

Understanding Your Organization

Facilitator: Raj Sharma
GM Risk & Governance, HFC
22 June 2012

Contents

Nos	Subtopic
1	Objective of the Presentation
2	Risk Management & Processes
3	Risk Management Drivers & Challenges
4	ISO 31000 and Its Importance
5	Enterprise Risk Management (with Integration of Vision, Mission and Value)
6	Internal Audit Practices and Opinion Formulation
7	Conclusion & Recommendation
8	Questions & Answers



Objectives

To know :

- Status of the Risk Management Process in an organization;
- Drivers of the Risk Management in an organization;
- Risk Management Responsibilities and Challenges;
- The principles of ISO 31000 and the importance;
- The ERM Challenges and Success Factors;

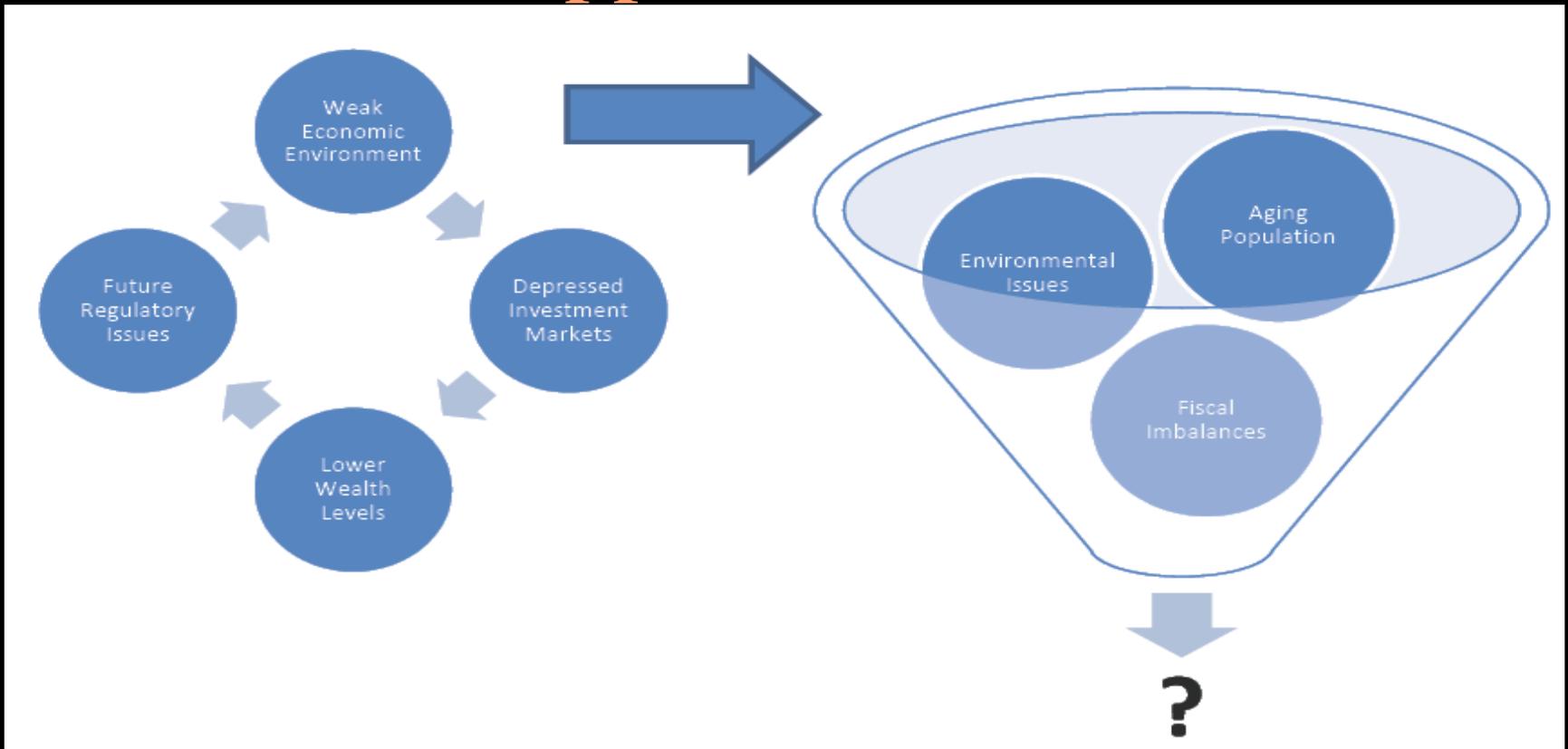
Objectives (con't)

- Integration of ERM to Corporate Vision/ Mission and Objectives;
- Essential Practices of Risk Management;
- Internal Audit Risk Management Practices; and
- Formulating Internal Audit Opinions.

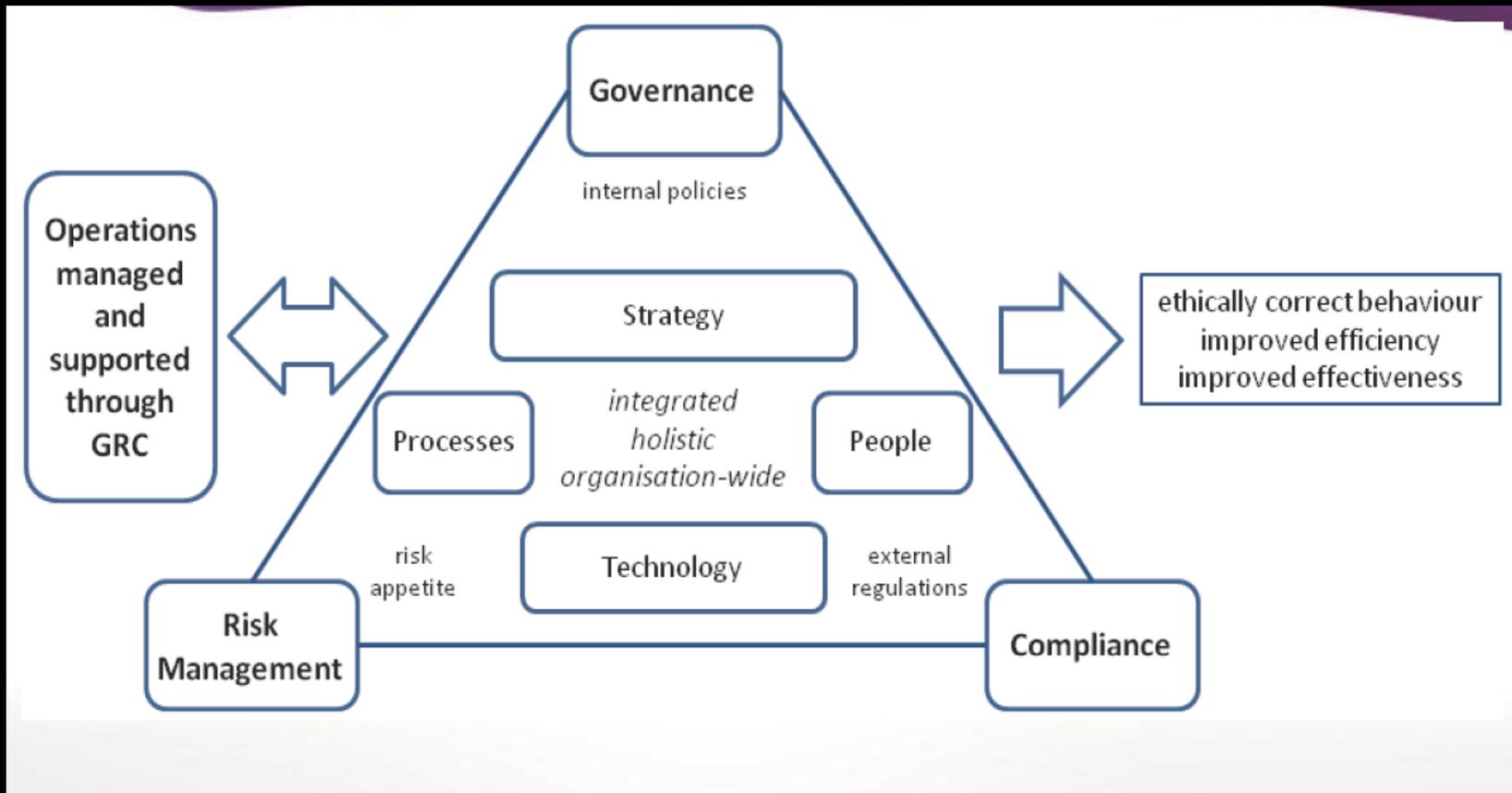
Risk Management

Your Understanding of:	Limited	Some	Good	Expert
Risk Management Practices and Frameworks				
Your Organization's Risk Management Process	Forming	Evolving	Stabilized	Established

Risk Management Challenges & Opportunities



Internal Dynamics of GRC



Drivers of Risk Management

- What is “driving” your organization’s interest ?
- Who is the risk management “champion”?
- Who “manages and coordinates” the risk management process?
- What is the “mix” of Internal Audit’s assurance and consulting services in the organization’s risk management process?
- Has your organization had a formal assessment of the risk management process?

IA's Risk Management Responsibilities and Challenges

- Internal audit activity must evaluate the effectiveness;
- Contribute to the improvement of risk management processes;
- Whether risk management processes are effective judgment resulting from the internal auditor's assessment;

IA's Risk Management Responsibilities and Challenges

- Organizational objectives that support and align with the organization's mission;
- Significant risks are identified and assessed;
- Appropriate risk responses are selected that align risks with the organization's risk appetite; and
- Risk information is captured and communicated in a timely manner across the organization, enabling staff, management, and the board to carry out their responsibilities.

IA's Risk Management Responsibilities and Challenges

- **2120. A1** – The internal audit activity must evaluate risk exposures relating to the organization's governance, operations, and information systems regarding the:
 - Reliability and integrity of financial and operational information.
 - Effectiveness and efficiency of operations and programs.
 - Safeguarding of assets; and
 - Compliance with laws, regulations, policies, procedures and contracts.

IA's Risk Management Responsibilities and Challenges

- The internal audit activity must evaluate the potential for the occurrence of fraud and how the organization manages fraud risk.
- **2120.C1** – During consulting engagements, internal auditors must address risk consistent with the engagement's objectives and be alert to the existence of other significant risks.
- **2120.C2** – Internal auditors must incorporate knowledge of risks gained from consulting engagements into their evaluation of the organization's risk management processes.
- **2120.C3** – When assisting management in establishing or improving risk management processes, internal auditors must refrain from assuming any management responsibility by actually managing risks.

IA's Risk Management Responsibilities and Challenges

- Providing assurance on ERM –Key requirements of the board or its equivalent is to gain assurance;
- That risk management processes are working effectively; and
- That key risks are being managed to an acceptable level.

IA's Risk Management Responsibilities and Challenges

Other sources include external auditors and independent specialist reviews. Internal auditors will normally provide assurances on three areas:

- Risk management processes, both their design and how well they are working;
- Management of those risks classified as 'key', including the effectiveness of the controls and other responses to them; and
- Reliable and appropriate assessment of risks and reporting of risk and control status.

Enterprise Risk Management

Enterprise Risk Management (ERM) methods and processes used by organizations to manage risks related to the achievement of their objectives.

ERM provides a framework for risk management - identifying particular events or circumstances relevant to the organization's objectives (risks and opportunities),

- Assessing them in terms of likelihood Risk and magnitude of impact,
- Determining a response strategy, and monitoring progress.
- By identifying and proactively addressing risks and opportunities,
- Business enterprises protection and create value for their stakeholders,
- Including owners, employees, customers, regulators, and society overall

Best Practice Risk Management

The leading institutions will be distinguished by their intelligent management of risk.

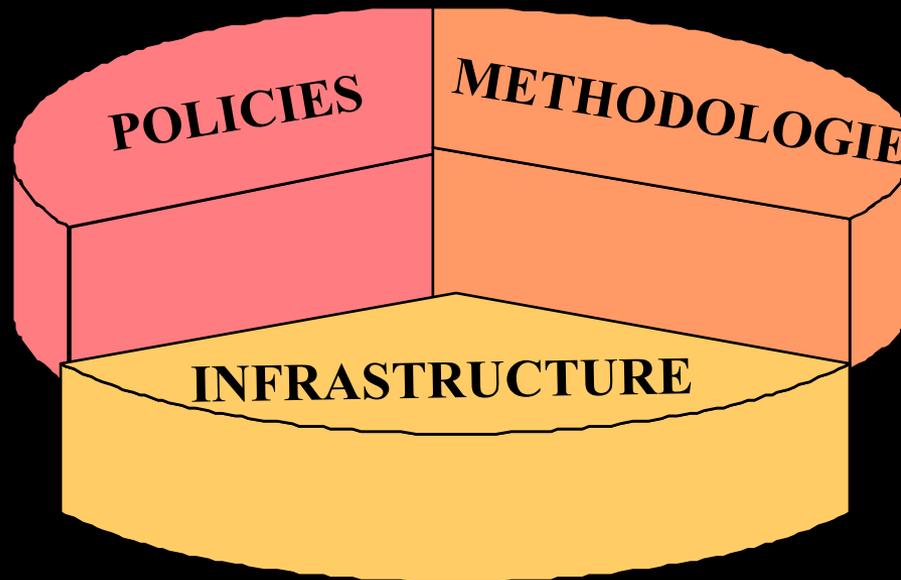
Goal:

- Independence And Partnership
- Establish A First Class Risk Management Function
- Which Is Independent Of The Direct Risk Takers
- But Works In Partnership With Them

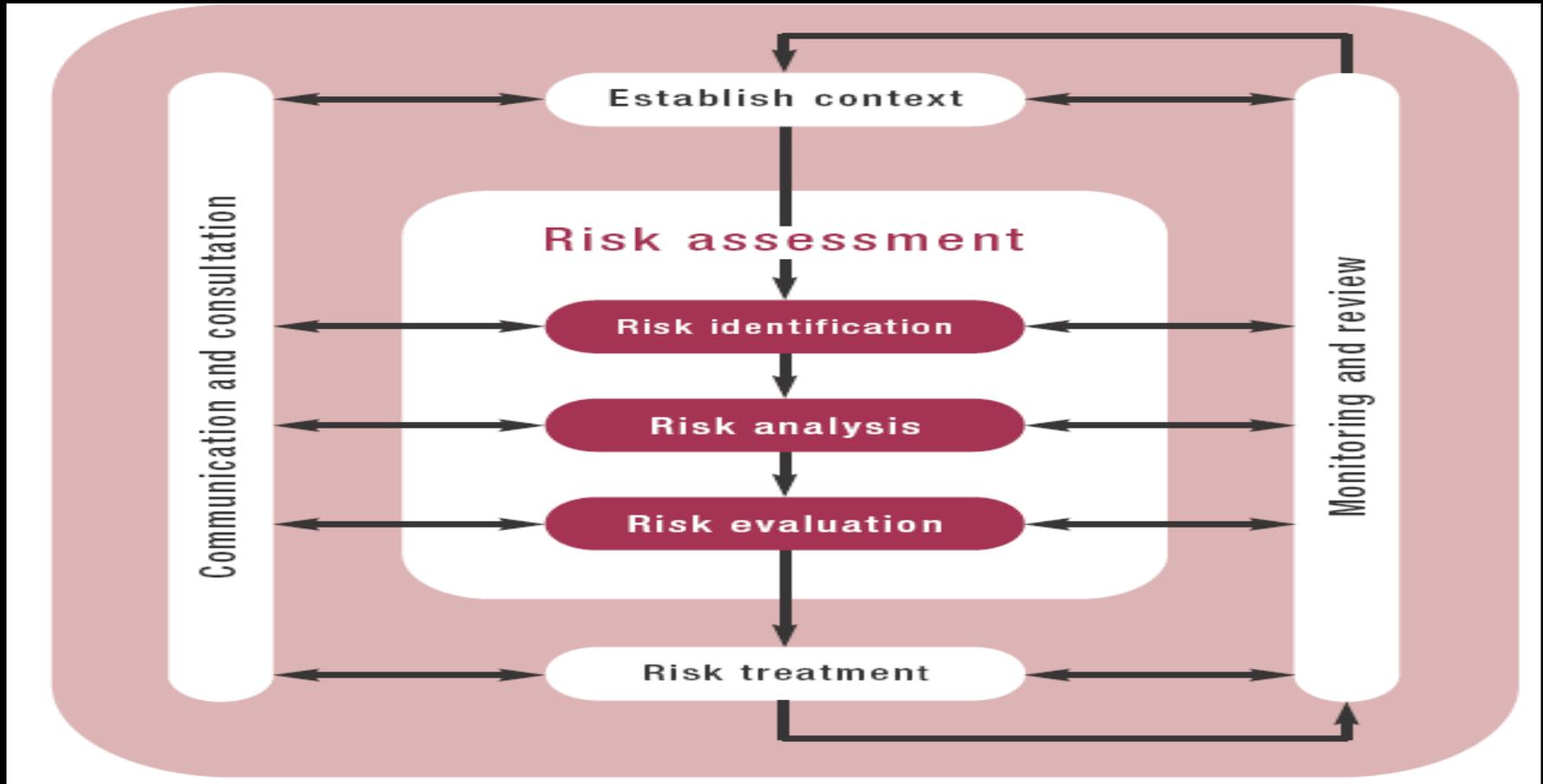


Best Practice Risk Management

- Framework for Risk Management can be benchmarked in terms of:



ISO 31000



ISO 31000

- Principles for managing risk (the foundation that can be used to embed the management of risk in all levels of the organization), and
- Processes for managing risk (which follow AS/NZS 4360)
 - Communication and Consultation
 - Establishing the Context
 - Risk Assessment
 - Risk Treatment
 - Monitoring and Review

ISO 31000 Principles

1. Creates and protects value
2. Is an integral part of all organizational processes
3. Is part of decision making
4. Explicitly addresses uncertainty
5. Is systematic, structured and timely
6. Is based on the best available information

ISO 31000 Principles (Con't)

7. Is tailored (and is aligned with the organization's internal/external context and risk profile)
8. Takes human and cultural factors into account
9. Is transparent and inclusive
10. Is dynamic, iterative and responsive to change
11. Facilitates continual improvement of the organization

ERM Challenges and Success Factors

- **Challenges**
 - Governance oversight (or ERM process override)
 - “Process Owners” (another unfunded mandate)
 - Disconnects (ERM & HR)
 - Finding the “right” KRI
 - Risk Identification (blind-spots & disconnects)

ERM Challenges and Success Factors

- **Success Factors**
 - Strong/visible support
 - ERM is linked to key objectives
 - ERM is built into a well-accepted process
 - Cross-functional & dedicated ERM group
 - Continuous process improvement

Activity: Initial Risk Mgmt “Maturity Assessment”

Culture (Entity-Level) Components	Forming	Evolving	Stabilized	Established
<u>INTERNAL ENVIRONMENT</u>				
• Risk Management Philosophy				
• Risk Appetite				
• Board of Directors				
• Integrity and Ethical Values				
• Commitment to Competence/HR Standards				
• Organization Structure/Assignment of Authority & Responsibility				
<u>RISK RESPONSE</u>				
• Evaluation & Selection of Risk Responses				
<u>INFORMATION AND COMMUNICATION</u>				
• Communication (entity-wide processes and channels)				
<u>MONITORING</u>				
• Reporting “Deficiencies” (to decision makers and appropriate governing body)				

Internal Environment

Risk Management Philosophy

- The entity's risk management philosophy represents the shared beliefs and attitudes characterizing how the entity considers risk in all activities
- It reflects the entity's values, influencing its culture and operating style
- It affects how enterprise risk management components are applied, including how events are identified, the kinds of risks accepted, and how they are managed
- It is well developed, understood, and embraced by the entity's personnel
- It is captured in policy statements, oral and written communications, and decision making
- Management reinforces the philosophy not only with words but also with everyday actions

Practices/"Controls"

- Organization Mission & Values
- Risk Management "Policy"
- Key Policies (& Procedures)
- Management Actions
- Risk Culture Surveys
- _____

Internal Environment

Risk Appetite

- The entity's risk appetite reflects the entity's risk management philosophy and influences the culture and operating style.
- It is considered in strategy setting, with strategy aligned with risk appetite.

Practices/"Controls"

- Strategic Planning Process
- Board Oversight
- Risk Mgmt "Policy"
- Key Policies
- Management Actions
- Risk Culture Surveys

Internal Environment

Board of Directors	Practices/"Controls"
<ul style="list-style-type: none"> • The board is active and possesses an appropriate degree of management, technical, and other expertise, coupled with the mind-set necessary to perform its oversight responsibilities • It is prepared to question and scrutinize management's activities, present alternative views, and act in the face of wrongdoing • It has at least a majority of independent outside directors • It provides oversight to enterprise risk management and is aware of and concurs with the entity's risk appetite 	<ul style="list-style-type: none"> • Risk Mgmt "Policy" (Roles/Responsibilities) • Board Committees & Member "Attributes" • Chief Risk Officer Communication • Mgmt Risk Council Reporting • _____

Internal Environment

Integrity & Ethical Values

- The entity's standards of behavior reflect integrity and ethical values
- Ethical values not only are communicated but also accompanied by explicit guidance regarding what is right and wrong
- Integrity and ethical values are communicated through a formal code of conduct
- Upward communications channels exist where employees feel comfortable bringing relevant information
- Penalties are applied to employees who violate the code, mechanisms encourage employee reporting of suspected violations, and disciplinary actions are taken against employees who knowingly fail to report violations
- Integrity and ethical values are communicated through management actions and the examples they set

Practices/"Controls"

- Organization Mission & Values
- Code of Conduct
- "Hot-Lines"
- Risk Culture Surveys
- _____

Internal Environment

Commitment to Competence

- Competence of the entity's people reflects the knowledge and skills needed to perform assigned tasks
- Management aligns competence and cost
- _____
- _____

Practices/"Controls"

- "Core" Competency Models/Forecasts
- Risk Mgmt Training Activities
- Risk Culture Surveys
- _____

Internal Environment

Human Resource Standards

- Standards address hiring, orientation, training, evaluating, counseling, promoting, compensation, and remedial actions, driving expected levels of integrity, ethical behavior, and competence
- Disciplinary actions send the message that violations of expected behavior will not be tolerated
- _____
- _____

Practices/”Controls”

- “Key” HR Policies & Procedures
- Compensation “Philosophy” & Program
- Risk Culture Surveys
- _____

Internal Environment

Organizational Structure	Practices/”Controls”
<ul style="list-style-type: none">• The organizational structural defines key areas of responsibility and accountability• It establishes lines of reporting• It is developed in consideration of the entity’s size and nature of activities• It enables effective enterprise risk management	<ul style="list-style-type: none">• Organization “Design”• Risk Mgmt “Policy”• Management Actions• Risk Culture Surveys• _____

Internal Environment

Assignment of Authority and Responsibility

- Assignment of authority and responsibility establishes the degree to which individuals and teams are authorized and encouraged to use initiative to address issues and solve problems, and provides limits to authority.
- The assignments establish reporting relationships and authorization protocols.
- Policies describe appropriate business practices, knowledge and experience of key personnel, and associated resources.
- Individuals know how their actions interrelate and contribute to achievement of objectives.

Practices/”Controls”

- Entity-Level Approval Matrix
- Risk Mgmt “Policy”
- Key Policies
- Risk Culture Surveys
- _____

Risk Responses – Sample Principles

Evaluating Possible Responses

(Avoid, Reduce, Share, Accept – or Exploit)

- Responses are evaluated with the intent of achieving residual risk aligned with the entity’s risk tolerances
- In evaluating risk responses, management considers their effects on likelihood and impact
- Management considers their costs versus benefits, as well as new opportunities

Practices/”Controls”

- Chief Risk Officer
“Aggregation” Activities
- “Dashboard or Heat Map” Reporting
- Mgmt Risk Council Activities (& Decisions)
- Management Actions
- Board Oversight
- Risk Mgmt (Identification & Assessment) Methodology
- _____

Risk Responses – Sample Principles

Evaluating Possible Responses (Avoid, Reduce, Share, Accept – or Exploit)	Practices/”Controls”
<p>Selected Responses</p> <ul style="list-style-type: none"> • Responses chosen by management are designed to bring anticipated risk likelihood and impact within risk tolerances • Management considers additional risks that might result from a response <p>Portfolio View</p> <ul style="list-style-type: none"> • Management considers risk from an entity-wide, or portfolio, perspective • Management determines whether the entity’s residual risk profile is commensurate with its overall risk appetite 	<ul style="list-style-type: none"> • Chief Risk Officer “Aggregation” Activities • “Dashboard or Heat Map” Reporting • Mgmt Risk Council Activities (& Decisions) • Management Actions • Board Oversight • Risk Mgmt (Identification & Assessment) Methodology • _____

Information and Communication – Sample Principles

Communication	Practices/”Controls”
<ul style="list-style-type: none"> • Management provides specific and directed communication addressing behavioral expectations and responsibilities of personnel, including a clear statement of the entity’s risk management philosophy and approach and clear delegation of authority • Communication about processes and procedures aligns with, and underpins, the desired culture • All personnel receive a clear message from top management that enterprise risk management must be taken seriously • Personnel know how their activities relate to the work of others, enabling them to recognize problems, determine cause, and take corrective action • Personnel know what is deemed acceptable and unacceptable behavior 	<ul style="list-style-type: none"> • Organization Mission & Values • Risk Mgmt Policy • Key Policies (& Procedures) • Code of Conduct • Hot-Lines • Mgmt Communication “Vehicles” • Management Actions • CRO Communication “Vehicles” • Risk Culture Surveys • _____

Information and Communication – Sample Principles

Communication	Practices/”Controls”
<ul style="list-style-type: none"> • There are open channels of communication and a willingness to listen, and personnel believe their superiors truly want to know about problems and will deal with them effectively • Communications channels outside normal reporting lines exist, and personnel understand there will be no reprisals for reporting relevant information • An open communications channel exists between top management and the board of directors, with appropriate information communicated on a timely basis • Open external communications channels exist, where customers and suppliers can provide significant input • The entity communicates relevant information to regulators, financial analysts, and other external parties 	<ul style="list-style-type: none"> • Organization Mission & Values • Risk Mgmt Policy • Key Policies (& Procedures • Code of Conduct • Hot-Lines • Mgmt Communication “Vehicles” • Management Actions • CRO Communication “Vehicles” • Risk Culture Surveys • _____

Monitoring – Sample Principles

Reporting Deficiencies	Practices/"Controls"
<ul style="list-style-type: none"> • Deficiencies reported from both internal and external sources are carefully considered for their implications for enterprise risk management, and appropriate corrective actions are taken • All identified deficiencies that affect the entity’s ability to develop and implement its strategy and to achieve its established objectives are reported to those positioned to take necessary action • Not only are reported transactions or events investigated and corrected, but potentially faulty underlying procedures also are reevaluated • Protocols are established to identify what information is needed at a particular level for effective decision making 	<ul style="list-style-type: none"> • “Dashboard or Heat Map” Reporting • Key Risk (& Performance) Indicators • Mgmt Risk Council Activities (& Decisions) • Chief Risk Officer Communication • Board Oversight • _____

ERM Roles & Responsibilities

Board of Directors

- Risk management effectiveness, risk appetite, and significant risk & appropriateness of responses

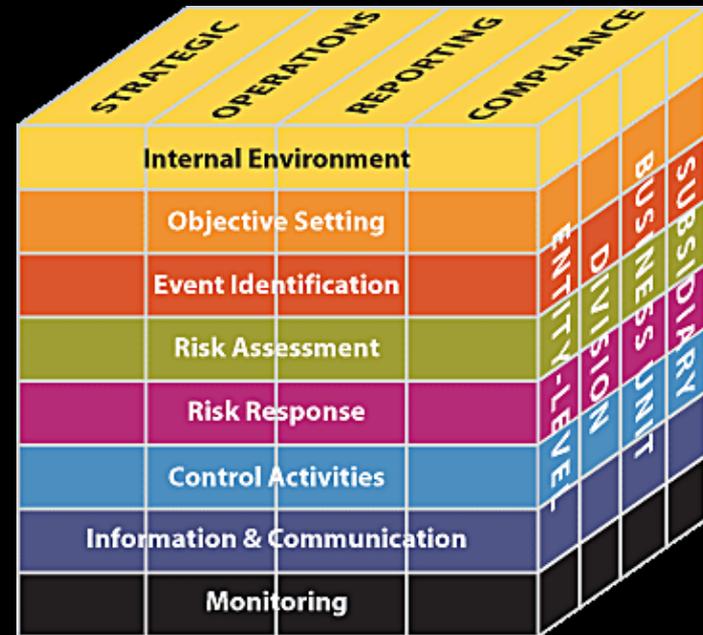
Management

- CEO ultimate responsibility
- Senior management – manage risks in their “units” within tolerances
- Operating management – accountable to next higher level for his/her portion of risk management
- Other Personnel

The ERM Framework

ERM considers activities at all levels of the organization (COSO):

- Enterprise-level
- Division or subsidiary
- Business unit processes



The ERM Framework

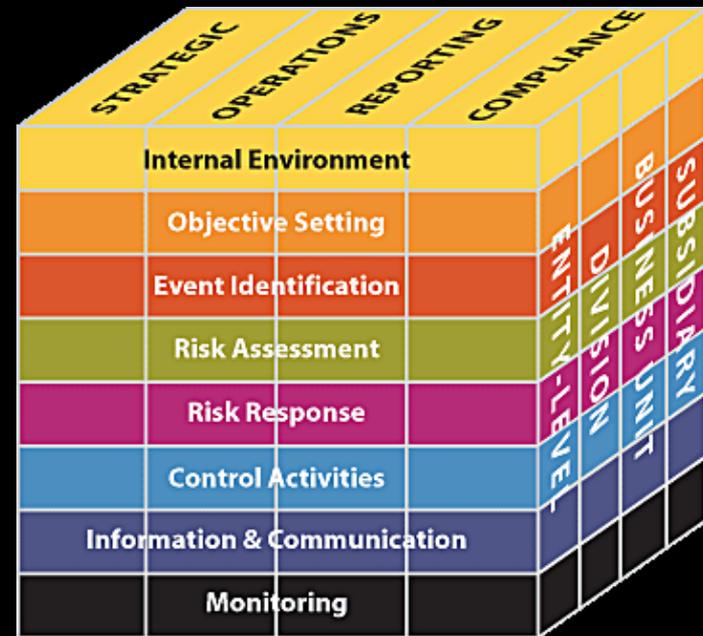
Enterprise risk management
requires an entity to take a *portfolio view*
of risk.

The ERM Framework

- Management considers how individual risks interrelate.
- Management develops a portfolio view from two perspectives:
 - Business unit level
 - Entity level

The ERM Framework

The eight components
of the framework
are interrelated ...



Linking Vision/Mission/Objectives

Vision	To be the leading and most trusted provider of _____.
	To provide high-quality, accessible and affordable _____.
Strategic Objectives	<ul style="list-style-type: none"> • Market share growth of ____% • Annual rate of return of ____% • Service quality rank
Strategies	<ul style="list-style-type: none"> • Acquisitions in target markets • Eliminate low-performing locations and exit low-return markets • Improve infrastructure and control costs
Operations Objectives	<ul style="list-style-type: none"> • Hold focus group discussions in existing/new target markets • Upgrade IT and Human Resource capacity and capabilities • Implement quick start-up and shut-down methodologies
Reporting Objectives	<ul style="list-style-type: none"> • Improve “key performance indicator” monitoring information • Ensure that reports from all locations are timely and accurate
Compliance Objectives	<ul style="list-style-type: none"> • Initiate exit strategy dialogues in low-performing locations/market • Establish a compliance office and monitor compliance with key laws and regulations

Risk Management Process and “Essential Practices

Risk Identification/Assessment Methodology

- Common Language
- Event Inventories and Categories
- Rating Scales and Criteria
- Risk Management Training Activities

Risk/Control Assessment Documents (Matrix, Template...)

- Objectives, Risk Events/Causes, Controls/Responses
- Control/Response Owners
- Risk/Control Self-Assessment Workshops

Risk Management Process and “Essential Practices”

Risk/Control “Owner” Ongoing Monitoring & Periodic Reporting

CRO “Aggregation” Activities

- “Quality” and “Interdependency” Reviews
- Key Risk Indicators/Escalation Triggers

Senior Management (“Champions”) Risk Council Activities

- Dashboard/Heat Map/Risk Register Reporting
- Risk Response Decisions

CRO Reporting to the Board/or Audit Committee

Internal Audit Assurance Reviews

Formulating/Expressing Internal Audit “Opinions”

When an overall opinion is issued

- It must take into account the expectations of senior management;
- The board, and other stakeholders; and
- Must be supported by sufficient, reliable, and useful information.

Formulating/Expressing Internal Audit “Opinions”

- **Interpretation:**
 - The communication will identify:
 - The scope, including the time period to which the opinion pertains;
 - Scope limitations;
 - Consideration of all related projects including the reliance on other assurance providers;
 - The risk or control framework or other criteria used as a basis for the overall opinion; and
 - The overall opinion, judgment, or conclusion reached.
 - The reasons for an unfavorable overall opinion must be stated.

IA Assurance & Consulting Strategy Challenges

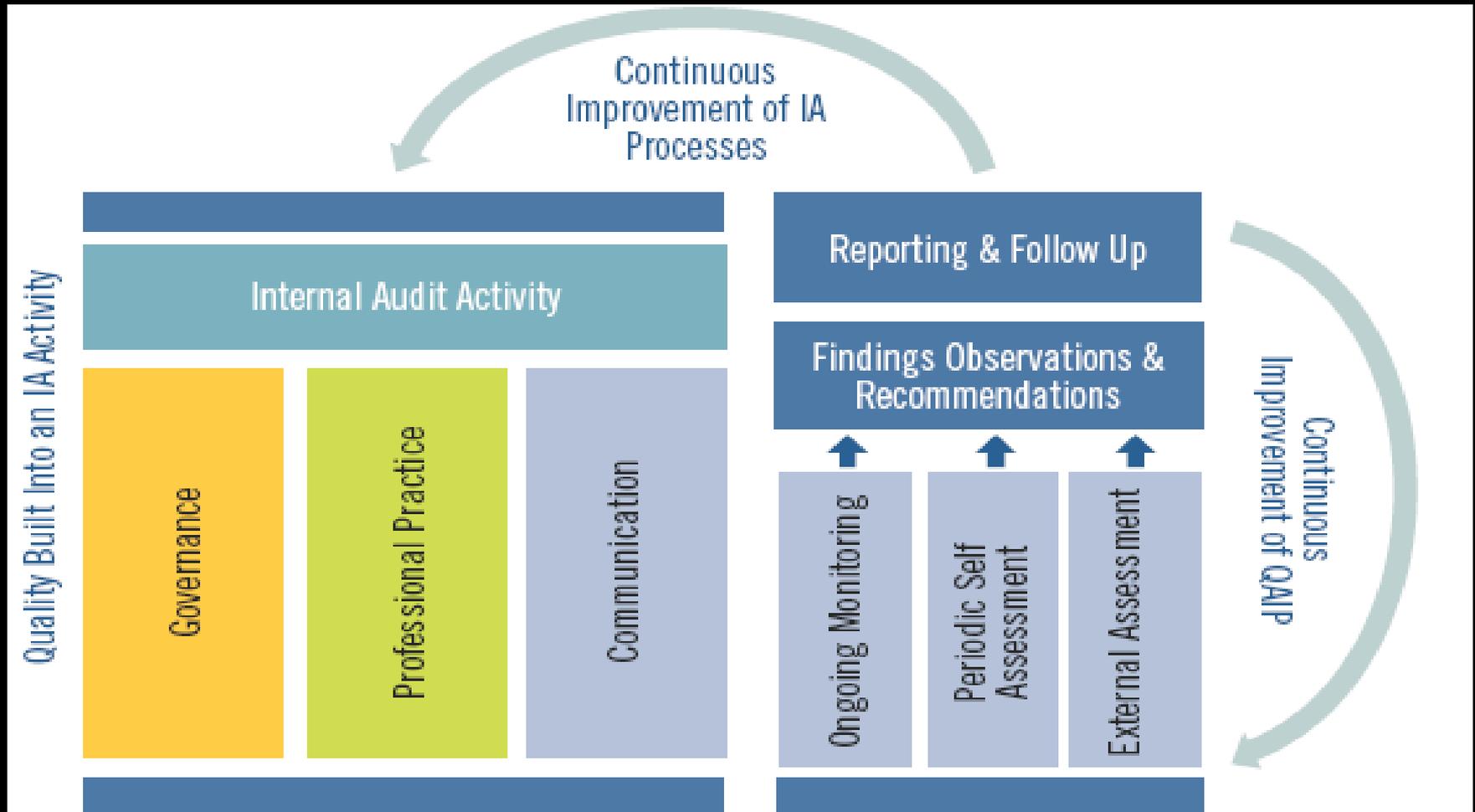
Common Challenges

- IA Staff “Competency” Challenges
- Technical (Hard skills)
- Behavioral (Soft skills)
- Areas of Knowledge (Subject matter expertise)

Other Challenges

- Band width or resource constraints
- Cultural factors
- What are your strategies/tactics for dealing with the challenges?

Conclusion



Conclusion

- Risk management seeks to identify and ultimately control possible future events;
- Should be proactive rather than reactive;
- To be effective, risk management must rely on tools and techniques;
- Help predict the likelihood of future events;
- The effects (Impact) of these future events;
- Methods to deal with these future events; and
- Risk management should really be considered the responsibility of everyone involved.

Thank You

Questions ??

