Presented by : Patrick Rozario
Managing Director ,Moore Stephens Advisory Services Limited
Venue: Room 201, 2/F Duke of Windsor Social Service Building, Wanchai
Date: 26 January 2018

CPA for NGO social responsibility programme

Internal Control and Risk Oversight
內部監控與風險管理

Hong Kong Institute of Certified Public Accountants
香港會計師公會

Introduction

What are the challenges we face?

- Leading a cohesive organization
- Establishing the right culture
- Finding first signs of problems / risks
- Motivating employees & yourself
- Reviewing performance
- A safe and rewarding place to work

CPA
Hong Kong Institute of
Certified Public Accountants
香港會計師公會

Introduction

What are the challenges we face?

- How to comply with regulations
- How to find the value from compliance
- How to meet the board demands
- Ability to create efficiencies and able to deliver your objectives / improve your bottom line ($$$)
- Setting strategy and aligning it to business processes
- Multiple jurisdictions and culture differences

Hong Kong Institute of
Certified Public Accountants
香港會計師公會

Introduction

Public Sector

- Public services directly delivered by the state / government through civil services / department
- Many public sector activities are now delivered by private, quasi-privatised organisations or voluntary sectors and social enterprises
- Greater efficiency and economy in delivering public resources
- Poor governance: lack of transparency and disclosure
- These entities (NGOs) are not subject to the discipline of shareholder investment and the capital markets
- Some receive government subvention and or private / public funding (fund raising)

Hong Kong Institute of
Certified Public Accountants
香港會計師公會

Introduction

- Complex social, economic and political objectives
- Accountability to various stakeholders: interest but no ownership rights
- Reputation and stakeholders confidence
- Good governance poses particular challenges
- Not one size fits all approach
- Large statutory bodies to sporting clubs
- Art & culture, education, religion, political parties, health, …
- Fragmentation

Hong Kong Institute of
Certified Public Accountants
香港會計師公會

Introduction

Third Sector

- Third Sector in HK to work with the Government and the private sector
- Common good, long term sustainability and effectiveness
- Wide ranging studies
- Review current legal and regulatory framework for NGO
- Respective registration and incorporation are inadequate for the proper functioning of NGO
- Lack of development

Hong Kong Institute of
Certified Public Accountants
香港會計師公會

Enterprise Risk Management Framework

Introduction

- The updated Committee of Sponsoring Organisations of the U.S. Treadway Commission ("COSO")'s ERM Framework: Enterprise Risk Management – Integrating with Strategy and Performance released in September 2017.

- An organisation ERM framework fosters continuous monitoring of the risk environment, and an integrated evaluation of risks and their interactions. It is built around developing an appropriate and mindful risk culture at every level of the organisation in support of the orgnisation's strategic objectives.

- The ERM framework provides business units with appropriate tools, processes and capabilities for the identification, assessment and, where required, upward referral of identified material risks for further evaluation. It also ensures a consistent approach to monitoring, managing and mitigating the risks that the organisation accepts and sustain in its activities.

Hong Kong Institute of
Certified Public Accountants
香港會計師公會

Enterprise Risk Management Framework

Introduction

- The Group's ERM consists of the following key components and principles:

Hong Kong Institute of Certified Public Accountants 香港會計師公會

Enterprise Risk Management Framework

Governance & Culture

Principle 1 – Exercise board oversight

- The board of directors provides oversight of the strategy and carries out governance responsibilities to support management in achieving strategy and business objectives.

Accountability and responsibility

- The board of directors has the primary responsibility for risk oversight in the entity, it has a fiduciary responsibility to the entity's stakeholders, including conducting reviews of enterprise risk management practices. The full board is responsible for risk oversight, leaving the day-to-day responsibilities of managing risk to management.

CPA Hong Kong Institute of Certified Public Accountants 香港會計師公會

Enterprise Risk Management Framework

Governance & Culture

Skills, experience, and business knowledge

- The board of directors is well positioned to offer expertise and provide oversight of enterprise risk management through its collective skills, experience, and business knowledge.

Independence

- The board overall should be independent. Independence enhances directors' ability to be objective and to evaluate the performance and well-being of the entity without any conflict of interest or undue influence of interested parties.

Hong Kong Institute of
Certified Public Accountants
香港會計師公會

Enterprise Risk Management Framework

Governance & Culture

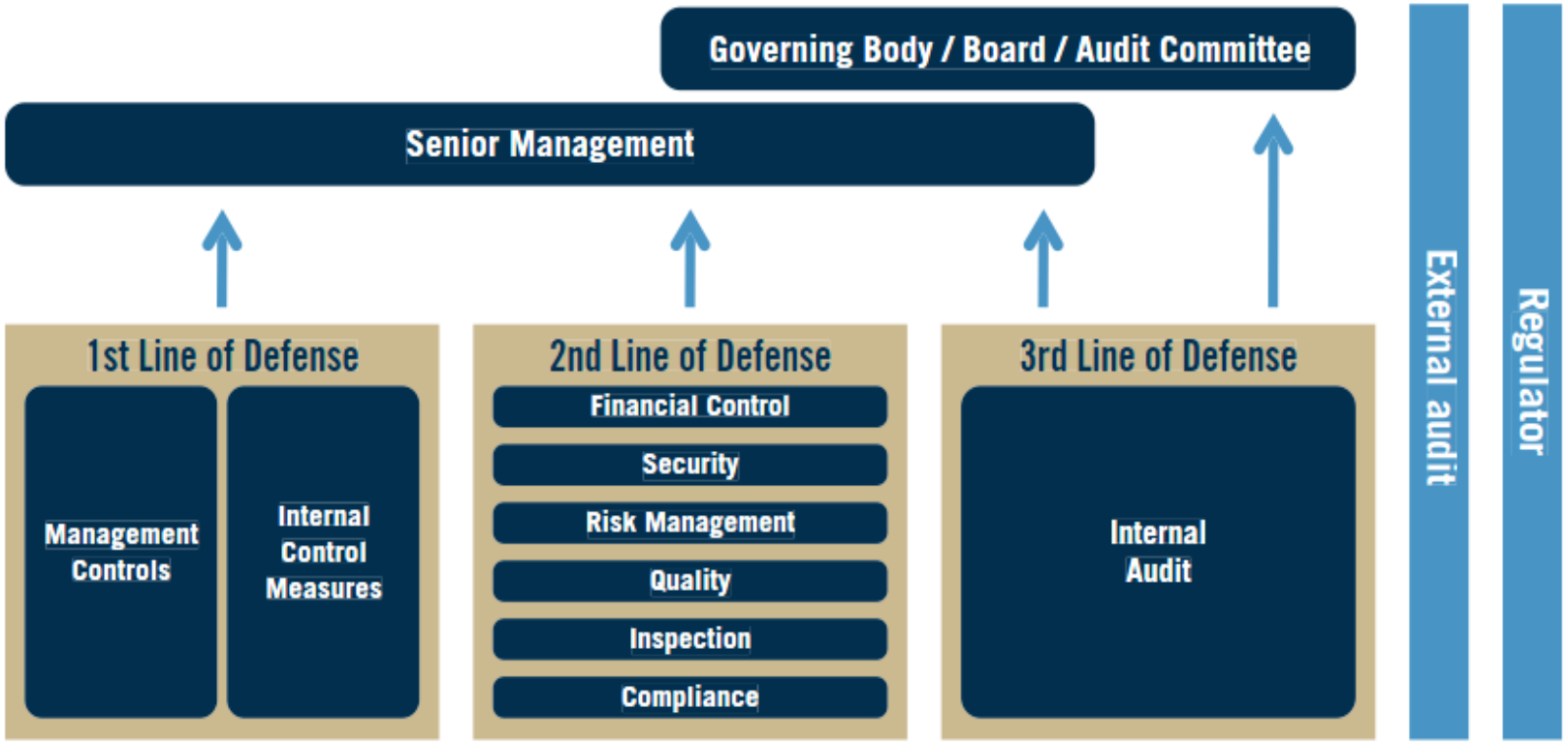
Principle 2 – Established operating structures

- An operating structure describes how the entity organises and carries out its day-to-day operations. Through the operating structure, personnel are responsible for developing and implementing practices to manage risk and stay aligned with the core values of the entity. In this way, an operating structure contributes to managing risk to the strategy and business objectives.

Operating structure and reporting lines

- The organisation establishes an operating structure and designs reporting lines to carry out the strategy and business objectives. It is important for the organisation to clearly define responsibilities when designing reporting lines. The organisation may also enter into relationships with external third parties that can influence reporting lines (e.g., strategic business alliances, outsourcing, or joint business ventures).

Three lines of defence



Adapted from ECIIA/FERMA *Guidance on the 8th EU Company Law Directive, article 41*

CPA Hong Kong Institute of Certified Public Accountants 香港會計師公會

Enterprise Risk Management Framework

Governance & Culture

Authority and responsibilities

- In an entity that has a single board of directors, the board delegates to management the authority to design and implement practices that support achievement of strategy and business objectives. In turn, management defines roles and responsibilities for the overall entity and its operating units. Management also defines roles, responsibilities, and accountabilities of individuals, teams, divisions, and functions aligned to strategy and business objectives.

Hong Kong Institute of Certified Public Accountants 香港會計師公會

Enterprise Risk Management Framework

Governance & Culture

Principle 3 – Defines desired culture

- The organisation defines the desired behaviours that characterize the entity's desired culture.

Culture and desired behaviours

- An organisation's culture reflects its core values, behaviors, and decisions. Decisions are in turn a function of the available information, judgment, capabilities, and experience. An entity's culture influences how the organisation applies this Framework: how it identifies risk, what types of risk it accepts, and how it manages risk.

CPA Hong Kong Institute of Certified Public Accountants 香港會計師公會

Enterprise Risk Management Framework

Governance & Culture

Principle 4: Demonstrates commitment to core values

- The organisation demonstrates a commitment to the entity's core values.

Reflecting core values throughout the organisation

- Understanding the entity's core values is fundamental to enterprise risk management. Core values are reflected in actions and decisions applied across the entity. Without a strong and supportive understanding of, and commitment to, those values communicated from the top of the organisation, risk awareness can be undermined and risk-inspired decisions may be inconsistent with those values. The manner in which values are communicated across the organisation is often referred to as the "tone" of the organisation.

CPA Hong Kong Institute of Certified Public Accountants 香港會計師公會

Enterprise Risk Management Framework

Governance & Culture

Corporate culture / Core values

- **Business philosophy:** professionalism, proactive
- **Management principle:** rigorousness,
- **Innovation**
- **Risk management**
- **Talent concept**
- **Team spirit**

Hong Kong Institute of Certified Public Accountants 香港會計師公會

Enterprise Risk Management Framework

Governance & Culture

Principle 5: Attracts, develops, and retains capable individuals

- The organisation is committed to building human capital in alignment with the strategy and business objectives.

Establishing and evaluating competence

- Management, with board oversight, defines the human capital needed to carry out strategy and business objectives. Understanding the needed competencies helps in establishing how various business processes should be carried out and what skills should be applied. That is, the board of directors evaluates the competence of the chief executive officer and, in turn, management evaluates competence across the entity and addresses any shortcomings or excesses as necessary. The human resources function helps promote competence by assisting management in developing job descriptions and roles and responsibilities, facilitating training, and evaluating individual performance for managing risk.

CPA Hong Kong Institute of Certified Public Accountants 香港會計師公會

Enterprise Risk Management Framework

Governance & Culture

Attracting, developing, and retaining individuals

- The ongoing commitment to competence is supported by and embedded in the human resource management processes to attract, develop and retain talented individuals. In addition, organisations must continually identify and evaluate those roles that are essential to achieving strategy and business objectives.

Preparing for succession

- To prepare for succession, the board of directors and management must develop contingency plans for assigning responsibilities important to enterprise risk management. In particular, succession plans for key executives need to be defined, and succession candidates should be trained, coached, and mentored for assuming the role. Typically, larger entities identify more than one person who could fill a critical role.

Enterprise Risk Management Framework

Strategy and objective-setting

Principle 6: Analyses business context

- The organisation considers potential effects of business context on risk profile.

Understanding business context

- An organisation considers business context when developing strategy to support its mission, vision, and core values. “Business context” refers to the trends, relationships, and other factors that influence an organisation’s current and future strategy and business objectives.

Hong Kong Institute of Certified Public Accountants 香港會計師公會

Enterprise Risk Management Framework

Strategy and objective-setting

Principle 7: Defines risk appetite

- The organisation defines risk appetite in the context of creating, preserving, and realizing value.

Applying risk appetite

- Decisions made in selecting strategy and developing risk appetite are not linear, with one decision always preceding the other. Nor is there a universal risk appetite that applies to all entities. The best approach for an entity is one that aligns with the analysis used to assess risk in general, whether that is qualitative or quantitative. Developing the risk appetite statements is an exercise in seeking the optimal balance between risk and opportunity.

CPA Hong Kong Institute of Certified Public Accountants 香港會計師公會

Enterprise Risk Management Framework

Strategy and objective-setting

- The Group's Risk Appetite Statement (RAS) is the foundation of its ERM framework. Key objectives of RAS include:
- By considering the risk and return trade-off, RAS plays a critical role in guiding senior management on how to govern business risks to be able to achieve key objectives of the Board and shareholders.
- RAS helps the Group to withstand contingencies such as a market turmoil influencing the performance of the Group, operational losses, or a liquidity crisis.
- RAS plays as a cornerstone to help senior management do commitments with the Board in building a robust risk management framework with a risk practice in vogue.
- RAS helps to define risk profiles, risk limits and risk thresholds for each kind of risks.

Enterprise Risk Management Framework

Strategy and objective-setting

Principle 8: Evaluates alternative strategies

- The organisation evaluates alternative strategies and potential impact on risk profile.

Select business strategy

- An organisation must evaluate alternative strategies as part of strategy-setting and assess the risk and opportunities of each option. Alternative strategies are assessed in the context of the organisation's resources and capabilities to create, preserve, and realize value. A part of enterprise risk management includes evaluating strategies from two different perspectives: (1) the possibility that the strategy does not align with the mission, vision, and core values of the entity, and (2) the implications from the chosen strategy.

CPA Hong Kong Institute of Certified Public Accountants 香港會計師公會

Enterprise Risk Management Framework

Strategy and objective-setting

Principle 9: Formulates business objectives

- The organisation considers risk while establishing the business objectives at various levels that align and support strategy.

Establishing business objectives

- The organisation develops business objectives that are specific, measurable or observable, attainable, and relevant. Business objectives provide the link to practices within the entity to support the achievement of the strategy.

Hong Kong Institute of Certified Public Accountants 香港會計師公會

Enterprise Risk Management Framework

Performance

Principle 10: Identifies risk

- The organisation identifies risk that impacts the performance of strategy and business objectives.

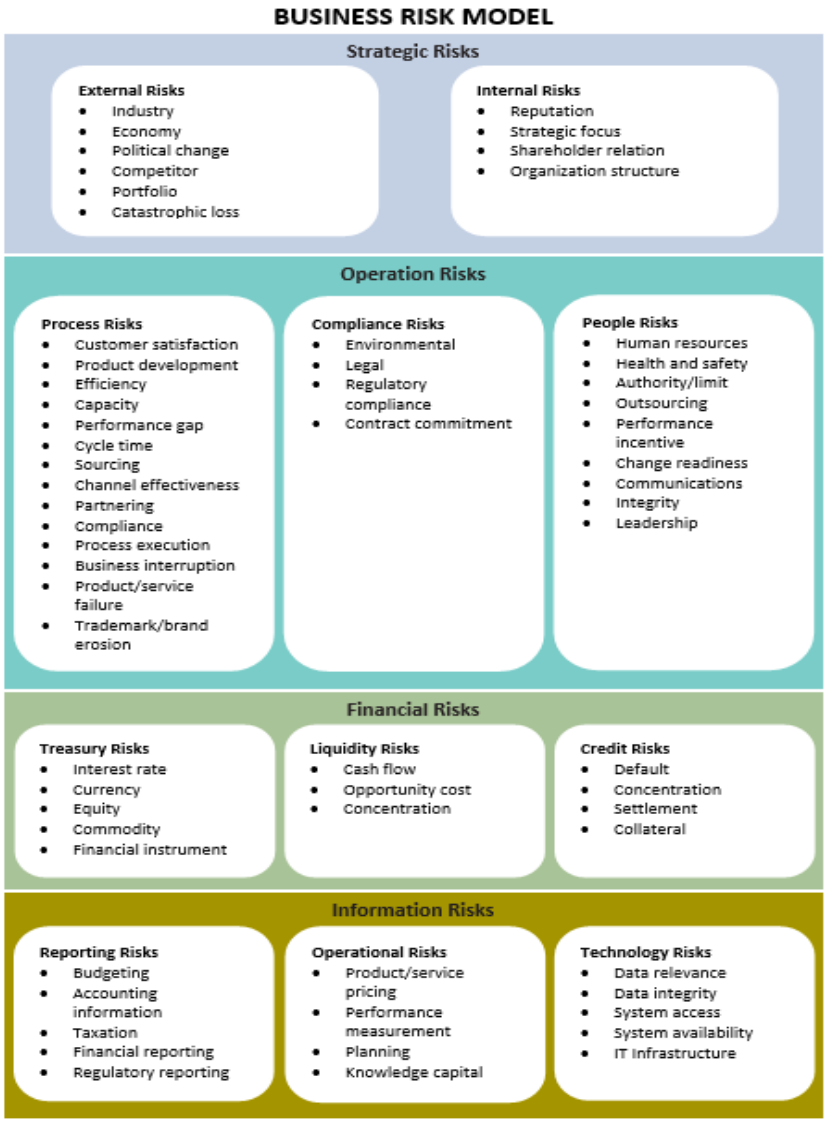
Identifying risk

- The organisation identifies new, emerging, and changing risks to the achievement of the entity's strategy and business objectives. It undertakes risk identification activities to first establish an inventory of risks, and then to confirm existing risks as being still applicable and relevant. As enterprise risk management practices are progressively integrated, the knowledge and awareness of risks is kept up-to-date through normal day-to-day operations.

CPA Hong Kong Institute of Certified Public Accountants 香港會計師公會

Enterprise Risk Management Framework

Performance



Hong Kong Institute of
Certified Public Accountants
香港會計師公會

Enterprise Risk Management Framework

Performance

Principle 11: Assesses severity of risk

- The organisation assesses the severity of risk.

Assessing risk

- Risks identified and included in an entity's risk inventory are assessed in order to understand the severity of each to the achievement of an entity's strategy and business objectives. Risk assessments inform the selection of risk responses. Given the severity of risks identified, management decides on the resources and capabilities to deploy in order for the risk to remain within the entity's risk appetite.

- Quantitative assessment
- Qualitative assessment

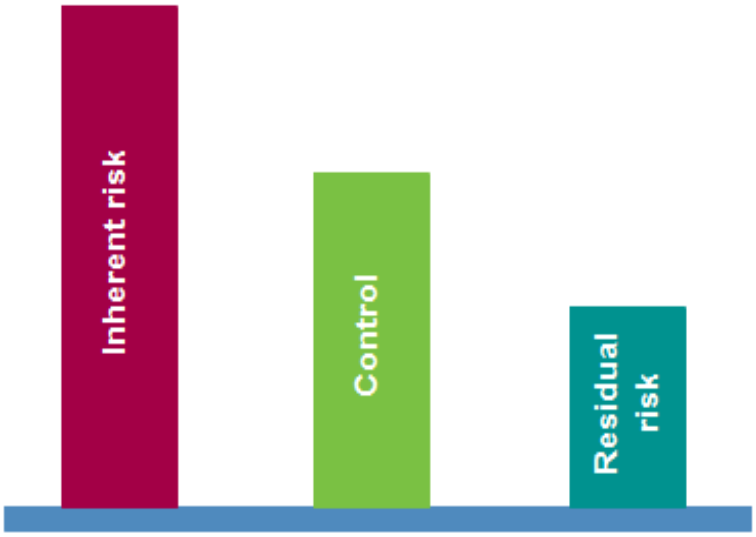
Hong Kong Institute of Certified Public Accountants 香港會計師公會

Enterprise Risk Management Framework

Performance

Inherent risk and residual

- Inherent risk can be defined as exposure when there is no control or control fails, while residual risk refers to exposure after action has been taken to control a risk, making the assumption that the action of control is effective. The residual risk therefore corresponds to the actual exposure of the Company



Hong Kong Institute of Certified Public Accountants 香港會計師公會

Enterprise Risk Management Framework

Performance

Principle 12: Prioritizes risks

- The organisation prioritizes risks as a basis for selecting responses to risks.

Prioritizing risk

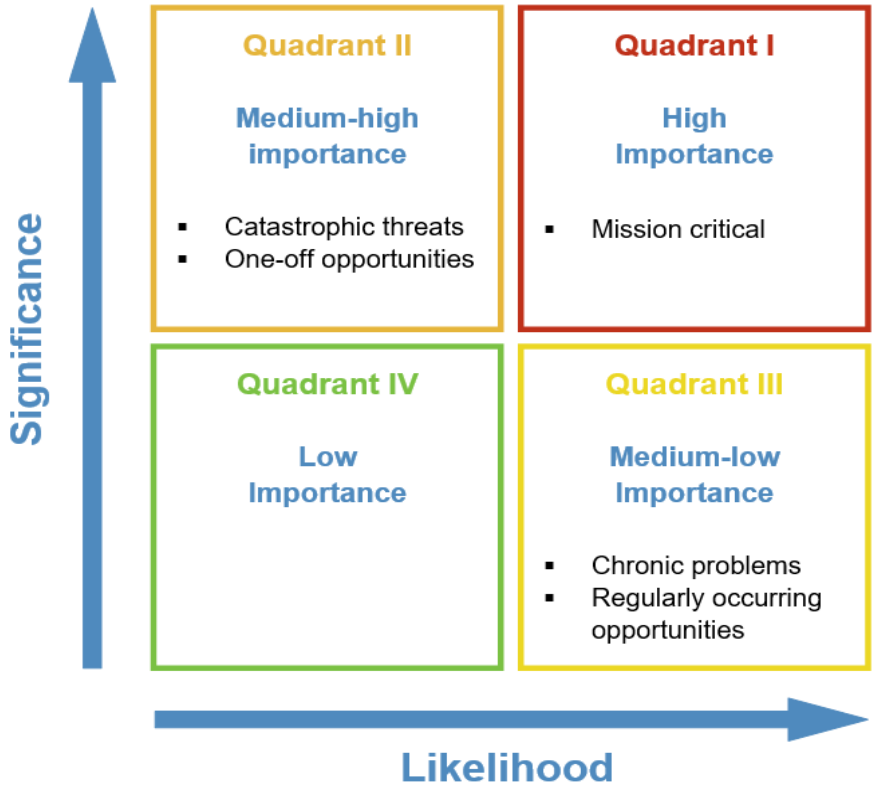
- Organisations prioritize risks in order to inform decision-making on risk responses and optimize the allocation of resources. Given the resources available to an entity, management must evaluate the trade-offs between allocating resources to mitigate one risk compared to another. The prioritization of risks, given their severity, the importance of the corresponding business objective, and the entity's risk appetite helps management in its decision-making.

Hong Kong Institute of
Certified Public Accountants
香港會計師公會

Enterprise Risk Management Framework

Performance

Risk Matrix



Hong Kong Institute of Certified Public Accountants 香港會計師公會

Enterprise Risk Management Framework

Performance

Principle 13: Implements risk responses

- The organisation identifies and selects risk responses.
-

Choosing risk responses

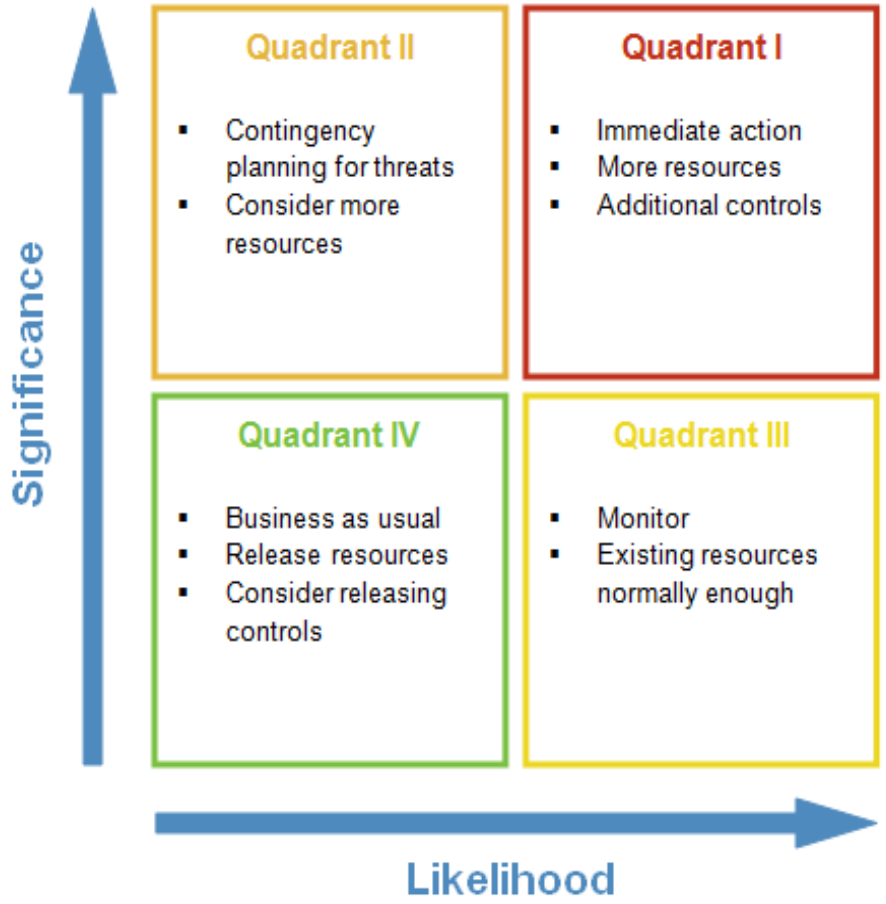
- For all risks identified, management selects and deploys a risk response. Management considers the severity and prioritization of the risk as well as the business context and associated business objectives. Finally, the risk response also accounts for the performance targets of the organisation. Risk responses fall within the following categories:

CPA Hong Kong Institute of Certified Public Accountants 香港會計師公會

Enterprise Risk Management Framework

Performance

Risk Responses



CPA Hong Kong Institute of Certified Public Accountants 香港會計師公會

Enterprise Risk Management Framework

Performance: Risk Responses

- *Accept:* No action is taken to change the severity of the risk. This response is appropriate when the risk to strategy and business objectives is already within risk appetite. Risk that is outside the entity's risk appetite and that management seeks to accept will generally require approval from the board or other oversight bodies.
- *Avoid:* Action is taken to remove the risk, which may mean ceasing a product line, declining to expand to a new geographical market, or selling a division. Choosing avoidance suggests that the organisation was not able to identify a response that would reduce the risk to an acceptable level of severity.
- *Pursue:* Action is taken that accepts increased risk to achieve improved performance. This may involve adopting more aggressive growth strategies, expanding operations, or developing new products and services. When choosing to pursue risk, management understands the nature and extent of any changes required to achieve desired performance while not exceeding the boundaries of acceptable tolerance.

Enterprise Risk Management Framework

Performance: Risk Responses

- *Reduce:* Action is taken to reduce the severity of the risk. This involves any of myriad everyday business decisions that reduce risk to an amount of severity aligned with the target residual risk profile and risk appetite.

- *Share:* Action is taken to reduce the severity of the risk by transferring or otherwise sharing a portion of the risk. Common techniques include outsourcing to specialist service providers, purchasing insurance products, and engaging in hedging transactions. As with the reduce response, sharing risk lowers residual risk in alignment with risk appetite.

Enterprise Risk Management Framework

Performance

Principle 14: Develops portfolio view

- The organisation develops and evaluates a portfolio view of risk.

Developing a portfolio view

- Enterprise risk management allows the organisation to consider potential implications to the risk profile from an entity-wide, or portfolio, perspective. Management first considers risk as it relates to each division, operating unit, or function. Each manager develops a composite assessment of risks that reflects the unit's residual risk profile relative to its business objectives and tolerance.

Enterprise Risk Management Framework

Review and revision

Principle 15: Assesses substantial change

- The organisation identifies and assesses changes that may substantially affect strategy and business objectives.

Integrating reviews into business practices

- Organisations typically anticipate many changes within setting of strategy and business objectives and performance, but they need to also be aware of the potential for larger, substantial changes that may occur and have a more pronounced effect. Substantial change may lead to new or changed risks, and affect key assumptions underpinning strategy. Practices for identifying such changes should be built into business activities and performed continually. Many management practices can identify substantial changes in the ordinary course of running the business.

Hong Kong Institute of Certified Public Accountants 香港會計師公會

Enterprise Risk Management Framework

Review and revision

Principle 16: Reviews risk and performance

- The organisation reviews entity performance and considers risk.

Integrating reviews into business practices

- Much of the focus on enterprise risk management is on managing risk—either reducing the type and amount of risk to acceptable levels or appropriately pursing new opportunities as they emerge. Over time, an entity may not conduct its practices as efficiently as intended, thereby causing risk to manifest and affect performance. From time to time, the organisation may wish to consider its enterprise risk management capabilities and practices.

Enterprise Risk Management Framework

Review and revision

Principle 17: Pursues improvement in Enterprise Risk Management

- The organisation reviews entity performance and considers risk.

Pursuing improvement

- Management pursues continual improvement throughout the entity (functions, operating units, divisions) to improve the efficiency and usefulness of enterprise risk management at all levels.

Hong Kong Institute of
Certified Public Accountants
香港會計師公會

Enterprise Risk Management Framework

Information, communication, and reporting

Principle 18: Leverages information and technology

- The organisation leverages the entity's information and technology systems to support enterprise risk management.

Putting relevant information to use

- Organisations leverage relevant information when they apply enterprise risk management practices. "Relevant information" is simply information that helps organisations be more agile in their decision-making, giving them a competitive advantage. Organisations use information to anticipate situations that may get in the way of achieving strategy and business objectives. Risk information is more than a repository of historical risk data. It needs to support an understanding and development of a complete current and evolving risk profile.

Enterprise Risk Management Framework

Information, communication, and reporting

Principle 19: Communicates risk information

- The organisation uses communication channels to support enterprise risk management.

Communicating with stakeholders

- Various channels are available to the organisation for communicating risk data and information to internal and external stakeholders. These channels enable organisations to provide relevant information for use in decision-making.

Communicating with the board

- Effective communication between the board of directors and management is critical for organisations to achieve the strategy and business objectives and to seize opportunities within the business environment.

Enterprise Risk Management Framework

Information, communication, and reporting

Principle 20: Reports on risk, culture, and performance

- The organisation reports on risk, culture, and performance at multiple levels and across the entity.

Identifying report users and their roles

- Reporting supports personnel at all levels to understand the relationships between risk, culture, and performance and to improve decision-making in strategy- and objective-setting, governance, and day-to-day operations. Reporting requirements depend on the needs of the report user. Report users may include:

Hong Kong Institute of Certified Public Accountants 香港會計師公會

Enterprise Risk Management Framework

Information, communication, and reporting

- Management and the board of directors with responsibility for governance and oversight of the entity.
- Risk owners accountable for the effective management of identified risks.
- Assurance providers who seek insight into performance of the entity and effectiveness of risk responses.
- External stakeholders (regulators, rating agencies, community groups, and others).
- Other parties that require reporting of risk in order to fulfill their roles and responsibilities

Hong Kong Institute of
Certified Public Accountants
香港會計師公會

Enterprise Risk Management Framework

Key Risks / Controls

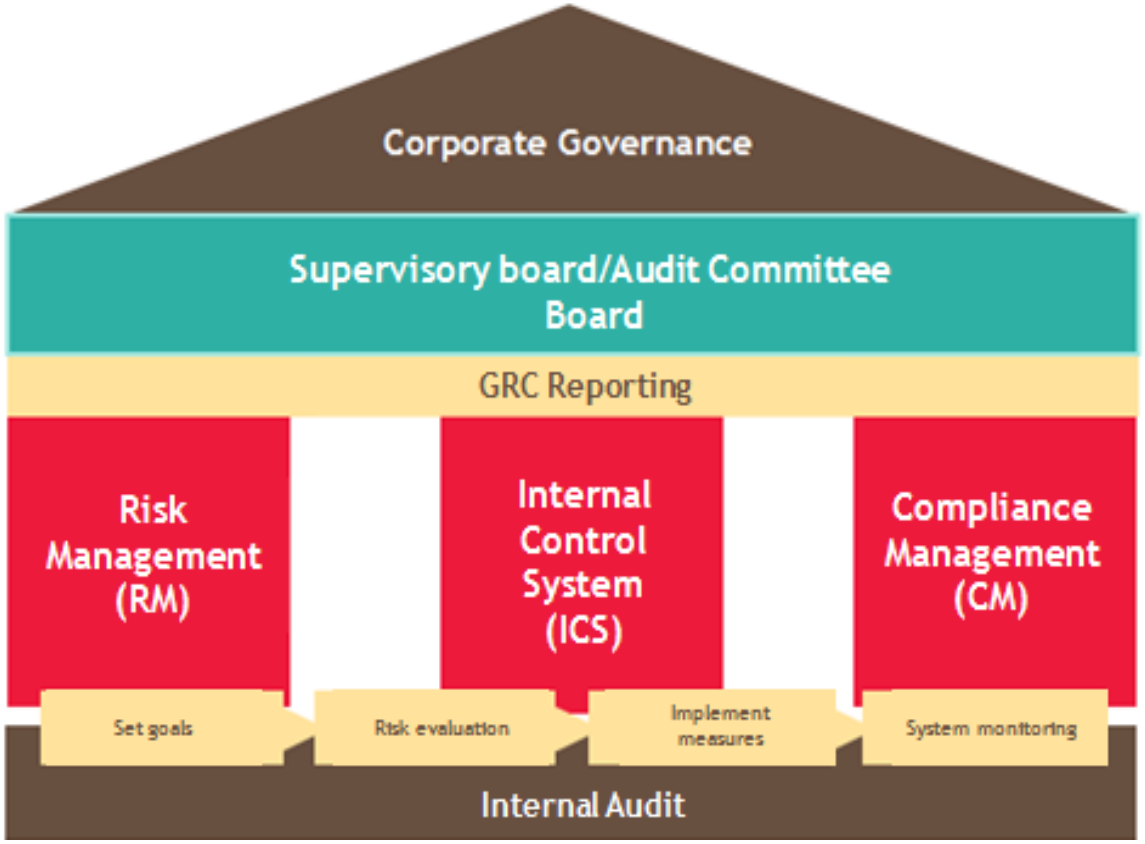
- Lack of diversity / skills of board: Set up nomination committee to identify and recruit suitable directors

- Lack of controls of cash donation :
  - Arrange opening of the collection bags or boxes in a locked room with restricted access as soon as practicable after the fundraising activity.
  - Count the cash collected immediately after the opening of collection bags or boxes.
  - Appoint independent persons or volunteers to witness the opening of collection bags or boxes and counting of cash donations (e.g. using services of a bank or a security company).
  - Record the amount of cash counted, and require the witnessing persons and the counting staff/volunteers to sign on the record, certifying correctness.

- Cyber Security: Conduct IT securities vulnerabilities and threats analysis – firewall, intrusion detection systems .

Hong Kong Institute of Certified Public Accountants 香港會計師公會

Integrated Governance, Risk and Controls / Compliance (GRC)



Hong Kong Institute of
Certified Public Accountants
香港會計師公會

Integrated GRC

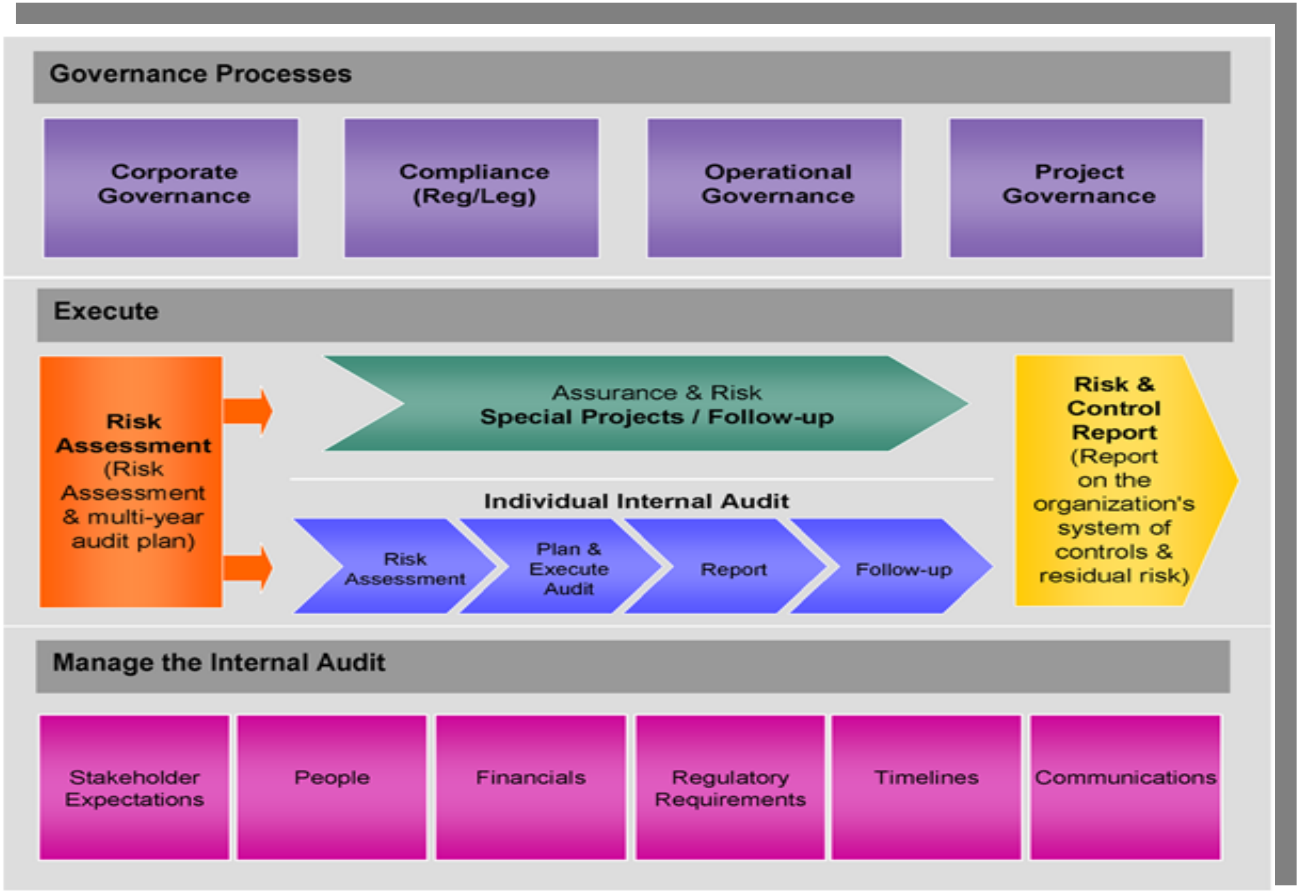
Internal Controls

- Perform risk assessment: Obtain an overview understanding of business structure, processes and assess the corporate governance, and other inherent risks;
- Identify key risks and implement controls of relevant processes in respect of financial, operational, compliance and risk management
- Key controls should be designed so as to be able to prevent and detect error or fraud.
- Key controls should be designed to ensure operating efficiencies and safety .

Hong Kong Institute of Certified Public Accountants 香港會計師公會

Integrated GRC

Internal Audit



Hong Kong Institute of Certified Public Accountants 香港會計師公會

Integrated GRC

Internal Audit

Phase I – Planning and Risk Assessment

- Understand the key business areas and risk, the key processes and systems through enquiry and analyzing its business information and financial data.

Phase II – Control Design Analysis

- Identify the key controls in place by conducting a walkthrough of the key processes identified in Phase I above to confirm existence.

- Determine whether there are any significant gaps within the design of the controls. Key controls should be designed so as to be able to prevent and detect error or fraud; and or ensuring efficiencies and safety (design effectiveness)

Hong Kong Institute of Certified Public Accountants 香港會計師公會

Integrated GRC

Internal Audit

Phase III – Design and Execute Testing

- Based on the work in Phase II, we further perform the following to test the operating effectiveness of the key controls:

  a. Design the testing procedures.
  b. Execute the testing procedures.
  c. For each of the key controls identified, sample sizes are risk-based as well as determined based on frequency of control performance.

Phase IV – Reporting

- Report findings and make recommendations on any measures which the Company should take in order to rectify any design weaknesses and/or to enhance operating effectiveness which have been identified as a result of the work detailed above.

Activity of the workshop

Risk, Controls and enhancements

- Organise into 4 groups
- Identify 5 key risks and the respective controls of your organisations
- Suggestions for enhancing the controls
- Duration: 15 minutes discussion
- Share the findings and recommendation (15 minutes)

Hong Kong Institute of
Certified Public Accountants
香港會計師公會

Q& A