



Reputational Risk Governance and Response Training Course

1 – 5 November 2027
Kuala Lumpur

Reputational Risk Governance and Response Training Course

Ref: 1292_195489 **Date:** 1 – 5 November 2027 **Location:** Kuala Lumpur **Fees:** 5200 Euro

Overview

Reputational Risk Governance and Response Training Course is a one-week course for risk, compliance, communications, legal, audit, and strategy professionals who leave with a Reputational Risk Governance and Response Framework. Participants map stakeholder expectations, assess reputation drivers, detect emerging issues, set indicators, test scenarios, and govern response choices. The course connects dispersed signals and ownership through evidence-led assessment, escalation, monitoring, assurance, and board reporting. Agile Leaders Training Center frames reputational risk governance and response as a cross-functional risk discipline.

Who Should Attend

- Functions responsible for enterprise and strategic risk oversight
- Teams monitoring stakeholder expectations and reputation signals
- Functions governing conduct, compliance, ethics, and culture
- Teams managing communications, digital channels, and crisis interfaces
- Functions assuring third-party, sustainability, and operational exposure

The course assumes participants already assess organizational risks or stakeholder issues and leaves out introductory public relations and media-writing skills.

Departments and Industries

The course supports departments and industries exposed to stakeholder trust, conduct, digital, and operational reputation risks.

- Risk, compliance, legal, audit, and ethics functions
- Communications, corporate affairs, investor relations, and strategy teams
- Financial services, insurance, and investment organizations
- Energy, manufacturing, logistics, and technology organizations
- Healthcare, education, nonprofit, and public-service organizations

Learning Objectives

By the end of this course, participants will be able to:



- Analyze stakeholder expectations and reputation drivers
- Apply reputational risk identification and assessment methods
- Build indicators, thresholds, dashboards, and escalation paths
- Evaluate conduct, third-party, and digital exposure scenarios
- Prioritize preventive and responsive treatment choices
- Build monitoring, assurance, and board-reporting evidence

Course Agenda

Day 1: Reputation Risk Architecture

- Reputation Asset and Risk Boundary Map
- Stakeholder Expectation and Trust Matrix
- Reputation Driver and Dependency Model
- Risk Ownership and Accountability Map
- Reputational Risk Governance Charter

Day 2: Exposure Identification and Assessment

- Emerging Issue and Signal Register
- Conduct and Culture Exposure Assessment
- Third-Party and Supply-Chain Reputation Map
- Digital, Cyber, and Social-Media Exposure Scan
- Reputation Impact and Velocity Matrix

Day 3: Indicators and Escalation

- Reputation Key Risk Indicator Library
- Stakeholder Sentiment Evidence Dashboard
- Risk Appetite and Tolerance Statement
- Threshold Breach and Escalation Protocol
- Cross-Functional Issue Triage Model

Day 4: Scenarios, Response, and Reporting

- Reputation Scenario Analysis Method
- Preventive and Reactive Treatment Portfolio
- Crisis Interface and Decision Rights Map
- Response Evidence and Recovery Tracker
- Board Reputational Risk Reporting Pack



Day 5: Reputational Risk Practice

- Exercise: Stakeholder and Driver Mapping
- Exercise: Exposure and Indicator Calibration
- Exercise: Scenario Escalation and Response Decision
- Exercise: Monitoring and Board Assurance Briefing
- Capstone Exercise: Reputational Risk Governance and Response Framework

Practical Exercises

The course uses suggested activities that connect stakeholder evidence, risk decisions, response ownership, and governance reporting.

- Suggested activity: map trust drivers and early signals for a financial-services organization.
- Suggested activity: assess third-party, digital, and conduct exposures for a technology organization.
- Suggested activity: calibrate indicators and escalation thresholds for an emerging stakeholder issue.
- Suggested activity: present a scenario response and assurance position to a board risk committee.

FAQs

Who suits reputational risk governance and response training?

Reputational risk governance and response training suits professionals who assess organizational risks, stakeholder issues, conduct, digital exposure, communications, or assurance and already contribute to cross-functional risk decisions.

How does reputational risk management differ from crisis communications training?

Reputational risk management identifies, assesses, governs, monitors, and treats reputation exposure before and after events, while crisis communications training concentrates on messages, channels, spokespeople, and media engagement during disruption.

What are the main drivers of reputational risk?

Reputational risk drivers include stakeholder expectations, conduct, culture, governance, service outcomes, cyber events, digital narratives, third parties, environmental effects, supply chains, and the quality of organizational response.

How can reputational risk indicators support escalation?

Reputational risk indicators support escalation by translating stakeholder, conduct, operational, digital, and third-party signals into thresholds, ownership, review triggers, and documented decisions.



How should boards receive reputational risk reporting?

Boards should receive reputational risk reporting that connects exposure, stakeholder evidence, trends, thresholds, scenarios, treatment status, assurance gaps, decisions required, and accountable owners.

Conclusion

The course integrates stakeholder analysis, reputation drivers, exposure assessment, indicators, appetite, escalation, scenarios, response, monitoring, assurance, and board reporting. Participants take back a Reputational Risk Governance and Response Framework containing maps, registers, dashboards, protocols, and reporting evidence. The framework changes how teams connect signals, assign ownership, choose treatments, and govern reputation exposure.