OPERATIONAL RESILIENCE & BUSINESS CONTINUITY

Course overview

This training teaches you practical methods to deal with business continuity and scenario planning in the banking/ financial institution environment. This is an intensive course on Business Continuity and operational resilience focused on the banking and non-financial institution environments. Business Continuity Planning is the process through which an organization ensures the maintenance or recovery of operations, including services to customers, when faced with disruptive events such as natural disasters, technological failures, human error or terrorism. The course will allow participants to explore operational disruptions and how they can benefit from future challenges and opportunities. Participants will learn the best practices for integrating an effective crisis management plan. They'll learn how to break down silo boundaries to improve operational resiliency as well as leverage emerging technology to improve operation agility and robustness. Delegates will have the opportunity to enhance their skills in governance and compliance while ensuring the operational resiliency framework aligns with wider organization recovery objectives.

Learn How To

- Identify key elements that should be in place to adapt and respond to threat.
- Integrate business continuity management framework and strategies.
- Understand the challenges and benefits of impact intolerance.
- Define the importance of data to define tolerances in emerging technology.
- Prepare for incidents that mat occur through an effective crisis response.
- Apply best TPRM practical approaches for integration into the supply chain.

Who should Attend?

Relevant departments may include but are not limited to:

- Operational risk
- Business continuity management
- Incident management
- Crisis management
- Third-party risk management
- Technology/IT.

COURSE MODULES

Module 1: Operational Resilience: Overview & Regulatory Landscape

- Defining operational resilience and how it compares to operational risk and business continuity.
- Operational resilience key global regulations
- Operational resilience core components
- Assessing operational resilience

Module 2: Creating Operational Resilience Frameworks

- The role of governance in operational resilience frameworks
- Dependency mapping and identifying important business services.
- What key elements of resilience should be in place to adapt and respond to any threat?
    - Human resiliency
- Ensuring operational resilience framework aligns with wider organization recovery objectives.

- How will these frameworks be used day-to-day?

Module 3: Business Continuity Management

- Practical BCM insights aligned with current BoE, PRA, and FCA requirements.
- Integrating BCM framework and strategies
- Launching clear reporting functions for continuous monitoring
- BCM connection with operational resiliency
- Breaking down silos boundaries to improve operational resilience.

Module 4: Understanding Impact Tolerance

- Defining financial, regulatory, and client impact
- Effective scenario testing and planning
- Setting impact tolerance: challenges and benefit
    - Experimental empiricism vs judgement vs model/metrics
    - Business objectives vs products vs processes
- Who is responsible for setting them?
- Find the 'right' type of historical data to facilitate impact analysis.

Module 5: Emerging Technology in Operational Resiliency

- The importance of data to define tolerances.
- Investing and integrating data analytics and estate monitoring technology
    - Enhance governance and compliance process.
- Improve operational agility and robustness.
- Future challenges and opportunities

Module 6: Effective Crisis Management

- Regulatory requirements
- Identifying vulnerabilities and risks within the organization
- Planning and preparing for incidents that may occur.
    - Design considerations for effective crisis response
- Creating communication plans for possible disruptions
- Outcome based approach: practical consequences of ops. res.
    - In-crisis capability
    - Enhanced service recovery

Module 7: Third-Party Management

- Understanding the TPRM lifecycle
- Identifying key TPRM risks through:
    - Risk assessments
    - Effective controls
    - Validation
- Impact on the lifecycle of resiliency: business continuous modelling
- Practical approaches for integration into the supply chain
- Implications of subcontracting
    - Fourth parties + Nth parties
    - Cloud services

Module 8: Learning from Operational Disruptions

- COVID-19: lessons learned.
    - Response to crises
    - Control framework
- Proactively learning from incidents
    - Assessing probability of threats
- Improving internal and external party collaboration
- Aggregating data on failures and near misses
- Exploring alternate methods of servicing clients

End of Course & Wrap Up

COURSE DURATION	DELIVERY MODE	DELEGATE CLASS SIZE	COURSE FEE/PARTICIPANT
3 DAYS	In-Plant	8 (Guaranteed Minimum)	For quote, please click ***http://demvros.com/contact/***
Discount is available for class size above the minimum. Please visit ***www.demvros.com*** or call 08056154199 or e-mail for enquiries.			