

Risk Management and Cyber Security

From risk environment to risk culture, the course covers in breadth and depth the most topical elements of non financial risk management and its challenges for the financial services industry.

Designed by a world leading expert in the field and delivered by a highly regarded speaker, the course is a must-have for all the operational risk practitioners wishing to benchmark their practice and discuss best practices. It is also a fantastic opportunity for newcomers to gain a comprehensive overview what modern operational risk managers need to know.

Delegates will leave the course equipped with a new network of practitioners, a wealth of content, additional references and readings, and an open line for further questions with the training designer and delivery team, Ariane Chapelle and David Lannoy.

Key Objectives and Learning Outcomes :

After the course, participants will know about:

- Identification of emerging risks
- Risk networks rather than risk registers
- Key elements of cyber security
- Must-know about cyber security and threats
- Leading KRIs framework for identification and design
- Preventive KRI for cyber and information security
- Implementing ORM: the invisible framework
- How to differentiate and address human errors
- How to use root cause analysis most effectively
- Influencing behaviours for better control
- All best practices in operational risk management for financial companies
- Risk Reporting and Conduct reporting
- Building a framework for risk culture change
- Scenario analysis and assessment

Who Should Attend

- Heads of Operational Risk
- Enterprise Risk Managers
- Operational Risk Managers
- Operations Managers
- Internal Auditors
- HR officers
- Compliance officers
- Consultants
- Regulators

Course outline

Day One: Emerging risks, Conduct and Risk Culture
--

Session 1: Risk identification tools and emerging risks

- Tools and techniques for risk identification
- Risk register: a list
- Risk connectivity: network of risks
- Emerging risks

Class Exercise: identify the network of your top risks and class feedback

Session 2: Implementing ORM: the invisible framework

- Governance of Operational Risk
- 1st line and 2d line: The partnership model
- Use and reuse: The Invisible Framework
- Business value of ORM

Workshop: build a business case for risk management

Session 3: Risk reporting and Conduct reporting

- Modern issues on events and risk reporting: the regulator's view
- Analysing operational risk data: get insight, tell a story
- Management information: the "reporting cake"
- Aggregate and escalate risk information: your options
- Conduct reporting: themes and details

Highlights of best practice, Group discussion and sharing of experience

Session 4: Implementing the Desired Risk Culture: a method

- Defining Risk Culture
- Acting on behaviours: the *Influencer*
- Necessary conditions: willingness and ability
- Risk Culture: DESIRE steps: Define – Inspire – Support – Enable – Reinforce - Evaluate
- Assessing the risk culture

Group work: Plan your own culture change

Day 2: Risk Appetite, Internal controls and KRIs

Session 1 : Defining Risk Appetite statements and tolerance limits

- Industry guidance on Risk Appetite
- Risk appetite, tolerance, risk limits and controls
- Templates and options for actionable Risk Appetite
- Risk Appetite Statements: Features and Examples
- Cascading Risk Appetite: RCSA & Indicators
- KRI and risks limits

Session 2: Internal Controls: Human Error and Control Design

- Slips and mistakes: Typology and causes of human errors (J. Reason)
- HRA: Human Reliability Analysis and other methods
- Understand and treat the causes of human error
- Effective or Illusory controls
- Prevention by Design

Group work: best and worst controls in the business: sharing of experience

Session 3: Root causes analysis – the bow-tie

- Root cause analysis: tool and method
- Benefits of root cause analysis: tracking the common failures and systematic patterns
- Treating causes over symptoms
- Bow-tie: a most effective tool to define
 - Preventive and corrective controls
 - Leading KRIs
 - Risk likelihood and expected impact

Session 4

Exercise: apply the bow-tie to one of your incident; share the lessons learnt

Day 3: Cyber Security and Key Risk Indicators

Session 1 : Features and types of leading KRIs

- Features of leading KRIs
- KRI, KPI, KCI: definitions and uses.
- A typology of Key Risks indicators
- KRIs: metrics of risks drivers
- **Case studies on selecting metrics of risk drivers**

Session 2: Cyber threats and information security

- Cyber threat landscape
 - Key controls in cyber security
 - Physical and behavioural measures
 - Priorities in prevention
 - Lessons learnt from some incidents
- Q&A, benchmarking and exchange*

Session 3: KRI applied to Cybre risks

- KRI for key cyber controls
- Governance KRIs
- Behavioural KRI

Session 4

Case studies on cyber attack and practical workshop

Day 4; Scenario Analysis and Project Risks and Conclusions

Session 1: Scenario Analysis: Governance, Stress testing and Assessment methods

- Four dimensions of stress-testing
- Steps and governance of scenario analysis
- Tackling behavioral biases in scenario assessment
- Industry practices and lists of scenarios
- Assessing probabilities of rare events through structured scenarios
- Acting on Scenario Analysis

Session 2

Class exercise: structure your own scenario in probability and impact

Session 3: Reorganisation risk and project management

- Risk due to changes and reorganisations
- The trap of cost-cutting
- Invisible opportunity costs
- Essentials of project risk management

Class debate and sharing of best practice

Session 4: Key messages and wrap-up

- What have you learnt?
 - What will you remember?
 - What will you apply?
-