Foundations of IT Risk Management

Course Schedule – Topics & Activities

IT Risk Governance

- IT & enterprise risk management integration
- Risk universe
- Risk governance & management definition, roles & responsibilities
- Enterprise risk culture
- Risk appetite & risk tolerance
- Stakeholders in risk management
- Responsibilities & accountabilities for IT risk management
  - RACI charts
- Standards, frameworks, & best practices for IT risk management
- Risk maps

Risk Identification

- Risk analysis workflow
  - Risk identification
  - When & who will participate
- Risk scenario components & vocabulary
- Identifying the components of a risk scenario
- Consideration of business objectives when identifying risks
  - Determining the scope & number of risk scenarios
  - Risk factors that apply to risk scenarios
  - Risk & reward in a competitive environment
  - Caveats to risk identification
- Internal & external risk factors
- Identify relevant sources of risk data
- Tools available to extract & analyze data
  - Loss, threat, & vulnerability events
  - Additional key terms & formulas for risk identifications
  - Risk calculations
  - Inherent, current, & residual risk
  - Elements of a risk register
  - Best practices to building a set of risk scenarios
- Risk reporting guidelines
Customizing risk reporting
- Risk reporting communication process
- Applying risk aggregation concepts for enhanced risk communication
- Expressing IT risk in business terms

• Develop & support risk awareness training tools & techniques
  - Relate security concepts to risk assessment

Risk Assessment, Evaluation, & Analysis

• Key terms “frequency” & “magnitude”
  - Risk aggregation, risk analysis, IT risk & risk reduction

• Identification of different IT-related business risks
• Collecting data on external & internal operating environments
• Facets of risk to assist in risk evaluation
• Analyzing data to report exposures & opportunities
• Value enablers / inhibitors / destructors for risk scenarios

• Risk analysis methods
  - Quantitative
  - Qualitative
  - Semi-quantitative

• Risk calibration
• Tools & techniques for data extraction, aggregation, & analysis
• Components of a risk profile
• Customizing a risk register template
• Components of a risk response plan
• Building specific risk scenarios from generic scenarios

Risk Response

• Risk response key terms
  - Avoid
  - Mitigate
  - Share / transfer
  - Accept
  - How residual risk relates to inherent risk & risk appetite

• Leading practices for risk response
• Effective risk reporting to enable informed business decisions
• Cost / benefit analysis in evaluating risk response
• List various parameters for risk response selection
• Exception management & its relation to risk management
• Business case to support project management of IT risk response
• Key sections of a risk response plan

**Risk Monitoring**

• How risk monitoring enables the risk management process over time
• Principles of risk ownership
• Standards, frameworks, & best practices related to risk monitoring
• Differentiate between key risk indicators (KRIs) & key performance indicators (KPIs)
• Evaluate performance & risk levels
• Apply concepts of effective reporting to ensure value-added risk monitoring
• Common risk & compliance reporting requirements, tools, & techniques
• Common risk reporting communication flows
• Risk assessment methodologies
• Data extraction, aggregation, & analysis tools & techniques
• Sources of information for the risk monitoring process

*Topics and activities may vary by class and instructor.*