Boston Chapter
AGA
2018 Regional Professional Development Conference

Brandeis University

Professor Erich Schumann

May 2018

Identifying Strategic Risk
Risks Owned by Strategic Risk Taker

- Strategic Risk = Positive or negative impact of risk on an organization
- Sub-culture Risk = problem that occurs because unit cultures vary in terms of their ability to operate effectively in terms of their ability to operate effectively within a larger structure
- Leadership Risk = Leadership is doing the right thing at the right time to get people to perform in a timely fashion. Exposure arises when the organization has weaknesses in the roles played by those who are expected to lead
- Life Cycle Risk = the reality that products, business units and business lines start up, grow to maturity and, in many case enter a period of stagnation or decline
- Horizon Risk = external exposure that arises when the organization is not actively scanning its external environment for developments and changing trends that could affect business and operations

Typical Risk Universe

- Market Risk = risk of loss due to adverse movements in the mark to market value of the company's asset and liabilities
- Credit Risk = risk of loss through exposure to counterparty default
- Strategic Risk = risk of employing a strategy that fails to secure the optimum returns available from capital employed
- Business Risk = risk of unfavorable fiscal, economic, competitive, legal, tax or regulatory changes in the market
- Operational Risk = risk of loss caused by failures in operational processes or the systems that support them, including those adversely affecting reputation, legal enforcement of contracts and claims

Key Components of Operational Risk

- Core operational capability = risk that people, premises or systems are unavailable
- People = most important resource; continues to be major contributory factor in many dramatic failures
- Transactional systems = includes data capture, processing and protection; also settlement risk
- Change and new activities = change in industry and developing of new activities causes much higher operational risk than stable business
- Expense volatility = traditionally focus is on revenue volatility, however, expense volatility is more relevant, especially related to expenditure in technology and bonuses and variable compensation

Objectives of Operational Risk Management Function

- To avoid catastrophic losses
- To generate a broader understanding of operational risk issues at all levels of the firm
- To enable organizations to anticipate risks more effectively
- To provide measurement of performance
- To enhance the "Culture of Control" within the organization
- To provide objective information so that services offered by the organization take account of operational risks

The 10 Commandments of Good Operational Risk Management

1. Understand your financials = large surpluses you don’t understand are more dangerous than large losses you don’t understand
2. Focus on distance = operational risk increases with distance
3. Honor the Sabbath = people who never take holidays or always stay late are not necessarily good corporate employees
4. Prepare to pay = there is no such a thing as cheap risk management or segregation of duties
5. Invest with authority = The CEO is not the risk control function but a risk control function without the CEO’s backing will not work

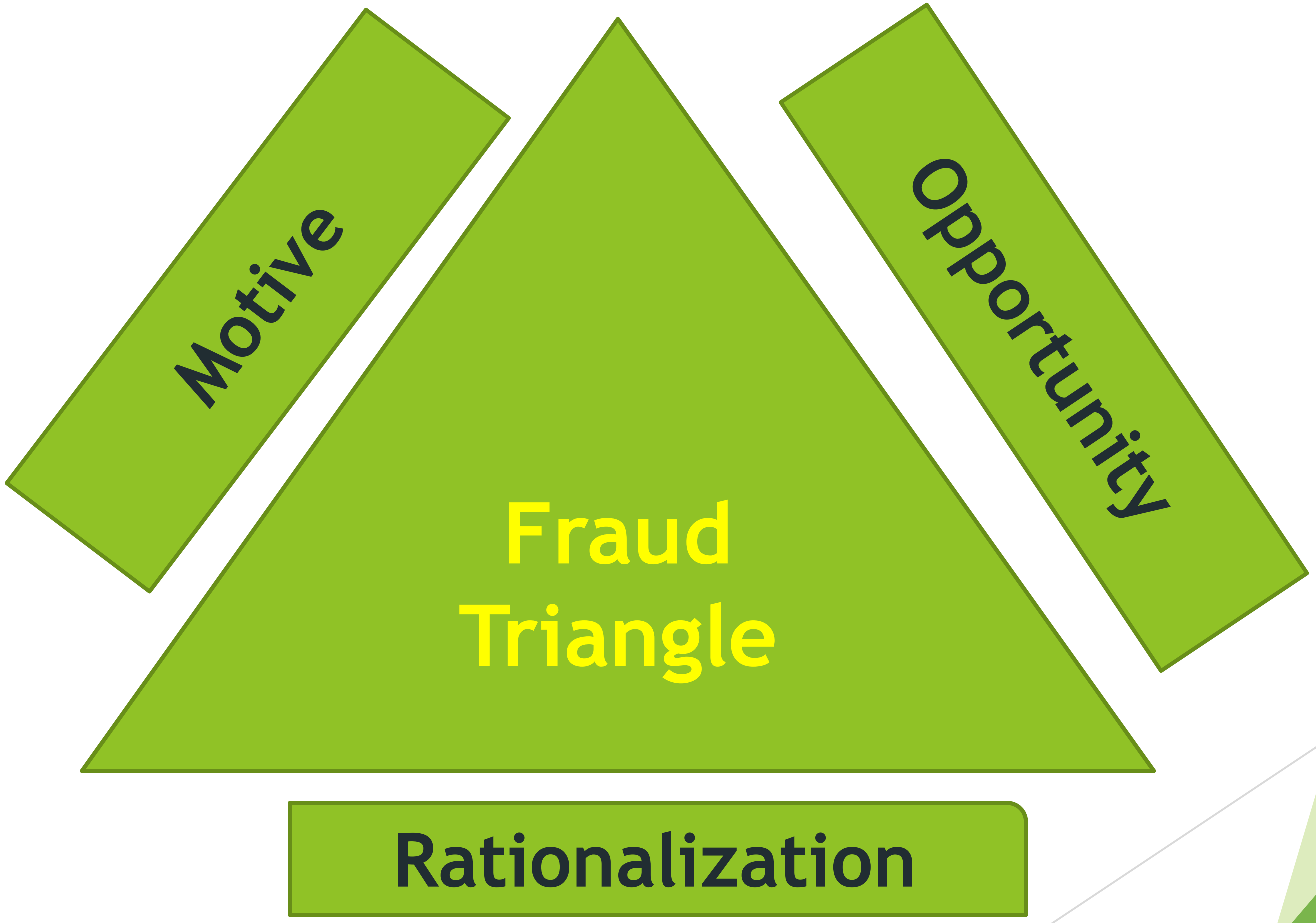
The 10 Commandments of Good Operational Risk Management

6. Reconcile with diligence = reconciliation problems usually indicate losses
7. Track the cash = accounting entries can be manipulated, cash disbursements can't, it's the fundamental control
8. Respect business quality = volume is no substitute for value
9. Ensure the numbers add up = accounting losses reflect business realities
10. Watch your technology = computer systems are an open door into the heart of your business, and their integrity and security is not as complete as it appears

Projection of Operational Risks

Operational Risks Projected						
Internal Fraud	External Fraud	Employment Practices and workplace safety	Clients, products and business practice	Damage to physical assets	Business disruption and system failures	Execution, delivery & process management

Operational Risk - Fraud Risk
Fraud Triangle



Operational Risk
Fraud Risk Assessment Process

- Form a team with the following members:
  - **Accounting/finance** personnel, who are familiar with the financial reporting process and internal controls
  - **Nonfinancial business** unit and operations personnel, to leverage their knowledge of day-to-day operations
  - **Legal and compliance** personnel
  - **Internal audit** personnel

Operational Risk
Fraud Risk Identification

- Discussions of the incentives, pressures, and opportunities to commit fraud
- Risks of management override of controls
- Population of fraud risks relevant to the organization
- Other risks, such as regulatory and legal misconduct risk
- Impact of Information Technology and related fraud risks

consider the potential for management override of controls established to prevent or detect fraud

Fraud Risk Identification

- Assessing the likelihood and significance of each potential fraud risk is a subjective process
- All fraud risks are not equally likely, nor will all frauds have a significant impact
- Assessing the likelihood and significance of identified inherent risks allows the agency to manage its fraud risks and apply preventive and detective procedures rationally. (Risk without consideration of known controls)
- Management must evaluate the potential significance of those residual risks and decide on the nature and extent of the fraud preventive and detective controls and procedures to address such risks

Benefits of Good Operational Risk Management Process

- Improving the reliability of operations
- Improving the effectiveness of the risk management operations
- Strengthening the decision-making process where risks are involved
- Increases in losses caused by poorly-identified risks
- Early identification of unlawful activities
- Lower compliance costs
- Reduction in potential damage from future risks
- Gain competitive advantage

Importance of Risk Assessment

- Risk assessment involves
  - Recognition of risks
  - Rating to determine the significance
- Risks are attached to
  - Corporate objectives
  - Stakeholders expectations
  - Core processes
  - Key dependencies

Importance of Risk Assessment

- Risk assessment is vitally important
  - But only useful if the conclusions of the assessment are used to inform decisions

And / Or

  - To identify the appropriate risk responses for the type of risk under consideration

Risk assessment is the starting point of the risk management process

Risk Assessment Techniques

Technique	Brief Description
Questionnaires and checklists	Use of structured questionnaires and checklists to collect information that will assist with the recognition of the significant risks
Workshops and brainstorming	Collection and sharing of ideas at workshops to discuss the events that could impact the objectives, core processes or key dependencies
Inspections and audits	Physical inspections of premises and activities and audits of compliance with established systems and procedures

Risk Assessment Techniques Advantages/ Disadvantages

Technique	Advantages	Disadvantages
Questionnaires and checklists	• Consistent structure • Greater involvement	• Rigid approach, might result in some risks being missed • Questions will be based on historical knowledge
Workshops and brainstorming	• Consolidated opinion from all interested parties • Greater interaction produces more ideas	• Senior management tends to dominate • Issues will be missed if incorrect people are involved
Inspections and audits	• Physical evidence forms the basis of opinion • Audit approach results in good structure	• Audit approach tends to focus on historical experience

Risk Assessment Techniques
Risk Perception

- Different people have different views of risks
  - By exploring why their view differs it is often possible to reach an agreed common position
  - Different views of the importance of risks can be present at different levels of seniority within the organization
- To understand the risks facing an organization and to be able to undertake an accurate risk assessment, extensive knowledge of the organization is required
- In relation to public perception of risk, members of the public often only have access to incomplete information and are subject to strong arguments from lobbying and other special interest groups

Risk Assessment Techniques
Risk Perception

Issue: concern that media coverage will distort risk and create disproportionate fear

Checklist questionnaire:

1. What exactly is the risk, how big is it and who does it affect?
2. Can the audience judge the significance of any statistics or other research?
3. Is it more appropriate and measured to ask "How safe is this?" rather than "Is this 100% safe?
4. Have you considered the impact of public perceptions of risk if we feature emotional pictures and personal testimony?
5. Is there an everyday comparison that may make the size of the reported risk easier to understand?
6. Would information about comparative risks help the audience to put the risk in context and make properly informed choices?

Mitigate Assessed Risk - Control Activities Simple Rules to Follow

- The cost of control activities should not exceed the cost that would be incurred by the organization if the undesirable event occurred
- Management should build control activities into business processes and systems as the processes and systems are being designed. Adding control activities after the development of a process or system is generally more costly
- The allocation of resources among control activities should be based on the significance and likelihood of the risk they are preventing or reducing

Mitigate Assessed Risks - Control Activities Two Categories of Controls

- Prevention control activities:

  Are designed to deter the occurrence of an undesirable event. The development of these controls involves predicting potential problems before they occur and implementing ways to avoid them

- Detection control activities:

  Are designed to identify undesirable events that do occur, and alert management about what has happened. This enables management to take corrective action promptly

Prevention controls tend to be more expensive than detection controls. No one control activity provides all answers to risk management problems. Combination of control activities should be used

Summary

Risk Assessment Process is simple:

1. Identify what can go wrong
2. Identify who might be effected and how they might be harmed
3. Identify controls that are needed to stop it going wrong
4. Show that any remaining risk after all reasonable controls are in place is low enough to be accepted
5. Record all your findings and keep it
6. Tell everyone what they need to know and do
7. Make sure all gets done
8. Make sure changes are reflected and included in updated risk assessment

Good Risk Management Process is teamwork