MERCURY

Third Party Risk Management (TPRM)

Third Party Risk Management (TPRM)

Introduction:

Third-party risk is a form of operational risk and includes the risk that arises from relationships with third-party providers such as suppliers, contractors and other business partners.
Regulators are concerned about the types of risks that third parties and, in turn, firms could be exposed to.
This course is aimed at providing a comprehensive overview of Third-Party Risk Management TPRM from defining its scope, through the design of a robust framework, to the day-to-day operation of the TPRM processes.
Our Third-party Risk course will help your team understand the various third-party risks and how to manage them.

Targeted Groups:

- Those involved in risk management
- Those involved in cybersecurity
- Anyone who wants to get a better understanding of TPRM best practices and tools

Course Objectives:

At the end of this course the participants will be able to:

- Appreciate why third-party risk has become so important
- Recognise risks companies face in their third-party population and the specific threats they present
- Identify the key features of third-party risk management TPRM
- Appreciate the regulatory landscape and key terminology used in third-party risk management TPRM
- Distinguish between the stages of the TPRM lifecycle
- Create a business continuity, termination strategy and exit plan for material outsourcing relationships

Targeted Competencies:

- Third-party risk management
- Vendor management
- Operational risk
- Resiliency
- Business continuity
- Risk management
- Internal audit
- IT/Data risk

Course Content:

Unit 1: Defining Third Party Risk Management TPRM

- Defining the scope of TPRM
- What third parties should be covered?
- Classifying your third parties

Unit 2: Identifying and understanding the risks relating to the third parties

- Identifying the objectives impacted by third parties
- Defining the impact types from third party risks
- Direct risks to your organisation
- Indirect risks within your third parties
- Developing a taxonomy of third party risks
- Using Risk Bow Tie analysis to map and understand the risks

Unit 3: A Third Party Risk Management Framework

- Aligning to ISO 31000
- Mapping the 8 elements of ISO 31000 to your TPRM processes
- Communicate and Consult. Consider native language/
- Scope, Context, Criteria
- Risk Identification
- Risk Analysis
- Risk Evaluation
- Risk Treatment
- Monitoring and Review
- Recording and Reporting
- Mapping a TPRM ecosystem

Unit 4: Compliance requirements

- Understanding the key compliance requirements for TPRM, including:
- Outsourcing
- Modern Slavery
- Anti-bribery and corruption
- Privacy and data protection
- Due Diligence
- Factoring compliance and compliance management into your TPRM processes

Unit 5: Mapping the steps in TPRM

- Third party selection criteria and process
- Initial screening and tiering
- Initial Due Diligence
- Decision and approval process
- Onboarding including contractual arrangements
- Ongoing monitoring and maintenanc
- Incident management: Non-performance, Failure.
- Offboarding
- Linkage to other risk types and processes
- Link to key risks types internally e.g. Cyber, Fraud, Technology, Data etc.
- Linkage to Operational Resilience

Unit 6: Initial screening, tiering and Due Diligence

- Key factors to consider in initial screen e.g. Data security, financial security etc.
- Sourcing the information: Internal or use of third party bureaus?
- The role of, and link to Risk Appetite
- Tiering methodology to understand importance of third party
- Determining the extent of Due Diligence
- Carrying out Due Diligence

Unit 7: Ongoing monitoring and maintenance

- Due diligence updates
- Ongoing compliance
- Ongoing SLA / contract monitoring
- Ongoing management including third party training
- Risk metrics and monitoring, external and internal data, and alerts
- Escalation and treatment
- Reporting and Analytics