Risk Management in a For-profit Organisation

1

Objectives

- Explain the risk management framework
- The underlying process and cycle, and resources and people involved
- The framework can be applied in for profit and non profit organisations as well as for personal use
- It can also be scaled to meet the needs of large or small organisations

2

WHERE ARE THEY NOW?

3

RISK MANAGEMENT BACKGROUND

- Nov 2004 The Stock Exchange of Hong Kong Limited published the "Code on Corporate Governance Practices and Corporate Governance Report".
- These were incorporated into Appendices 14 - Corporate Governance Code and 23 - Corporate Governance Report of the Main Board Listing Rules.
- April 2012 Appendix 23 was merged with Appendix 14.

4

Code provision C.2.1 on "Internal Controls"

- The directors should at least annually conduct a review of the effectiveness of the system of internal control of the issuer and its subsidiaries.
- Report to shareholders that they have done so in their Corporate Governance Report.
- The review should cover all material controls, including financial, operational and compliance controls and risk management functions.

5

Why do non profit organisations need risk management?

6

WHY RISK MANAGEMENT FOR NON PROFIT ORGANISATIONS

- Involves less significant sum, but can be the entire fund of the service organisation
- Affects service targets and social workers themselves
- Affects funding from government or through fund raising
- Forces NGOs to re-consider their vision, missions and risk appetite
- Leads NGOs to assess risks and deploy measures to mitigate risks, ensuring effective use of resources and sustainability

7

RISK MANAGEMENT FRAMEWORK

8

RISK MANAGEMENT FRAMEWORK

- Most organisations follow the principles and guidelines set out in the guide of "Internal Control and Risk Management" issued by HKICPA;
- Adopt the approach outlined in the COSO report;
- Use the ISO31000 standard on risk management.

- HKICPA – Hong Kong Institute of Certified Public Accountants
- COSO - the Committee of Sponsoring Organizations of the Treadway Commission.
- ISO - International Organization for Standardization

9

DEFINITION OF RISK (ISO31000)

- Risk is the 'effect of uncertainty on objectives'.
- In this definition, uncertainties include events (which may or may not happen) and uncertainties caused by ambiguity or a lack of information.
- It also includes both negative and positive impacts on objectives.
- Risk can be an opportunity as well as a threat.

10

Enterprise risk management framework (COSO)

- Enterprise risk management is a process,
- effected by an entity's board of directors, management and other personnel,
- applied in strategy setting and across the enterprise,
- designed to identify potential events that may affect the entity,
- and manage risk to be within its risk appetite,
- to provide reasonable assurance regarding the achievement of entity objectives.

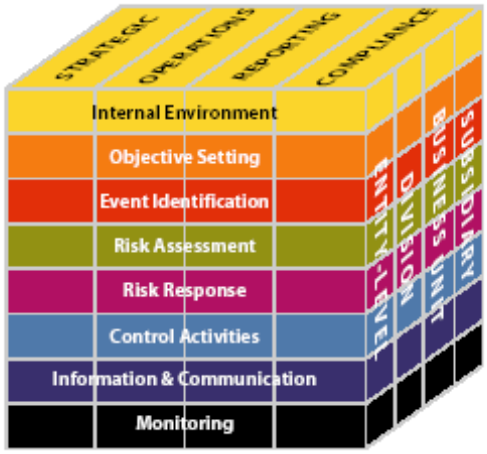
11

Risk appetite

- Risk appetite reflects the enterprise's risk management philosophy, and in turn influences the entity's culture and operating style.
- It is considered in strategy setting.
- The risk appetite statement frames the risks the organization should accept, the risks it should avoid and the strategic, financial and operating parameters within which the organization should operate.

12

Components of Enterprise Risk Management (COSO)



13

Control Environment

- The internal environment encompasses the tone of an organization
- Sets the basis for how risk is viewed and addressed by an entity's people, including risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate.

14

Objective Setting

- Objectives must exist before management can identify potential events affecting their achievement.
- Enterprise risk management ensures that management has in place a process to set objectives and that the chosen objectives support and align with the entity's mission and are consistent with its risk appetite.

15

Objective Setting

- This enterprise risk management framework is geared to achieving an entity's objectives, set forth in four categories:
- Strategic – high-level goals, aligned with and supporting its mission
- Operations – effective and efficient use of its resources
- Reporting – reliability of reporting
- Compliance – compliance with applicable laws and regulations.

16

Event identification

- Internal and external events affecting achievement of an entity's objectives must be identified, distinguishing between risks and opportunities.
- Opportunities are channeled back to management's strategy or objective-setting processes.

17

Risk Assessment

- Risks are analyzed, considering likelihood and impact, as a basis for determining how they should be managed. Risks are assessed on an inherent and a residual basis.

18

Risk Response

- Management selects risk responses – avoiding, accepting, reducing, or sharing risk – developing a set of actions to align risks with the entity's risk tolerances and risk appetite.

19

Control Activities

- Policies and procedures are established and implemented to help ensure the risk responses are effectively carried out.

20

INFORMATION AND COMMUNICATION

- Relevant information is identified, captured, and communicated in a form and timeframe that enable people to carry out their responsibilities.
- Effective communication also occurs in a broader sense, flowing down, across, and up the entity.

21

MONITORING

- The entirety of enterprise risk management is monitored and modifications made as necessary. Monitoring is accomplished through ongoing management activities, separate evaluations, or both.

22

IMPLEMENTATION OF RISK MANAGEMENT

23

POSSIBLE RISKS FACED BY A COMPANY
BUSINESS RISKS

- Wrong business strategy
- Competitive pressure on price / market share
- General / regional economic problems
- Industry sector in decline
- Political risks
- Adverse government policy
- Inattention to information technology (IT) aspects of strategy and implementation
- Obsolescence of technology
- Substitute products
- Takeover target
- Inability to obtain further capital
- Bad acquisition
- Too slow to innovate and reengineering
- Too slow to respond to demands from market and customers

24

FINANCIAL RISKS

- Market risk
- Credit risk
- Interest risk
- Currency risk
- Liquidity risk
- Overtrading
- High cost of capital
- Misuse of financial resources
- Going concern problems
- Occurrence of types of fraud to which the business is susceptible
- Misstatement risk related to published financial information
- Breakdown of accounting system
- Unreliable accounting records
- Unrecorded liabilities
- Penetration and attack of IT systems by hackers
- Decisions based on incomplete or faulty information
- Too much data and not enough analysis
- Unfulfilled promises/pledges to investors

25

COMPLIANCE RISKS

- Breach of Listing Rules
- Breach of financial regulations
- Breach of Companies Ordinance requirements
- Breach of competition regulations
- Breach of other regulations and laws
- Litigation risk
- Tax problems
- Health and safety risks
- Environmental problems

26

Operation and other risks

- Inefficient / ineffective management process
- Business processes not aligned to customer / market demand and strategic goals
- Loss of entrepreneurial spirit
- Missed or ignored business opportunities
- Other business probity issues
- Other issues giving rise to reputational problems
- Poor brand management
- Failure of major change initiative
- Inability to implement change

27

Operation and other risks

- Stock-out of raw materials
- Skills shortage
- Physical disasters (e.g., fire and explosion)
- Computer viruses or other system malfunctions
- Failure to create and exploit intangible assets
- Loss of intangible assets
- Loss of physical assets
- Loss of key people
- Loss of key contracts

28

Operation and other risks

- Lack of orders
- Lack of business continuity
- Succession problems
- Inability to reduce cost base
- Over-reliance on key suppliers or customers
- Onerous contract obligations imposed by major customers
- Failure of new products or services
- Failure to satisfy customers
- Poor service levels
- Quality problems

29

Operation and other risks

- Failure of major projects
- Failure of big technology related projects
- Failure of outsource providers to deliver
- Lack of employee motivation or efficiency
- Industrial action
- Problems arising from exploiting employees in developing countries
- Inefficient / ineffective processing of documents
- Breach of confidentiality

- Adapted from Implementing Turnbull – A Boardroom Briefing, ICAEW

30

How to do it

- Risk impact/ consequence table
- Likelihood table
- Risk rating table
- Risk register

31

When to do it

- When to develop/update the risk register?
  - Ongoing assessment of emerging or significant risks
  - Should there be new business processes or new projects, do at planning stage
  - Half-yearly and yearly for submission to the Management and Board

32

When to do it

- What if there is no change to the business process since last submission ?
  - External environment may change;
  - Control activities may not be working effectively
  - Other factors like staff turnover or job rotation
  - So, yes, you still need to perform the risk assessment but effort involved may be less than the first assessment
- Expect to do a thorough re-assessment from zero base every 3 years

33

Resources involved

- There are risk management software in the market
- Use Word or spreadsheet

34

People involved

- Risk facilitator
- Board
- Top Management
- Middle Management
- Risk champions

35

Use of framework for small organizations

- Can scale down impact, likelihood and risk rating to 3 levels
- Can perform risk assessments on an annual basis
- May involve only the shop in-charge

36

Questions?

37

CONTACT

- samsytong@gmail.com

38

Thank you

39