Governance, Risk Management, and Internal Control

Vincent Tophoff, International Federation of Accountants (IFAC)

ICMA Pakistan

Webinar, May 5, 2015
International Federation of Accountants

• Global organization of the accountancy profession
• Supports professional accountants in following areas:
  – Governance and ethics
  – Risk management and internal control (RM/IC)
  – Sustainability and corporate responsibility
  – Financial and performance management
  – Business reporting
  – Promoting and contributing to the value of professional accountants
• All areas of critical importance to professional accountants
Today’s Agenda

• IFAC Governance Guidance
• IFAC/CIPFA Public Sector Framework
• Risk Management & Internal Control
• COSO / ISO 31000 Standards
• Risk Management & Internal Control Maturity
• Professional Accountant “Call to Action”
• Q&A
IFAC Governance Guidance
Relation of Governance, RM & IC

- Governance
- Risk Management
- Internal Control

Diagram showing the relationship between Governance, Risk Management, and Internal Control.
Global Crisis

• Global Crisis, according to IFAC research, caused by:
  ➢ Ethical flaws
  ➢ Governance in name, but not in spirit
  ➢ Regulatory overload, leading to legalistic compliance
  ➢ Risk management & internal control too narrowly focused on only financial reporting controls

• Conclusions from the crisis:
  ➢ Application of governance principles is often the problem
  ➢ Organizations should also take a broader approach to governance
Broader Approach to Governance

• Governance is not just about protecting shareholders’ interests
  …or a compliance exercise to satisfy the requirements of regulators

• Instead, good governance supports building sustainable value in organizations and society
Successful organizations have a governance structure and culture that go beyond conformance with regulations to also support the organization’s efforts to improve its performance.
Governance integrated in
Drivers of Sustainable Organizational Success:

- **Customer and Stakeholder Focus**
  - Understanding and satisfying customer or service-user needs
  - Aligning all parts of an organization to these needs

- **Effective Leadership and Strategy**
  - Providing ethical and strategic leadership focused on sustainable value creation
  - Enabling key performance enablers, including strong corporate values, ethical culture, and organizational structures and processes

- **Integrated Governance, Risk and Control**
  - Deploying effective governance structures and processes with integrated risk management and control systems
  - Balancing performance and conformance in governance

- **Innovation and Adaptability**
  - Innovating processes and products to improve reputation and performance
  - Adapting the organization to changing circumstances

- **Financial Management**
  - Achieving strong financial management to support decision making and investments for sustainable growth
  - Managing cash flow, liaising with providers of finance, providing financial leadership in tax and treasury, and cost and profitability improvement

- **People and Talent Management**
  - Enabling people and talent management as a strategic function
  - Applying talent management to the finance function so it better serves the needs of the wider organization

- **Operational Excellence**
  - Aligning resource allocation with strategic objectives and the drivers of shareholder and stakeholder value
  - Supporting decision making with timely and insightful performance analysis

- **Effective and Transparent Communication**
  - Engaging stakeholders effectively to ensure that they receive relevant communications
  - Preparing high-quality business reporting to support stakeholder understanding and decision making
What are the main challenges for good governance in public sector organizations?

- Sovereign debt crisis
- Shortage of funding / rationalization
- Short-termism
- Internationalization, technology, complexity
- Corruption
What can a governance framework accomplish?

- Establish a benchmark for good governance
- Serve as a reference point for those developing or reviewing national codes
- Help public sector organizations continually improve governance systems
- Where no code/guidance exists, provide:
  - A shared understanding of what constitutes good governance
  - A powerful stimulus for positive action
Good Governance in the Public Sector: An International Framework
<table>
<thead>
<tr>
<th>Name</th>
<th>Affiliation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yoseph Asmelash</td>
<td>United National Conference on Trade &amp; Development (UNCTAD)</td>
</tr>
<tr>
<td>Ian Ball</td>
<td>Formerly IFAC</td>
</tr>
<tr>
<td>Andreas Bergmann</td>
<td>International Public Sector Accounting Standards Board (IPSASB)</td>
</tr>
<tr>
<td>Jón Blöndal</td>
<td>Organisation for Economic Co-operation &amp; Development (OECD)</td>
</tr>
<tr>
<td>Carlo Cottarelli</td>
<td>International Monetary Fund (IMF)</td>
</tr>
<tr>
<td>Robert Dacey</td>
<td>US Government Accountability Office (GAO)</td>
</tr>
<tr>
<td>Steve Freer</td>
<td>Formerly CIPFA</td>
</tr>
<tr>
<td>Gert Jönsson</td>
<td>International Organization of Supreme Audit Institutions (INTOSAI)</td>
</tr>
<tr>
<td>Mervyn King</td>
<td>King Committee on Corporate Governance</td>
</tr>
<tr>
<td>Ian McPhee</td>
<td>Australian National Audit Office</td>
</tr>
<tr>
<td>Maurice McTigue</td>
<td>George Mason University (USA)</td>
</tr>
<tr>
<td>Roger Tabor</td>
<td>Professional Accountants in Business Committee, IFAC</td>
</tr>
</tbody>
</table>
Public Sector Governance: Framework Layout

Framework:
• Foreword by Mervyn King, Chair, IIRC, and King Report, South Africa
• Definitions
• Principles-based to maximize relevance, applicability
• Sub-principles and supporting guidance to provide explanation

Supplement:
• Examples
  – Provide practical experience and aid understanding
• Evaluation questions to consider
• Further reading
The fundamental function of *good* governance in the public sector is to ensure that entities achieve their intended outcomes while acting in the public interest at all times.

- Good governance tied to:
  - Achieving intended outcomes
  - Acting in the public interest at all times
Public Sector Governance: Achieving Intended Outcomes While Acting in the Public Interest at all Times

A. Behaving with integrity, demonstrating strong commitment to ethical values, and respecting the rule of law

B. Ensuring openness and comprehensive stakeholder engagement

C. Defining outcomes in terms of sustainable economic, social, and environmental benefits

D. Determining the interventions necessary to optimize the achievement of the intended outcomes

E. Developing the entity’s capacity, including the capability of its leadership and the individuals within it

F. Managing risks and performance through robust internal control and strong public financial management

G. Implementing good practices in transparency, reporting, and audit, to deliver effective accountability
Public Sector Governance: Explicit Attention to Managing Risk

• “Proper risk assessment assists public sector entities in making informed decisions about the level of risk they are prepared to take, and implementing the necessary controls, in pursuit of the entities’ objectives.”

• “Effective risk management better enables public sector entities to achieve their objectives, while operating effectively, efficiently, ethically, and legally.”

• “Governing bodies should ensure that entities have effective risk management arrangements in place.”
• “Internal control supports a public sector entity in achieving its objectives by managing its risks while complying with rules, regulations, and organizational policies.”

• “Controls are a means to an end: the effective management of risks enables an entity to achieve its objectives.”

• “Public sector entities should also consider the need to remain agile, avoid over-control, and not become overly bureaucratic.”
Risk Management & Internal Control
Serious Risk Management & Internal Control Flaws

- Having a compliance-only mentality
- Treating risk as only negative and overlooking idea that entities need to take risk in pursuit of their objectives
- Risk management & internal control that is overly focused on external financial reporting
- Regarding risk management & internal control as a separate function or process
- Viewing risk management & internal control as predominantly important for operations
Current Thinking About Risk

The safest place for a ship…

… is to stay in the harbor

But that’s not what ships were made for…
Current Thinking About Risk

…Instead, ships were made to transport people & goods to other destinations…

…And that involves risk…

So, what is risk?

• Risk is defined as the “effect of uncertainly on (setting and achieving the organization’s) objectives” (ISO 31000)
• No Objectives = No Risk
• Therefore, risk should always be assessed in light of (setting and achieving) the organization’s objectives!
Q: How does your organization address uncertainty in achieving its strategic objectives?
A: Through our strategic management system
   – Line management engaged in plan-do-check-act cycle
   – Focused on achieving the organization’s objectives

Q: How does your organization address risk?
A: Through our risk management system
   – (Separate) risk and control system, staff functionaries, risk register
   – Focus on mitigating risk
Current Thinking About Risk Management

What does this example tell us?

• That we, risk management professionals, have made great progress in the area of risk management & internal control…

• ..But that we, in the process, lost the other people in our organization!
Current Thinking About Risk Management

Five lines of defense:
Current Thinking About **Risk Management**

**Five lines of defense:**

1. Players
2. Captain
3. Coach
4. Referee
5. PFF/FIFA
Current Thinking About Risk Management

Five lines of defense:

1. Players (Operational Staff)
2. Captain (Supervisor /Line Manager)
3. Coach (Risk Manager)
4. Referee (Internal Auditor)
5. PFF/ FIFA (External Auditor)
Current Thinking About Internal Control

From

Hindering the organization

To

Enabling the organization

Good internal control = The Invisible Hand
Main Objective of an Organization

• Is *not* to have effective controls…
• Is *not* to effectively manage risk…

But to

• Properly set & achieve its objectives
• Better adapt to surprises and disruptions
• And create sustainable value
Risk Is Inherent to Setting Your Objectives
Achieving Your Objectives Through Planning & Control

Strategic, tactical, and operational planning & control cycles
RM/IC Integral to Achieving Your Objectives

Level of Uncertainty

P A D C
P A D C
P A D C
P A D C
P A D C

Risk

Time

Strategic Level

Tactical Level

Operational Level

Controls

Objective
Managing Risk as an Integral Part of Managing an Organization
COSO Frameworks
2013 COSO Internal Control Cube
2004 COSO ERM Cube

Will be revised soon!
COSO IC vs. COSO ERM

Expanded into 3 components

Internal Environment
- Objective Setting
- Event Identification
- Risk Assessment
- Risk Response
- Control Activities
- Information & Communication
- Monitoring

Enterprise Risk Management—Integrated Framework

Internal Control—Integrated Framework
ISO 31000 Risk Management Standard
ISO 31000 Principles, Framework & Process

- a) Creates value
- b) Integral part of organizational processes
- c) Part of decision making
- d) Explicitly addresses uncertainty
- e) Systematic, structured and timely
- f) Based on the best available information
- g) Tailored
- h) Takes human and cultural factors into account
- i) Transparent and inclusive
- j) Dynamic, iterative and responsive to change
- k) Facilitates continual improvement and enhancement of the organization

Principles for managing risk (Clause 3)

Framework for managing risk (Clause 4)

Process for managing risk (Clause 5)

Diagram:
- Design of framework for managing risk (4.3)
  - Mandate and commitment (4.2)
  - Implementing risk management (4.4)
  - Continual improvement of the framework (4.6)
  - Monitoring and review of the framework (4.5)

- Establishing the context (5.3)
- Risk assessment (5.4)
  - Risk identification (5.4.2)
  - Risk analysis (5.4.3)
  - Risk evaluation (5.4.4)
  - Risk treatment (5.5)
- Communication and consultation (5.2)
- Monitoring and review (5.6)
ISO 31000 Risk Management Principles

• Creates Value
• Integral Part of Organizational Processes
• Part of Decision Making
• Explicitly Addresses Uncertainty
• Systematic, Structured & Timely
• Based on “Best Available Information”
• Tailored
• Considers Human & Cultural Factors
• Transparent & Inclusive
• Dynamic, Iterative & Responsive to Change
• Facilitates Continuous Improvement
ISO 31000 Risk Management Process

To be applied in every decision making process and subsequent execution!
**COSO ERM vs. ISO 31000**

Many organizations use both COSO ERM & ISO 31000…

<table>
<thead>
<tr>
<th>COSO</th>
<th>ISO 31000</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lengthy</td>
<td>Short</td>
</tr>
<tr>
<td>Focused on ERM</td>
<td>General approach to managing risk</td>
</tr>
<tr>
<td>One cube</td>
<td>Principles, framework &amp; process</td>
</tr>
<tr>
<td>Skewed to negative</td>
<td>Risk can be positive or negative</td>
</tr>
<tr>
<td>Risk already exists</td>
<td>Risk tied to achieving objectives</td>
</tr>
<tr>
<td>Risk &amp; opportunities</td>
<td>Opportunities also source of risk</td>
</tr>
<tr>
<td>More sequential process</td>
<td>More iterative process</td>
</tr>
</tbody>
</table>

…Biggest challenge is that concepts are not aligned
Risk Management & Internal Control Maturity
RM/IC Maturity Levels

Level 1: Non-existent or ad hoc
- Crisis management

Level 2: Internal control only
- Formal internal control, mainly focused on external financial reporting

Level 3: RM/IC as a silo
- Internal control complemented by risk management but still being seen as separate

Level 4: Integrated RM/IC
- Risk management, including internal control, integrated in organization’s system of management
Thoughts on Assessing RM/IC Maturity

- Consult and Communicate!
- Consider good practice developments
- Use the Frameworks
- Perform gap analysis
- Determine performance
- Look at audit results
- Analyze serious flaws
- …
- Continuously move to improvement!
RM/IC Maturity: Continuous Improvement

From RM/IC as objective in itself to RM/IC to help achieve objectives
From Auditor / staff driven to Driven from top down
From Rules-based to Performance & principles-based
From Off-the-shelf systems to Tailored to the organization
From Focused on loss minimization to Also focused on value creation
From Mainly hard controls to Recognizing culture & attitude
From Imposed to Implemented organically
From Stand-alone / “bolt-on” to Integrated / ”built-in”
From Static, out-of-date to Dynamic, evolving
From Seen as overhead to Seen as a sound investment
From Abandoned to Integrated in governance
Professional Accountant “Call to Action”
Champion importance of good governance & RM/IC:

- Professional accountants communicate with their organization’s leadership
- Attitude and actions of Professional accountant sets tone for good governance and RM/IC in organizations
- Promote integrating RM/IC into overall management of organization

- Most important element: making RM/IC part of every decision-making process and subsequent execution!
Support line management by providing high-quality advice, insight, and assurance:

• Decisions should only be made with explicit understanding of related risks and their potential consequences for achieving an organization’s objectives

• Therefore, decision makers require relevant and reliable information for their decision-making and control processes
Key Take Aways

• There are many flaws in current governance & RM/IC practices
• Achieving the organization’s objectives is the overall goal; risk is an inherent part
• Risk management should, therefore, be fully integrated in the organization’s system of management
• Professional accountants support RM/IC in various ways in the organizations they work for
• IFAC supports professional accountants
• However, no matter the guidance provided…
There will always be some …

… who do it their own way!
IFAC publications free-of-charge at www.ifac.org:

- Coming in May 2015: *From Bolt-on to Built-in Managing Risk as an Integral Part of Managing an Organization*
- *IFAC/CIPFA International Framework: Good Governance in the Public Sector*
- *Evaluating and Improving Governance in Organizations*
- *Integrating Governance for Sustainable Success*
- *Evaluating and Improving Internal Control in Organizations*
- *Defining and Developing an Effective Code of Conduct for Organizations*

- Also visit our new *Global Knowledge Gateway*