BUSINESS RISK MANAGEMENT LTD

Risk Management and the Internal Audit Role
On-line course
2 days

Why you should attend

Most Heads of Internal Audit would say that their functions have adopted a risk based approach. However, has this process been fully embedded?

Have you for example:-

- **Linked your audit programmes and testing directly with the risk registers?**
- **Made suggestions for reducing controls for over-managed risks?**
- **Challenged management's evaluation of the residual risks? If so, do you have a consistent basis for this challenge?**
- **Encouraged management to determine a target for each risk?**
- **Reviewed the ERM process?**
- **Carried out audits of complex business activities such as Cyber risk, reputation management and IT Governance?**
- **Audited your organisation's website, or social media activities?**

This course is designed to cover these and other significant challenges of the modern Internal Audit role

Who should attend?

- **Audit managers and senior auditors**
- **Lead auditors**
- **Auditors responsible for developing or implementing a risk based approach**
- **Managers and Directors of business functions – to aid their knowledge of the modern IA approach.**

Course Level

- **This is an intermediary level course and delegates should have at least 12 months experience in Internal Audit (or other assurance roles) to attend**
- **Delegates should have a good educational standard and/or a professional qualification or be in the process of studying for such qualifications**
- **No advance preparation is required**

- **Delivery method – On-line-live (with exercises and case studies to provide practical application of the tools and techniques)**

After completing this course you will be able to

- **Advise management on the reality of controls and risk management effectiveness**
- **Challenge management's evaluation of risks and sell the benefits of proactive risk management**
- **Audit major and complex areas of risk for your business with confidence**
- **Promote ERM as a positive business process**
- **Add measurable value to your organisation by the application of risk-based audit services**
- **Help management to identify over-managed risks**

CPE credits

- **Participants will earn 8 CPE credits (6 in the Auditing field of study and 2 in the Management Advisory Services field of study)**

Day 1 The risk focus of internal Audit

Risk Management and Internal Audit

- **The need to focus audit attention towards the most significant risks**
- **The function needs to enhance organisational value by providing stakeholders with risk-based, objective and reliable assurance, advice and insight.**
- **IA must ensure that appropriate risk responses are selected that align risks with the organisation's risk appetite**
- **The need for much higher levels of assurance than ever before**
- **What level of assurance can really be provided?**
- **What should be the audit role in relation to identification and managing of risks**
- **Could working with management to identify and evaluate risks compromise the independence of the function?**
- **Is a risk based approach a methodology or a state of mind?**
- **Why has it become so important?**
- **IA needs to be available to offer advice and guidance**
- **The primary role of internal audit should be to help the Board protect the assets, reputation and sustainability of the business**

Exercise 1 – Re-defining the IA role for 2021 and beyond

The modern risk based audit approach

- **Worldwide trends in IA**
- **Trends (from GRC research and the BRM Internal audit best practice database)**
- **The need for auditors to provide wider assurance**
- **How risk based audit has changed the face of auditing**
- **Audit's primary roles, objectives and concerns**
- **Questions about the maturity of the audit process**
- **The need widen the coverage - to become more operationally based**
- **The importance of dealing with the audit risks not just the business risks**
- **The steps needed to enhance the risk based approach**
- **The key challenges resulting**

Exercise 2 - IA strengths and opportunities

Internal Audit and ERM (Enterprise risk management)

- **The key elements of Enterprise risk (ERM)**
- **The key relationship between risk and objectives**
- **Why senior management may lack a full understanding of the risks**
- **Risk cultures and the implications for IA**
- **Surprises and risk and why IA should ask about surprises**
- **Measurement of risk and why many organisations scoring process may lead to misunderstanding of significance**
- **Categories of risk**
- **The need to challenge risk assessments**

Exercise 3 - Analysing a disaster

Helping to make Risk Management a positive process

- **Ensure that staff know that risk management is not a fad or the latest initiative – it is a business process**
- **Ensure you define risk as the need to get things right – not what can go wrong**
- **'Ring fencing' risk exposure - never allow one part of the business to impact the whole organisation**
- **Determining and communicating your attitude to risk and your required risk culture to managers and stakeholders**
- **Recognise that reputation is both your biggest asset and the biggest risk you face – and one you cannot insure**
- **Do not wait until you are required to provide evidence of effective risk management by regulators or legislation – this will usually be too late**
- **Market the audit process internally and to stakeholders**
- **Recognise that your employees will only be interested in managing risks if there is a benefit for them in doing so**
- **Realise that if managers want to get a proposal through, they will tend to understate the risk (if you let them)**

- Promote risk as the pulse of the organization and make sure that you have personnel to regularly take this pulse

Exercise 4 - What steps can IA take to help make risk management a value added process?

Identifying over-managed risks

- These are likely to be the risks in the green zone of the risk matrix
- Why unnecessary controls are often not removed
- Why Internal Audit does not focus on this aspect
- When did you last suggest reducing controls?
- Challenge 'we have always done it this way'
- Do we have to do it?
- What are the benefits / penalties associated?
- Can you reduce effort in some areas to give time and resource for the priorities?
- Case studies

Exercise 5–How to identify over-managed risks

Day 2 Evaluating the Risk management process

Assessing the effectiveness of the risk process

- Reviewing the business objectives
- Are the objectives comprehensive and SMART?
- Do the risks in the register relate properly to the objectives?
- Are they specifically linked to the objectives and recorded?
- Are the inherent risks correctly evaluated?
- Are any key risks missing?
- Are the causes of the event identified?
- Have mitigating actions been recorded for each risk?
- Are there any actions in progress to deal with risk?
- Assess the status of such actions
- Are there any management decisions pending?
- Has a target risk been established?
- Assess confidence level in the potential for such actions to reduce the risk required
- Determining an audit risk and control assessment

Exercise 6: Reviewing the overall risk process

The risk based audit challenge

- The need to assess the risk maturity of the function
- Commitment to risk management
- The questions to ask
- Assessing risk appetite
- Determining which risks should be concentrated on in the audit

- **Reviewing risk ownership and identifying gaps**
- **Identifying residual risks above the risk appetite**
- **Assessing the 4 T's**
- **Monitoring of action plans**
- **Evaluation and reporting of actual versus perceived controls**
- **Determining which key risks are not readily auditable**
- **New audit programme – auditing ERM**

Exercise 7: Challenging risk asssessments

Auditing IT Governance

- **Global Technology Audit Guides (GTAG's)**
- **The need to determine the boundaries**
- **Defining the IT audit universe**
- **Focus on high risk areas**
- **Assess IT vulnerabilities**
- **Target areas where you are focusing on process rather than technical aspects**
- **Use of audit frameworks such as CoBIT and ISO 27000**
- **IIA new standard on IT Governance**
- **Risk based audit of general controls (GAIT)**
- **An ISO 27000 audit checklist will be shared**

Exercise 8 – Challenges of IT Governance audit

Auditing Cybersecurity risks

- **Statistics about cybersecurity crime**
- **Profiles of the Attackers**
- **Anatomy of a Breach**
- **How to prevent Cyber Incidents**
- **Network Controls (Internal and External)**
- **Domain and Password Controls**
- **Access rights and User Awareness**
- **Application Security**
- **Secure Software Development environment**
- **Data Controls**
- **Encryption**
- **Vulnerability Management**
- **Security Testing**
- **Social Media risks**

Exercise 9 – Cybersecurity risks

Auditing Brand and reputation

- **The rise of reputation as a key risk**
- **The increasing importance of a positive image – the need to be admired**

- Where does reputation come from?
- How do you measure it?
- The magnifying effect on reputation of business failures
- Global brands
- How to judge reputation
- Identifying Reputational Risks
- A checklist for reviewing reputational risk will be provided to all delegates

Exercise 10 –Auditing reputation management