The Role of Operational Risk in ERM Framework

Dr. Abdulaziz Al-Terki
Head of Operational Risk
Burgan Bank – Kuwait
aalterki@burgan.com

MetricStream
GRC
SUMMIT 2013
MIDDLE EAST
October 29 - 30, 2013 | Dubai, UAE

www.GRC-Summit.com/MEA2013

Content

- Risk Management Overview
- Enterprise Risk Management (ERM)
- ERM Standard Framework
- Operational Risk Management (ORM)
- ORM Framework
- Risk Governance vs. Management
- Operational Risk Register
- ORM – The Way Forward

Definitions

❑ What is risk management?

Risk management is a process of thinking systematically about all possible risks, problems or disasters before they happen and setting up procedures that will avoid the risk, or minimize its impact, or cope with its impact. It is basically setting up a process where you can identify the risk and set up a strategy to control or deal with it.

❑ What is Operational Risk?

Basel II: Operational risk is the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events. This definition includes legal risk, but excludes ***strategic*** and ***reputation*** risk.

Importance of Risk Management

- **Effective Risk Management is very important for banks as a result of various factors:**

1. **Changing Environment**
   - Regulatory & Legal Requirements
   - Technology
   - Globalization
   - Governance
   - Expensive Insurance cost
   - Stakeholders changes attitudes
   - Fraud
2. **Risk Measurement:**
   - It is the ability to monitor through ***qualitative*** & ***quantitative*** models the patterns & behaviors of different risk categories

Why do we need Risk Management?

The only alternative to risk management is crisis management --- and crisis management is much more expensive, time consuming and embarrassing.

JAMES LAM, Enterprise Risk Management, Wiley Finance © 2003

Without good risk management practices, government cannot manage its resources effectively. Risk management means more than preparing for the worst; it also means taking advantage of opportunities to improve services or lower costs.

Sheila Fraser, Auditor General of Canada

Enterprise Risk Management

What is Enterprise risk management (ERM)?

Enterprise risk management (ERM) is the process of planning, organizing, leading, and controlling the activities of an organization in order to minimize the effects of risk on an organization's capital and earnings.

By identifying and proactively addressing risks and opportunities, we can protect and create value for our stakeholders.,

ERM supports value creation by enabling management to:

- Deal effectively with potential future events that create uncertainty.
- Respond in a manner that reduces the likelihood of downside outcomes and increases the upside.

The Risk Management Association (RMA) ERM Definition

“the management capability to manage all business risks in pursuit of acceptable returns.”

WHAT IS ERM? It is the capability to effectively answer the following quesions:

- Circular depiction is highly intentional
- Components are meant to be dynamic (reviewed back/forth in any sequence)
- Having the right culture is key

According to RMA:

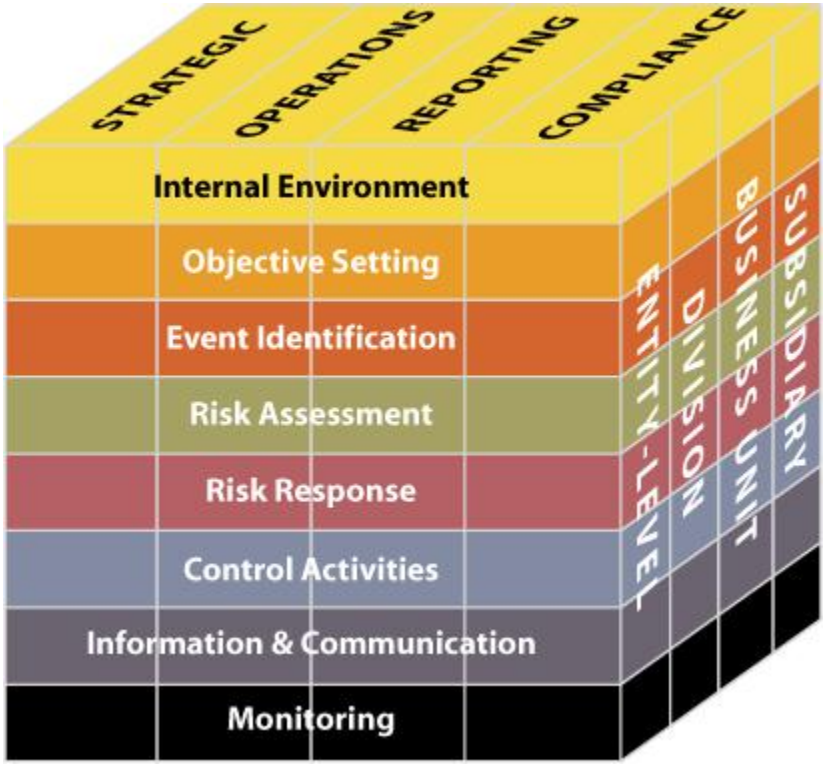
- Enterprise Risk Management, essential for any financial institution, encompasses all relevant risks.
- An ERM framework supports management competency to manage risks well, comprehensively, and with an understanding of the interrelationship/correlation among various risks.
- The successful institution incorporates a robust ERM capability as part of its culture by integrating what already exists to create a comprehensive and integrated view of the institution's risk profile in the context of its business strategy.

COSO defines ERM as:

"… 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 risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."

Source: COSO Enterprise Risk Management – Integrated Framework. 2004. The Committee of Sponsoring Organizations of the Treadway Commission (COSO)

COSO ERM Integrated Framework



COSO ERM Integrated Framework

- Defines essential enterprise risk management components
- Discusses key ERM principles and concepts
- Unifies ERM language across the organization
- Provides clear direction and guidance for enterprise risk management.

Enterprise Risk Management — Integrated Framework

- **Enterprise risk management expands the process to include not just risks associated with accidental losses, but also:**

- **Strategic :** These concern the long-term strategic objectives of the organization. They can be affected by such areas as capital availability, sovereign and political risks, legal and regulatory changes, reputation and changes in the physical environment.
- **Operations :** The risk incurred by an organization's internal activities which and sort of risk come under it. E.g.
  - IT Risk
  - Business Risk
- **Financial :** These concern the effective management and control of the finances of the organization and the effects of external factors such as availability of credit, foreign exchange rates, interest rate movement and other market exposures.
- **Compliance :** These concern such issues as health & Safety, environmental, job descriptions, consumer protection, data protection, employment practices and regulatory issues.

Operational Risk Management Framework (ORMF)

Key Elements of an Effective Operational Risk Framework

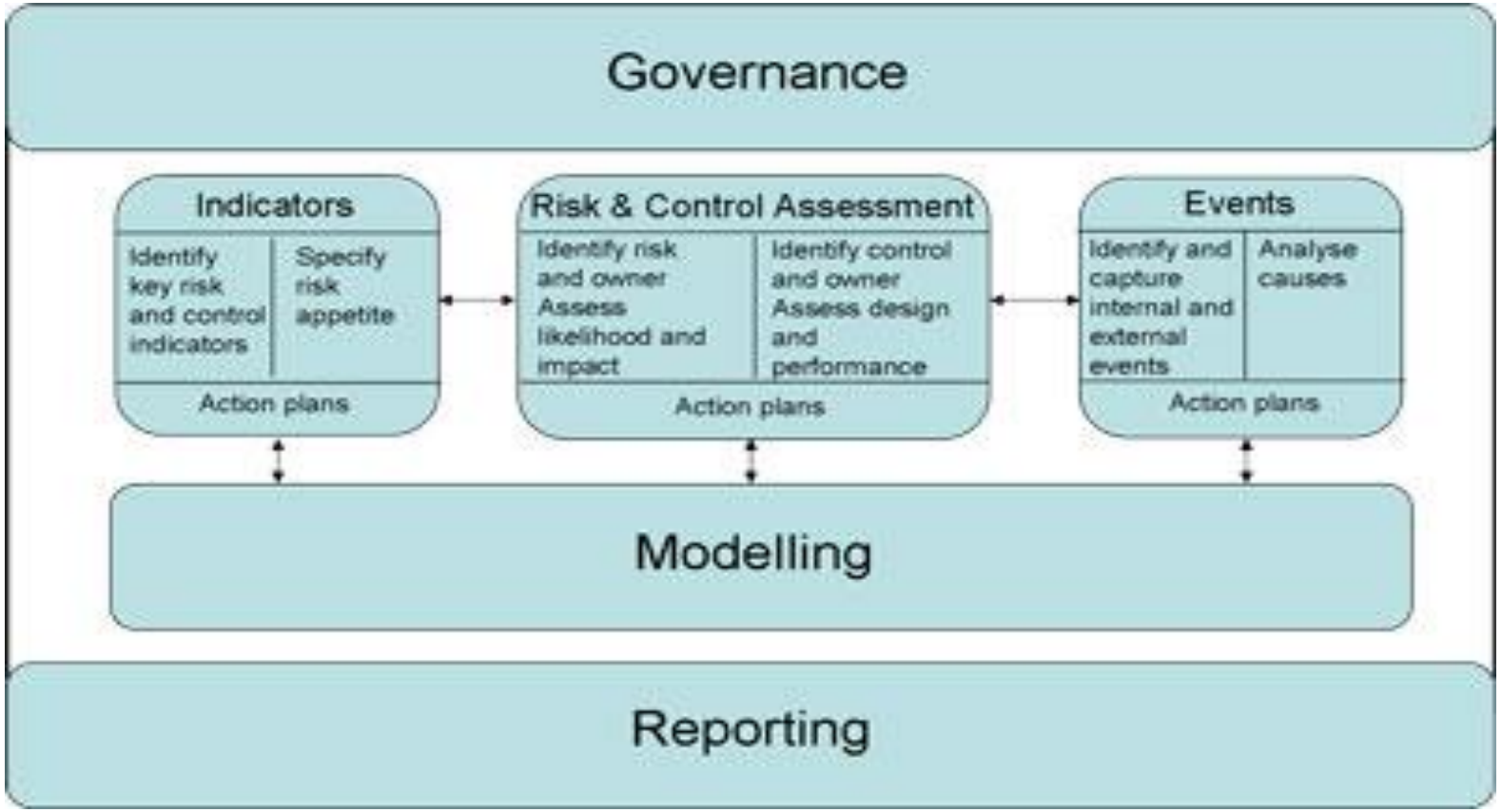
- Governance Structure
- Operational Risk Identification & Assessment methodology/process
- Operational Risk Measurement methodology
- Policies, procedures and processes for mitigating and controlling Operational Risks
- Process for the timely capture, analysis/monitoring and reporting of Operational
- Risks to key decision points within the bank

ORM Framework

Operational Risk Management Framework

Source: http://www.metricstream.com/solution_briefs/ORM.htm

ORM Governance Framework Structure



Source: http://www.chasecooper.com/Articles-Operational_Risk-Governance.php

Risk Governance vs. Management

The difference between Governance and Management

- Type of Processes and activities
- Roles and structures involved

Governance Aspects

- Risk Appetite and Tolerance
- Responsibilities and Accountability for Risk Management
- Awareness and Communication
- Risk Culture

Who Manage Risk ?

- **Different levels within an organization need different information from the risk management process.**

Board of Directors	Provides oversight
Risk Management Committee	Approve risk management policies Evaluate management of risks "Big Picture" analysis of risk trends
Risk Management	Assists in setting policies and standards that reflect the risk appetite of the organization
Senior Management	Manages and monitors risk
Audit and Compliance	Audit – Provides independent assurance Compliance – Provides independent review
Business Units	Responsible for owning and managing their business risks Set and implement policy consistent with Group-level policy

Type Of Risks

Basel II Type of Risk

Basel II was intended to create an international standard for banking regulators to control how much capital banks need to put aside to guard against the types of financial and operational risks banks face.

- **Basel II lists three types of risk:**
  - Credit risk
  - Market risk
  - Operational risk
- **What about liquidity risk?**
  - Market liquidity is the risk that a security can not be sold at all or quickly enough to prevent a loss.
  - Market liquidity risk is a type of market risk. It is addressed in ***Basel III***.
  - Funding liquidity risk is the risk that liabilities can not be met when due.
  - Funding liquidity risk is an operational risk.

Type of Operational Risk

- System Failure
- IT Security Breaches
- Human Error
- Regulatory Breaches
- Failure of Service Provider
- Server Storms
- Project Failure

The above Risks is sample of operational risk which result into:

- Direct Loss (e.g. expense, distraction)
- Indirect Loss (e.g. reputation, opportunity)

Operational Risk Register

There are Five steps to identify and qualify a risk into the Risk Register (RR):

- Identifying the risks that effect strategic and operational objectives
- Determining the actual owner of the risk
- Determining and assessing the existing controls in place
- Assessing the impact and likelihood of the risk after taking into account the existing controls to derive the net risk
- Determining further control improvements to mitigate the risk and indicate what their impact on net risk will be when they are fully implemented.

Operational Risk Management Role in ERM

❑ Identification of Risk:

- A systematic approach needs to be applied if all operational risks are to be identified and managed. By identifying areas of risk before an event or loss occurs, steps can be taken to prevent the event occurring and/or minimising the cost to the authority. Reacting to events only after they have occurred can be a costly method of risk identification.

❑ Analysis of risk:

- Having identified areas of potential risk they need to be systematically and accurately assessed. The process requires managers to make:
  - An assessment of the probability of a risk event occurring
  - An assessment of the potential severity of the consequences should such an event occur
  - An estimate of the likely cost of future incidents

Operational Risk Management Role in ERM

Once risks have been identified and assessed, all techniques to manage the risk fall into one or more of these four major categories:

- ❑ Avoidance (eliminate)
- ❑ Reduction (mitigate)
- ❑ Transfer (outsource or insure)
- ❑ Retention (accept and budget)

Operational Risk Management Role in ERM

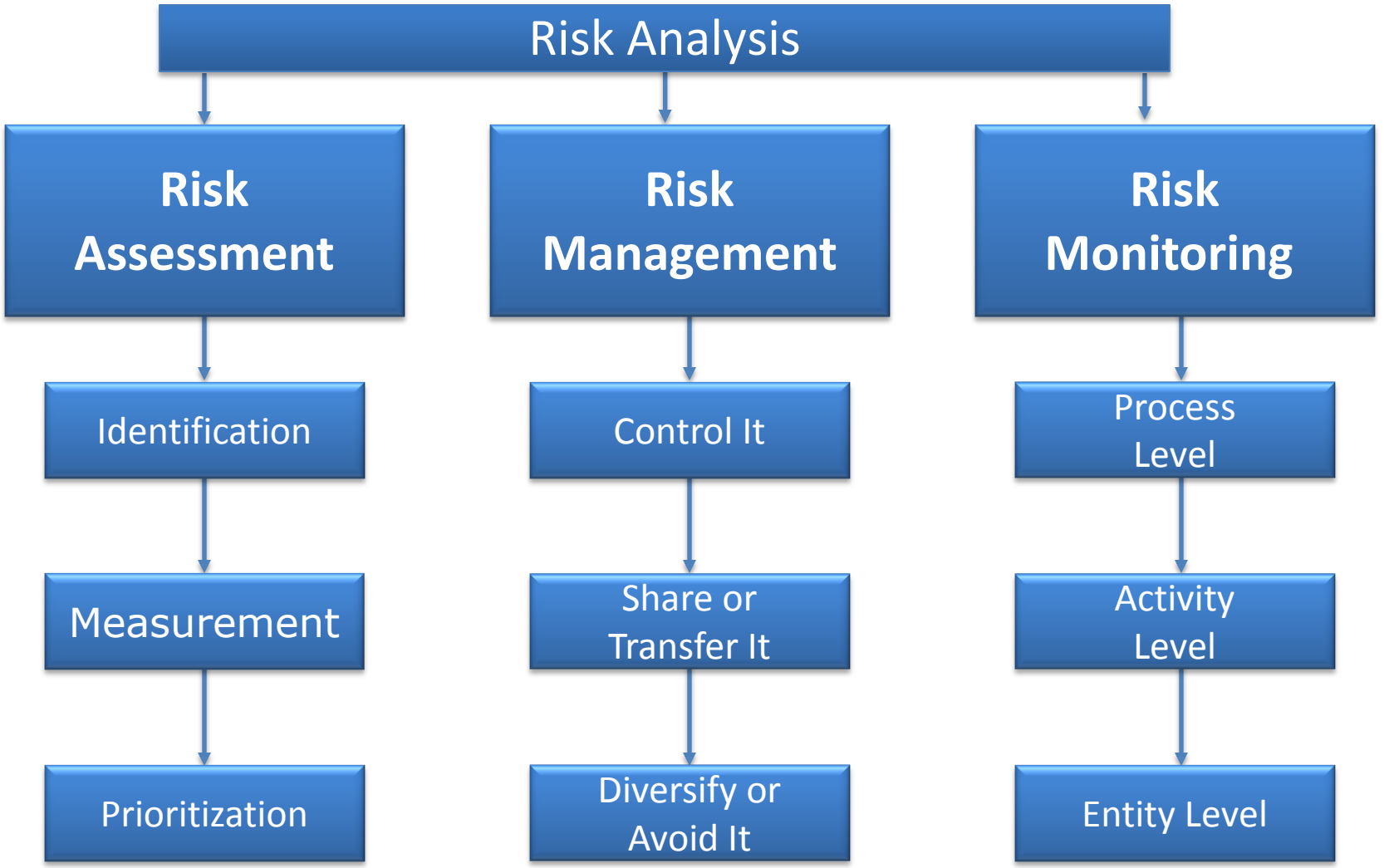
❑ Control of risk:

- Risk cannot be eliminated completely. Risk control is the process of taking action to minimize the likelihood of the risk event occurring and/or reducing the severity of the consequences should it occur. There are three options for controlling risk:
  - Accept = monitor
  - Avoid = eliminate (get out of situation)
  - Reduce = institute controls
  - Share = partner with someone (e.g. insurance, outsourcing)

❑ Monitoring and review of risk :

- The risk management process does not end when the risk control actions have been identified. Continuous monitoring and review should be applied on the following:
  - The implementation of the agreed control action
  - The effectiveness of the action in controlling the risk
  - How the risk has changed over time

Risk Analysis



Risk Assessment Methodology

For each and every risk category, a list of generic risks has been elaborated (risk register). Risk scenarios are identified using the risk register and assessed in terms of impact and likelihood considering a specific (worst-case) scenario with respect to critical activities / services / processes and their resources. Evaluation takes account of existing risk mitigation (prevention / protection) measures.

Risk Control Self Assessment (RCSA) can be conducted in Five steps:

- **Step 1**: Get the buy in from the Board and Upper Management to ensure their continuous support
- **Step 2**: Create a comprehensive Risk Assessment plan in coordination with the Business owners
- **Step 3**: Decide on an effective method to be used for conducting the RCSA
- **Step 4**: Register all information into the risk management tool
- **Step 5**: Monitor, report and incorporate the whole process into the yearly plan

Risk Assessment Methodology

- Sample of Risk Matrix:

LIKELIHOOD × IMPACT = RISK LEVEL

- **Suggested Impact Matrix:**
  - Financial Impact
  - Operational (IT & Business)

    (Impact on other activities / Services / processes)
  - Quality of Service /Customer Satisfaction Impact
  - Reputational Impact
  - Legal / Compliance / Regulatory Impact

Operational Risk Register - Sample

- **Asset Risks:**
  - **E.g. Building Collapse / construction defects**
- **Human Resource Risks:**
  - **E.g. Insufficient expertise**
- **Natural Hazards Risks:**
  - **E.g. Sever Storm**
- **Environmental Risks:**
  - **E.g. Civil commotion, war, terrorism**
- **IT Security Risks:**
  - **E.g. Virus / hacking**

Risk Register - Sample

Risk Description	Risk Category	Risk Impact	Impact	Likelihood	Risk Severity	Residual Risk	Residual Risk Severity	Risk Mitigation
Breach of IT security	Operational	Financial Reputation Customer Dissatisfaction Market Share	4	3	4 x 3 = 12	2	4 x 2 = 8	Documented IT security policies Staff training / awareness sessions Internal/ External Audit Reports Risk Assessment Logical Access Control

Risk Appetite & Tolerance

- Risk appetite: is the amount of risk an entity is prepared to accept when trying to achieve its objectives. Two factors are important:
  - The enterprise's objective capacity to absorb loss, e.g., financial loss, reputation damage
  - The (management) culture or predisposition towards risk taking – cautious or aggressive. What is the amount of loss the enterprise wants to accept to pursue a return?

- Risk tolerance is the tolerable deviation from the level set by the risk appetite definition, e.g. standards require projects to be completed within of 10% of budget or 20% of time are tolerated

- Risk appetite and tolerance change over time;

- New technology, new organizational structure, new market conditions, new strategy and many other factors require the enterprise to reassess its risk portfolio at regular intervals and reconfirm the risk appetite at regular intervals

Risk Appetite & Tolerance - Cont.

- The cost of mitigation options where the cost/business impact of risk mitigation options exceeds an enterprise's capabilities / resources, thus forcing higher tolerance for one of more risk conditions.
  - E.g. if a regulation says that 'sensitive data at rest must be encrypted'. Yet there is no feasible encryption solution or the cost of implementing a solution would have a large negative impact, the enterprise may choose to accept the risk associated with regulatory non-compliance, which is a risk trade-off

Risk Culture

Risk Culture – Potential Issues:

- Misalignment between 'real' culture and policies
  - Resulting in potential non-compliance and/or undue risk
- Blaming culture versus Learning culture

Risk Culture

Risk Management Reference Guide

Can be used across the enterprise to disseminate Risk Management culture and to asset the ERM

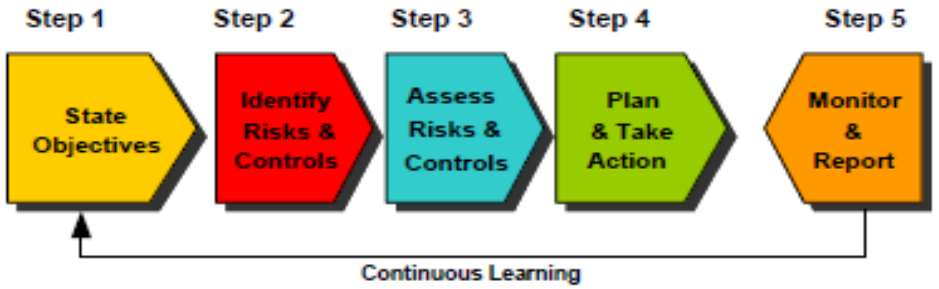
1- State Objectives
2- Identify Risk and Controls
3- Assess Risk and Control
4- Plan and Take Action
5- Monitor and Report

See the following sample

Sample

INTEGRATED RISK MANAGEMENT QUICK REFERENCE GUIDE

The OPS risk management process



Step 1: State (or establish) objectives

- Define context and confirm objectives
- Risks must be assessed and prioritized in relation to the objective
- The more specific the objectives (specific goals, key milestones, deliverables and commitments) the easier it is to assess potential risks
- Risks can be assessed at any level; operational, program, initiative, unit, branch, health system

Risk (uncertainty)
The chance that a future event will impact the achievement of established objectives. Risks can be positive or negative.

Control / Mitigation Strategy
Controls/ mitigation strategies put in place by management to minimize negative risks or maximize opportunities.

Consequences

- Identify the specific consequences of each risk, if the risk in fact occurred
- Consider and quantify consequences in relation to cost, quality, time, etc.

Cause/Source of Risk

- Understand the cause/source of each risk
- Use a cause/effect diagram

Step 2: Identify risks & controls

Identify risks - What could go wrong?

- Always use the 13 categories of risk
- Examine trends and consider past risk events
- Obtain information from similar organizations or projects
- Brainstorm with colleagues and/or stakeholders
- Increase awareness of new initiatives/ agendas and regulations, consider interdependencies
- Document short-term and long-term consequences for each risk (consider interdependencies)

Identify existing controls – What do you already have in place?

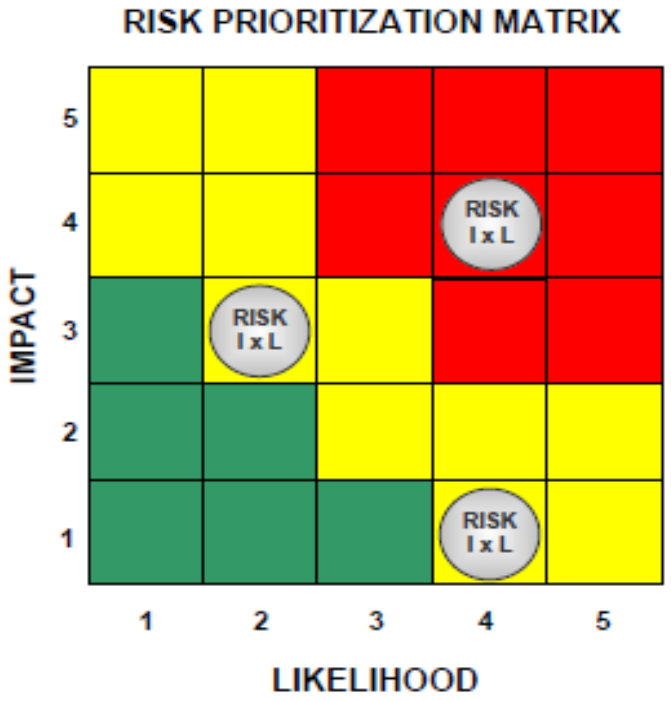
- Preventative controls (address causes and source of risk)
- Corrective / Recovery controls (focuses on reducing impact after risk has occurs)

13 categories of risk

RISK	DESCRIPTION
Compliance/ Legal	Uncertainty regarding compliance with laws, regulations, standards, policies, directives, contracts; may expose the ministry to the risk of fines, penalties, litigation.
Equity	Uncertainty that policies, programs, services will have an equitable impact on the population.
Financial	Uncertainty of obtaining, using, maintaining economic resources; meeting overall financial budgets/commitments; preventing, detecting or recovering fraud.
Governance / Organizational	Uncertainty of having appropriate accountability and control mechanisms such as organizational structures and systems processes; systemic issues, culture and values, organizational capacity, commitment, and learning and management systems, etc.
Information / Knowledge	Uncertainty regarding the access to or use of accurate, complete, relevant and timely information. Uncertainty regarding the reliability of information systems.
Operational or Service Delivery	Uncertainty regarding the performance of activities designed to carry out any of the functions of the ministry/unit, including design and implementation.
People / Human Resources	Uncertainty as to the ministry's/ business unit's ability to attract, develop and retain the talent needed to meet its objectives.
Political	Uncertainty of the events may arise from or impact any level of the government including the Offices of the Premier or Minister, e.g. a change in government political priorities or policy direction.
Privacy	Uncertainty with regards to the safeguarding of personal information or data, including identity theft or unauthorized access.
Security	Uncertainty relating to physical or logical access to data and locations (offices, warehouses, labs, etc).
Stakeholder / Public Perception	Uncertainty around the expectations of the public, other governments, media or other stakeholders; maintaining positive public image; ensuring satisfaction and support of partners.
Strategic / Policy	Uncertainty that strategies and policies will achieve required results or that policies, directives, guidelines, legislation will not be able to adjust as necessary.
Technology	Uncertainty regarding alignment of IT infrastructure with technology and business requirements. Uncertainty of the availability and reliability of technology.

V 2

Sample



Step 3: Assess Risks & Controls

Assess inherent risks

- *Inherent likelihood* – Without any mitigation, how likely is this risk to occur?
- *Inherent impact* – Without any mitigation, how big will be the impact of the risk on your objective?
- *Inherent Risk Prioritization* - Rate inherent likelihood, impact and proximity of the risk.
- *Risk Owner* - Identify the specific person accountable if the risk occurs. Involve Risk Owner if not already involved.

Assess existing controls

- *Controls* - Evaluate the effectiveness of existing mitigation strategies.
- *Control Owner* - Identify the person accountable for implementing specific control. Involve Control Owner if not already involved.

Reassess residual risks

- *Residual likelihood* – With existing mitigation strategies in place, how likely is this risk to occur?
- *Residual impact* – With existing mitigation strategies in place, how big an impact will this risk have on your objective?
- *Residual Risk Prioritization* - Re-assess the impact, likelihood and proximity of the risk with mitigation strategies in place.
- Use the 'Risk Assessment Worksheet' available through the Integrated Risk Management Team.

Rating Scale

VALUE	LIKELIHOOD	IMPACT	PROXIMITY	*SCALE*
1	Unlikely to occur	Negligible Impact	More than 36 months	*Very Low*
2	May occur occasionally	Minor impact on time, cost or quality	12 to 24 months	*Low*
3	Is as likely as not to occur	Notable impact on time, cost or quality	6 to 12 months	*Medium*
4	Is likely to occur	Substantial impact on time, cost or quality	Less than 6 months	*High*
5	Is almost certain to occur	Threatens the success of the project	Now	*Very High*

Step 4: Plan & Take Action

- For each of the 13 risk categories establish risk appetite and tolerances with senior management.
- Assess existing mitigation strategies have reduced the risk rating (Impact x Likelihood) so that the risk is below approved risk tolerance levels.
- Evaluate whether further mitigation strategies are needed.
- Develop SMART (Specific, Measurable, Achievable, Realistic, Time-specific) actions that will either reduce the likelihood of the risks or minimise the impact.
- Develop detailed action plans with timelines, responsibilities and outline deliveries.
- Use the 'Action Plan Worksheet' available through the Integrated Risk Management Team.

Step 5: Monitor & Report

- Ensure processes are in place to review risk levels and the effectiveness of mitigation strategies
- Use risk indicators
- Monitor and report by asking:
  - Have risks changed? How?
  - Are there new risks? Assess them.
  - Do you need to report or escalate risks? To whom? When? How?
- The Integrated Risk Management Team can help you establish monitoring processes.

Key Risk Indicators (KRI)

- *Leading Indicators* - Early or leading indicators that measure sources or causes to help prevent risk occurrences
- *Lagging Indicators* - Detection and performance indicators that help monitor risks as they occur

Risk Tolerance

- The amount of risk that the entity can manage for the area being assessed.

Risk Appetite

- The amount of risk that the entity is willing to manage for the area being assessed.

Operational Risk Management (The way forward)

Key Elements of an Effective Operational Risk within ERM Framework

- ORM Governance Structure needs to be developed using best practices and quality standards
- Effective Operational Risk Identification & Assessment methodology, process and techniques
- Effective Operational Risk Measurement methodology (***qualitative*** & ***quantitative***) and maturity
- Unification of policies, procedures and processes for mitigating and controlling Operational Risks
- Effective monitoring and reporting of Operational Risks to the decision makers and stakeholders
- Adopting effective and simplified risk assessment techniques that fits your organizational needs
- Connecting strategic objectives with risks to continue focusing on critical activities
- Effective and comprehensive Enterprise Risk Appetite will tie up all organizational risks together
- Develop and communicate ERM Reference Guide to disseminate the RM culture

In Summary

- Risk Management Overview
- Enterprise Risk Management (ERM)
- ERM Standard Framework
- Operational Risk Management (ORM)
- ORM Framework
- Risk Governance vs. Management
- Operational Risk Register
- ORM – The Way Forward

Q & A

MetricStream

GRC SUMMIT 2013

MIDDLE EAST

October 29 - 30, 2013 | Dubai, UAE

Thank You

MetricStream

GRC SUMMIT 2013

MIDDLE EAST

October 29 - 30, 2013 | Dubai, UAE

www.GRC-Summit.com/MEA2013