst multiple root causes
- Process mapping – identify all critical steps, what can go wrong, what controls can be in place
- Establish the relevant metrics for each root cause leading to process disruptions
- Action plans to alleviate or mitigate symptoms arising from root causes

UNIT 5
COMPLIANCE AND REGULATORY CHANGE

Unit Learning Aims and Objectives

On completion of this module, the successful participant will be able to:

- ★ **Describe the principal kinds of regulatory initiatives**
- ★ **Understand the focus on consumer protections in much regulatory policy in the financial sector**
- ★ **Recognise the growing focus amongst the regulatory community on macro-prudential tools of risk management**
- ★ **Articulate the key revisions to the regulatory framework for banking in the UK since the 2007/8 financial crisis**
- ★ **Explain the key concepts and methods related to the Basel III treatment of operational risk including the new framework which needs to be implemented by 2022**
- ★ **Recognise the value of aligning regulatory compliance and internal best practice regarding operational risk**
- ★ **Recognise the vital importance of compliance with all existing regulation and be vigilant with respect to new regulations that are in the pipeline**
- ★ **Know how to apply best practice in compliance with Basel III requirements regarding operational risk**

UNIT CONTENT

Public Policy and Role of Financial Regulators

- Balancing Regulatory Compliance and Internal Best Practice
- Increasing focus on macro-prudential regulation – stress testing
- Role of political action groups and commercial lobbying
- Surveillance of financial services sector by regulatory bodies
- Focus on boundaries between financial crime and operational vulnerabilities
- Examination of the robustness of procedures to avoid money laundering
- Description of $10 billion fine to BNP Paribas for dealing with clients in countries on US "black list"
- Capital adequacy, Basel III, role of banking supervisors
- Miscellaneous risks arising from government/supra national actions

COURSE SYLLABUS

- Confiscation, nationalisation, capital controls, FATCA
- Regulatory control of fund managements including hedge funds
- Consumer protection focus - SEC, FCA, CFTC, EU Commission

Case Study
- Revisions to the regulatory framework for banking in the UK since the 2007/8 financial crisis
- Role of BOE's Financial Policy Committee (FPC), examination of ring fencing
- Role of the Prudential Regulation Authority (PRA) and the Financial Conduct Authority (FCA) in the UK financial services sector

Basel Measurement Approaches for Operational Risks
- Brief outline of the Basel Basic Indicator Approach (BIA) and Standard Approach (SA)
- Explanation of the Basel III Advanced Measurement Approach (AMA)
- Scenario Based Approach (SBA)
- Loss Distribution Approach (LDA)
- Business environment and internal control factors (BEICFs)
- Key Risk Indicators (KRIs)
- Role of senior management in identifying adverse scenarios
- Distributions for occurrence and severity of losses
- Basel III Business Line and Event Type Codes
- Process Mapping – mapping processes to appropriate regulatory categories
- Templates for data capture for Basel compliance and internal reporting
- Role of external data – scaling of comparable institutions
- SBA templates
- Cascading of failures – how to "group" associated losses

The New Basel Approach to Operational Risk
- BCBS Consultative Documents on revisions to current op risk approaches
- Explanation of the Business Indicator metric
- Non-linear scaling of operational risk to total revenue of a bank
- Using absolute values for estimating bank's exposure to op risk
- Review of the BCBS Operational risk Capital-at Risk (Op CaR) model
- Internal Loss Multiplier and Loss Component

Case Study

Is the Basel Committee moving away from simulations and modelling tools for calibrating capital charges?

UNIT 6
QUANTIFICATION, SCENARIO ANALYSIS AND MITIGATION

Unit Learning Aims and Objectives

On completion of this unit, the successful participant will be able to:

- ★ **Understand the usefulness of a Pareto statistical distribution in calibrating extreme values**
- ★ **Recognise the limitations of internal loss data from previous operational mishaps**
- ★ **Understand the value of a strategic risk management philosophy and cultivation of an ethos of prudence and robust risk control**
- ★ **Understand the nature of power laws in financial modelling**
- ★ **Demonstrate competence in generating adverse scenarios for analysing how to control and mitigate operational losses**
- ★ **Understand how various insurance products can mitigate some kinds of operational losses**
- ★ **Know how to conduct a RCSA workshop for operational risk assessment**
- ★ **Apply techniques for modelling potential tail outliers in operational failures**
- ★ **Know the design principles for robust control procedures that can avoid and mitigate operational failures**

UNIT CONTENT

Risk Control Self-Assessment (RCSA)
- Risk identification – kinds of risks and associated internal processes
- Involvement of internal departmental heads and op risk committee
- Questionnaires – alerts to potential risk areas and points of failure
- Conducting an RCSA Workshop – role of facilitators, experts, back office
- Internal reporting mechanisms - iterations, validation protocols
- Key Risk Indicators – developing new KRIs and following peer groups
- Monitoring systems to ensure no misconduct in trading and reporting
- Adequacy of internal controls to prevent rogue trading
- Is collateral being posted according to all obligations with counter parties and CCPs?
- Are all trading activities being checked by at least two separate parties?

Methodologies for Measuring and Modelling Operational Risks
- Basel Committee requires close monitoring of internal modelling and model risk
- Loss Modelling Methods – contingency scenarios
- The Loss Distribution Approach (LDA)
- Templates for collecting loss data
- Using Scenario Based Analysis (SBA) for filling in gaps in data
- The role of Business Environment Internal Control Factors (BEICFs)
- Scarcity of historical data in the outliers for operational losses
- Different distributions for modelling severity of losses
- Monte Carlo based loss scenarios
- Stress testing methodologies
- Data limitations involved in quantifying operational risks
- Segregating internal vs. external software failures

Case Study

Estimating Extreme Losses with Extreme Value Theory (EVT) and Power Laws
- Lack of outlier loss data – challenge to statistical distribution analysis
- Usefulness of Pareto distribution in calibrating extreme value
- Worked examples of applying EVT to tail risk in operations
- Explanation of power laws in natural world – earthquakes
- Evidence for power laws in finance
- How to determine whether power laws are present

Managing and Mitigating Operational Risks
- Enterprise wide risk control environment – strategic management philosophy and cultivating an ethos of prudence and robust risk control

COURSE SYLLABUS

- Risk assessment process – how does the business identify and respond to potential and actual risks?
- Risk control systems need to be pro-active not reactive – not "fire-fighting"
- Avoid silos - when risk information is kept isolated in separate divisions supervision and vigilance at the senior level becomes impossible
- Fully resourced compliance officers check on whether regulations are being followed
- Use of insurance products to mitigate operational losses

Case Study
Legitimate and invalid uses of insurance to mitigate risk – taken from the Basel Committee's documentation on Operational Risk

UNIT 7
RISK CULTURE AND GOVERNANCE

Unit Learning Aims and Objectives

On completion of this unit, the successful participant will be able to:

- ★ **Identify the characteristics which give rise to a poor risk culture**
- ★ **Understand the dynamics of organisational change and how to impact the risk culture**
- ★ **Recognise that the risk governance philosophy should be fully integrated into all accounting, surveillance, IT systems and internal audit functions**
- ★ **Understand why "group think" can lead to poor risk governance**
- ★ **Recognise the value of ongoing learning and development associated with raising awareness and competence in risk management at all levels**
- ★ **Propose methods and changes to current practice that will lead to an improved risk culture**
- ★ **Understand the value of continuing refinement of quantitative protocols and reporting systems for detecting the causes of operational risk which result in financial loss**
- ★ **Appreciate the value of a holistic approach to operational risk management**

UNIT CONTENT

Symptoms of Poor Risk Culture

- Poor tone set by the key executives and weak governance
- Boards of directors with cronyism and lack of independent NED's
- "The Enron scandal grew out of a steady accumulation of habits and values and actions that began years before and finally spiralled out of control"
- Inconsistent approaches to mark to market accounting – e.g. JP Morgan's use of most favourable marks to avoid registering large Whale losses
- A "box ticking" mentality which produces myopia and failure to see the big picture
- Front office revenue generators not adequately subject to "internal controls"
- Over reliance on special purpose vehicles and off-balance sheet accounting
- Failing to eliminate dysfunctional, legacy business processes
- Failing to recognise "blind spots" of the organisation's culture
- Accepting a lack of transparency in high-risk areas
- Senior management endowed with "charisma" and an untouchable quality which makes them remote from internal criticisms

Case Study
Collapse of Enron in 2001 and the dissolution of its auditors, Arthur Andersen

Changing The Risk Culture

- Cultural change requires sustained effort and time to adapt to new norms
- Organization's structure and culture should reward adherence and advocacy of best practices and disown activities that detract from it
- Consistent, coherent, sustained and visible leadership in terms of tone and practice from the top of the organization – C-level executives and board members
- Support for ongoing learning and development associated with raising awareness and competence in risk management at all levels
- Privacy and protection to whistle-blowers
- Very clear articulation of accountabilities for those managing risks and uncompromising approach to holding them to accountability
- Demotion of the notion of box ticking and encouragement of more holistic views
- Avoidance of silos - lack of macro oversight
- Systems of accountability, responsibilities bounded by safety thresholds, alerts, disciplinary guidelines, sanctions for violation

Case Study
Avoiding group think – encourage diversity in thinking rather than ostracizing alternative viewpoints

Best Practices for Refining Governance and the Risk Culture

- Articulating a corporate culture which is fully aligned with the risk management process
- Enterprise wide risk control environment – strategic management philosophy and cultivating an ethos of prudence and robust risk control
- Risk control systems need to be pro-active and not reactive – not "fire-fighting"
- Risk governance philosophy should be fully integrated into all accounting, surveillance, IT systems and internal audit functions
- Frequent consideration of appointing new external auditors
- Selection of risk control strategies appropriate to the objectives of the business and implementation of such strategies
- Implementing an organisational structure including wellresourced internal audit systems, proper IT monitoring and back office functions.
- Continued development of quantitative protocols, and reporting systems for detecting causes of risk resulting in financial loss
- HR processes designed to screen new employees, conduct regular reviews, motivate and enhance employee morale
- Fully resourced compliance officers check on whether regulations are being followed

OPTION OF A POSTGRADUATE CERTIFICATE WITH MIDDLESEX UNIVERSITY

In partnership with Middlesex University London

You have the unique opportunity to choose a validated option for this course and receive a postgraduate certificate on completion. This is a Middlesex University qualification, jointly developed by Middlesex University and IFF, and quality assured by Middlesex University. However, if university validation isn't important to you there is still the opportunity to take the standard non-validated course.

WHAT DOES THE CERTIFICATE ENTAIL?

In addition to studying all the units and passing the short self assessment tests after each unit, you will need to submit a 5000 word assignment at the end of the course which will be assessed. The assignment will be a cumulative project that you will work through and build upon during each stage of the course.

If you wish to book on the certification course there will be an assessment fee of £360.

ENTRY REQUIREMENTS

Participants wishing to undertake the Postgraduate Certificate are required to have a degree or equivalent qualification (or relevant work experience).

Participants wishing to undertake the course but not receive the Postgraduate Certificate are not required to have any formal qualifications.

ABOUT OUR PARTNER MIDDLESEX UNIVERSITY

History

Middlesex University is a large London based university with a history in higher education dating from 1878. In 1992 it was granted the Royal Charter making it a university. The university offers a broad range of courses through four academic schools of Arts and Education; Business; Engineering and Information Sciences; Health and Social Sciences and their Institute for Work Based Learning.

Middlesex University has over 34,000 students studying on its courses worldwide, both at its own campuses and also with partner institutions, making it one of the largest providers of British university education to international students. Middlesex University has a long history of successful collaborations with the corporate sector. It was the first academic institution to develop industry specific MBA programmes (Shipping & Logistics and Oil & Gas) delivered 100% by distance learning.

INTERNATIONAL REACH

Middlesex University is committed to meeting the needs and ambitions of a culturally and internationally diverse range of students by providing challenging academic programmes. It has a major international business school based in London with overseas campuses in Dubai and Mauritius and a global portfolio of partnerships delivering high quality validated programmes in business and management.

Staff and students come from a wide spectrum of cultures and backgrounds with a common interest in executive education that is world class, modern and applicable. Middlesex University Business School is proud of its dedicated teachers and its rich range of learning resources including distance learning and virtual learning environments.

BENEFITS OF STUDYING FOR A POSTGRADUATE CERTIFICATE WITH US

A MIDDLESEX POSTGRADUATE CERTIFICATE:

- Is project based and practical
- Offers networking opportunities during and after the course
- Provides exceptional teaching staff
- Delivers applied learning experiences
- Combines academic rigour with individual support

HOW IS THE COURSE VALIDATED?

This programme is quality assured by Middlesex University and after successfully completing your studies you will receive a Postgraduate Certificate from Middlesex University. Middlesex Certificates are recognised worldwide.

QUALITY

The Quality Assurance Agency (QAA) visited Middlesex in 2015 and noted in its report that its auditors had confidence in the University's current and likely future management of its academic standards and of the learning opportunities available to students.

THE UNIVERSITY IS A MAJOR PROVIDER OF BUSINESS AND MANAGEMENT EDUCATION, WITH AN IMPRESSIVE TRACK RECORD OF WORKING IN PARTNERSHIP WITH THE PUBLIC AND THE PRIVATE SECTOR, AS WELL AS INTERNATIONAL ORGANISATIONS

THE MECHANICS OF

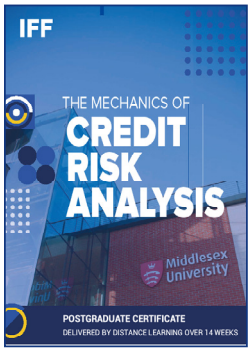
OPERATIONAL RISK

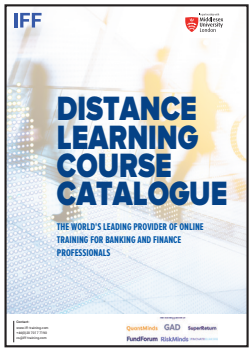
POSTGRADUATE CERTIFICATE

DELIVERED BY DISTANCE LEARNING OVER 14 WEEKS

APPLY ONLINE HERE

RELATED DISTANCE LEARNING COURSES





IFF is the learning partner of

RiskMinds

Contact:
www.iff-training.com
Tel: +44(0)20 7017 7190
Email: cs@iff-training.com

Duration:
14 Weeks

In partnership with
Middlesex University London