Enterprise Risk Management:
Achieving and Sustaining Success

Paul J. Sobel and Kurt F. Reding

February 7, 2013

The Institute of Internal Auditors | Georgia-Pacific | Wichita State University

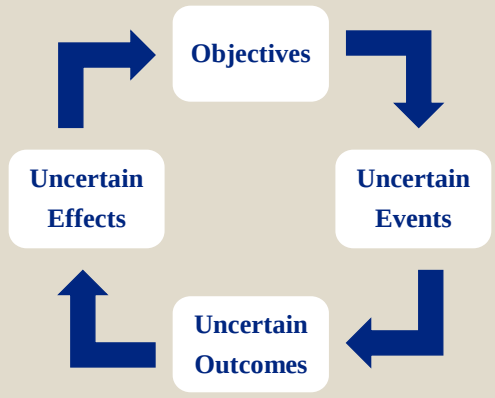
Seminar Outline

- Foundational ERM concepts.
- Achieving ERM success.
  - Getting started.
  - Determining risk criteria.
  - Assessing risks.
  - Treating risks.
  - Monitoring the ERM system.
  - Reporting on risks.
- Sustaining ERM success.

The Foundation

Risk

Risk is the aggregate effect of uncertain events and outcomes on the achievement of objectives.



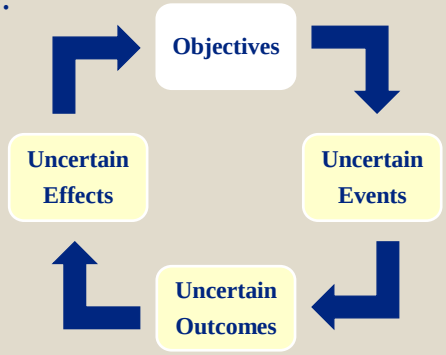
Objectives

- Business objectives:
  - Encompass the organization's vision and mission.
  - Reflect the organization's values.
- Performance objectives:
  - Strategic.
  - Operations.
  - Reporting.
  - Compliance.

Case Scenario: How Much "Moore" Is Enough? Part 1

Uncertainty

- Risks are fraught with uncertainty due largely to their prospective nature.
- Each facet of risk – events, outcomes, and effects – involves uncertainty.



Events

- An event is a happening.
  - Events occur inside and outside the organization.
  - They may occur naturally or be manmade.
  - Events include decisions (or non-decisions) and actions (or inactions).
  - An event may have happened already or may happen in the future.
  - Some future events are easier to anticipate than others.
  - Events may happen quickly or slowly.
  - Events may be good or bad.

Events

- Events do not always happen one at a time; nor do they always happen independently.
  - Events often happen in groups and interact with each other.
  - Two or more events may cluster together to form a larger event.
  - Events may cascade like dominos…
  - Bad events may partially offset good events or vice versa.

Outcomes

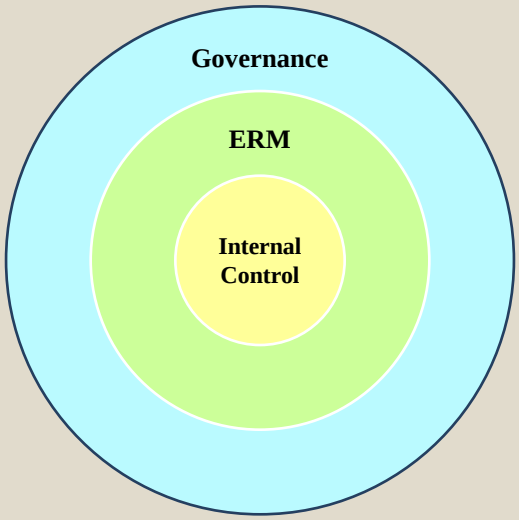
- Outcomes are results of, and contingent upon, events.
  - They may be financial or nonfinancial; tangible or intangible.
  - They may result from a single event or a combination of events.
  - Multiple, interrelated outcomes are common; individual, isolated outcomes are less common.
  - Multiple outcomes may take place simultaneously or in succession.
  - Outcomes may take place immediately or over time.
  - Outcomes may be desirable or undesirable, depending on the events that caused them.

Effects

- Effects are the consequences of outcomes on the achievement of objectives.
  - They may be favorable or unfavorable.
  - Favorable effects involve new value creation.
  - Unfavorable effects involve value destruction, i.e., impairment of new value creation or damage to existing value.

Case Scenario: How Much "Moore" Is Enough? Part 2

Governance, ERM, and Internal Control



Governance, ERM, and Internal Control

- **Governance** – an overarching system implemented by the board to direct and oversee the activities of the organization toward the achievement of its objectives.
- **Enterprise risk management (ERM)** – an integrated, entity-wide system that addresses the organization's portfolio of risks in a manner that creates and protects value and provides assurance that objectives will be achieved.
- **Internal control** – a system employed by management at all levels of the organization to carry out the prescribed risk treatment methods and, accordingly, address the risks that affect the achievement of the organization's objectives.

ERM Principles

- ERM is an integrated, entity-wide system.
- ERM is an integral component of governance.
- ERM is an integral component of management and day-to-day operations.
- ERM addresses the organization's portfolio of risks.
- ERM is a journey, not a destination.
- ERM is not a one-size-fits-all solution.
- ERM creates and protects value.
- Risk implications are considered in every important decision.
- ERM provides assurance that objectives will be achieved.

Internal Audit's Role in ERM

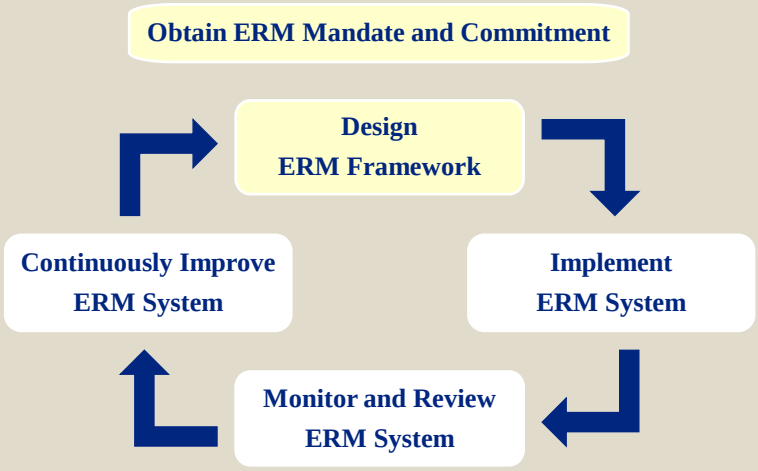
- The core role of internal auditors with regard to ERM is to provide independent and objective assurance to the board regarding the organization's ERM system.
- ERM consulting services provided by internal auditors comprise objective advisory, facilitative, and training activities specifically intended to improve the organization's ERM and internal control systems.

Getting Started

The ERM Framework

The ERM Framework is the organizational construct that enables the design, operation, and improvement of the ERM system.

The ERM Framework



Obtain ERM Mandate and Commitment

- Support from the board and senior management:
  - Define and endorse the risk management policy.
  - Align the organization's culture and risk management policy.
  - Align risk management objectives with the organization's objectives and strategies.
  - Align risk management performance indicators with the organization's performance indicators.
  - Assign accountabilities and responsibilities at appropriate levels.
  - Allocate the necessary resources to risk management.
  - Ensure legal and regulatory compliance.
  - Communicate the benefits of risk management to all stakeholders.
  - Ensure that the risk management framework continues to be appropriate.

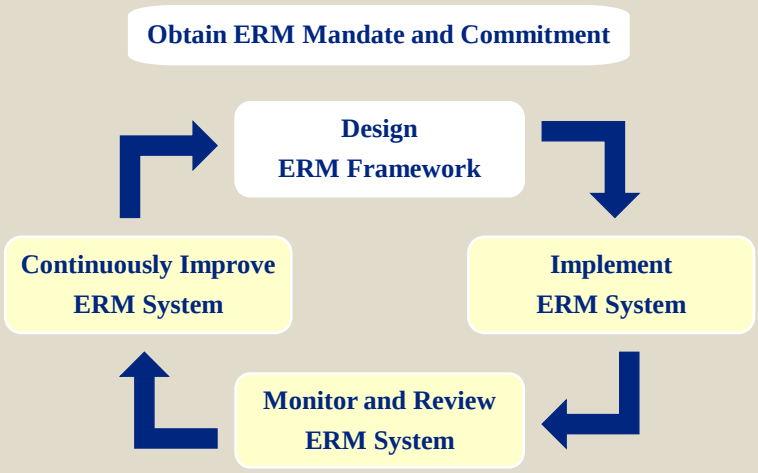
Obtain ERM Mandate and Commitment

- Practical considerations:
  - Why are we choosing to implement ERM at this time?
  - Where do we start?
  - What is our scope for implementation?
  - What outcomes do we expect, i.e., what does success look like?
  - How will we roll out ERM throughout the organization?

Design ERM Framework

- Fundamental components:
  - Understand the organization, its business, and the context for ERM.
  - Determine the organizational positioning of ERM.
  - Develop a risk management policy.
  - Assign accountability and authority.
  - Allocate resources.
  - Establish internal and external reporting mechanisms.
  - Link ERM to the performance appraisal process.

Remaining Steps in the ERM Framework



Internal Audit's Role in Getting Started

- Options to consider, depending on the circumstances:
  - Lead the ERM implementation with safeguards in place that prevent long-term impairment of internal audit's objectivity.
  - Provide consulting (advisory, facilitative, or instructive) in a manner that does not impair internal audit's objectivity.
  - Provide assurance that the implementation is proceeding as planned.

Determining Risk Criteria

What are Risk Criteria?

ISO 31000 defines risk criteria as "terms of reference against which the significance of a risk is evaluated."

- Governance Risk Criteria
- Assessment Risk Criteria

Governance Risk Criteria

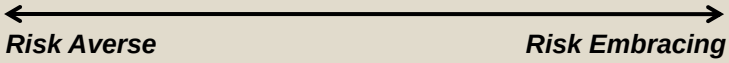
- Governance risk criteria define and support the success and operation of the organization.
  - Help define the direction for risk management.
  - Established by the board and senior management (i.e., top-down).
  - Consider real-life context affecting long-term survival.
    - Mitigation of downside risks
    - Pursuit of upside risks

Risk Capacity

- Organization's total capability to absorb negative outcomes.
- Defines the boundaries for survival.
- Could be individual event outcomes or aggregate outcomes of multiple events.
- Common examples:
  - Inadequate capital
  - Inadequate cash flow
  - Violations of laws and regulation
  - Damage to reputation

Risk Attitude

- *An organization's propensity to take on risk, which can be thought of along a spectrum:*



- Blends elements of COSO's and ISO's definitions:
  - Risk Management Philosophy (COSO) – "Set of shared beliefs and attitudes characterizing how the entity considers risk in everything it does, from strategy development and implementation to its day-to-day activities."
  - Risk Attitude (ISO 31000) – "Organization's approach to assess and eventually pursue, retain, take or turn away from risk."

Risk Appetite

- *Type and total amount of risk an organization is willing to take on in pursuit of its business objectives.*
- This also blends elements of COSO's and ISO's definitions:
  - COSO – "Amount of risk, on a broad level, an entity is willing to accept in pursuit of value."
  - ISO 31000 – "Amount and type of risk that an organization is willing to pursue or retain."

Risk Appetite

- Established as part of strategic planning by the governance process (Board/Senior Management).
- Reflected in statements that can be communicated.
- May be described quantitatively (amount) or qualitatively (type).
- May reflect desire to pursue positive outcomes or minimize negative outcomes.
- Must consider the organization's capacity to take on risk.
- Influenced by the organization's risk attitude.
- While appetite won't change often, changes in internal or external context may necessitate changes in appetite as well.
- Ultimately, it's about balancing success and survival.

Risk Appetite Examples

- We will put no more than 50% of our capital at risk.
- We will seek new markets for our products, but only operate in countries with a Global Integrity Index of "moderate" or higher.
- We will only use derivatives to hedge fuel positions to manage operating results; not to speculate.
- We will not build key manufacturing plants in areas prone to earthquakes or floods.
- We will maintain a debt/equity ratio of 1.5 or less.
- We will invest at least 10% of our revenues in R&D.

Risk Tolerance

- *Risk taking boundaries within which managers and employees are expected to perform in pursuit of the organization's strategic, operations, reporting and compliance objectives.*
- This also blends elements of COSO's and ISO's definitions:
  - COSO – "Acceptable level of variation relative to achievement of a specific objective, and often is best measured in the same units as those used to measure the related objective."
  - ISO 31000 – "Organization's or stakeholder's readiness to bear the risk after risk treatment in order to achieve its objectives."

Risk Tolerance

- Established as part of the risk management process, but subject to governance process.
- Influenced by the organization's risk attitude, but may vary somewhat between objectives.
- Aligns with risk appetite, but focused on short to medium-term performance.
- Relates to individual business objectives.
- Must consider from both an individual and aggregate (portfolio) perspective.
- May have a floor, ceiling or both.
- Measures performance and guides resource allocation.
- Considers cost/benefit of risk treatment strategies.

Risk Tolerance

- Boundaries are expressed as the ceiling and/or floor related to key risk outcomes and effects, for example:
  - Financial results (current or future)
  - Reputation (real or perceived damage)
  - Health & safety (injuries, lost time)
  - Environmental (exceedences, spills, remediation costs)
  - Compliance (fines, penalties, sanctions)
  - Customer satisfaction (ratings, market share)
  - Warranty defects (liability, cost to repair)

Risk Tolerance Examples

- Annual operating results should not be less than 90% of budget.
- We expect 15-30% of our operating earnings to be derived from non-U.S. sources.
- Our environmental and safety performance should place us in the top quartile of our industry.
- Our customer satisfaction rating should be > 95%.
- We should not have warranty claims on more than 3% of products sold.
- We will target an average rate of return on cash reserves above the Government bond rate.

Case Scenario: How Much "Moore" Is Enough? Part 3

Assessment Risk Criteria

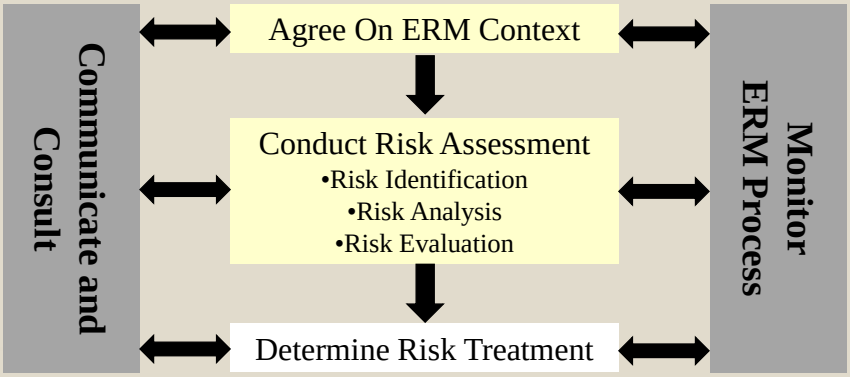
- Criteria against which individual risks will be assessed.
- Most common risk assessment criteria are impact and likelihood.
- Other criteria may influence the final prioritization of risks:
  - Inherent criteria, such as velocity, volatility and interdependence.
  - Capability criteria, such as readiness, agility, resilience, monitorability, maturity or degree of confidence.

Internal Audit's Role in Determining Risk Criteria

- Educate management on different criteria.
  - Governance Criteria
  - Assessment Criteria
- Facilitate determination and articulation of governance risk criteria.
- Facilitate consideration of risk assessment criteria (covered in next section).

Assessing Risks

The ERM Process



Agree on ERM Context

- External and internal parameters that may affect decisions round risk management.
  - External context –
    - Social and cultural, political, legal regulatory, financial, technological, economic, natural and competition.
    - Key drivers and trends affecting objectives.
    - Relationships with, and perceptions and values of, external stakeholders.
  - Internal context –
    - Governance, org structure, roles and responsibilities.
    - Policies, objectives, strategies, standards and guidelines.
    - Capabilities, in terms of resources and knowledge.
    - Information systems, information flows and decision-making processes.
    - Culture and relationships with internal stakeholders.
- Risk criteria that guide the ERM process.

Risk Assessment

- **Risk identification** – process of finding, recognizing and describing risks.
- **Risk analysis** – process to comprehend the nature of risk and determine its level.
- **Risk evaluation** – process of comparing risk analysis results with risk criteria and determining whether the residual risk is acceptable.

Risk Identification

- Identify risk events
  - Research possible events.
  - Brainstorm possible scenarios.
  - Determine outcomes from events.
- Develop risk universe
  - Group events with similar causes, sources or outcomes.
  - Determine the "theme" of grouped events and define the risk based on that theme.
  - Create a risk model to organize the universe.

Example Risk Model

Strategic/ Governance Risks	Market/ External Risks	Operations Risks
Risk A	Risk D	Risk G
Risk B	Risk E	Risk H
Risk C	Risk F	Risk I
Financial Risks	**Reporting Risks**	**Compliance Risks**
Risk J	Risk M	Risk P
Risk K	Risk N	Risk Q
Risk L	Risk O	Risk R

Risk Analysis

- Causes –
  - What gives rise to the risk event?
  - How do the outcomes occur?
- Sources –
  - Where does the risk arise?
- Interdependencies –
  - Will this risk cause another risk to occur?
  - Does the occurrence of another risk cause this risk to occur?

Risk Analysis

- It's important to remember that:
  - Risk events can have multiple outcomes and affect multiple objectives.
  - Risks exist in inherent and residual states.
  - Criteria beyond impact and likelihood should be considered.
  - Risk analysis can be done with varying levels of confidence and precision.
  - The outcomes of events may be expressed quantitatively, qualitatively or some combination of both.

Risk Evaluation

- Assess the Risk Universe
  - Impact and Likelihood
  - Other Risk Assessment Criteria
- Prioritize Risks
- Consider Upside Risks

Risk Assessment

- Impact – Measure of the size of potential risk outcomes.
  - Financial
  - Financial reporting
  - Reputation
  - Environmental
  - Safety
  - Legal
  - Other

Impact Example

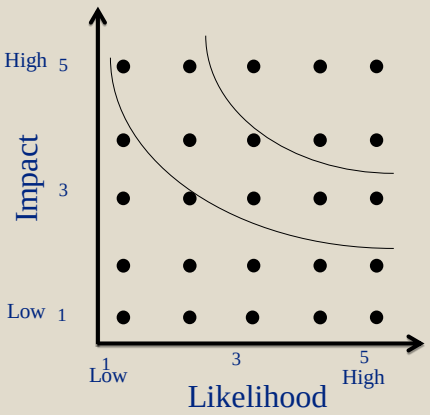
Level	Financial	Reputation	Safety
Catastrophic	Exceeds the risk capacity of $1 billion	Irreparable damage that threatens the organization's viability	Fatality(ies) of employees, visitors, or innocent people in the community
Major	Exceeds the risk appetite of $50 million	Significant damage that makes it difficult to achieve one or more business objectives	Life threatening injuries to employees, visitors, or innocent people in the community
Moderate	$10–50 million	Damage that makes it challenging to achieve at least one objective in the short term	Physical harm that may cause extended absence from the workplace
Minor	$1–10 million	Modest damage that requires some expenditure of resources to remediate	Physical harm that may cause short-term absence from the workplace
Insignificant	Less than $1 million	No noticeable impact	Minor injuries that result in no lost time

Risk Assessment

- Likelihood – The likelihood of that impact occurring.
  - What is the time horizon for the assessment?
  - Does the assessment focus on probability of a single occurrence or frequency of occurrence?
  - Should likelihood consider the impact of controls or other activities that are known to operate (e.g., inherent or residual level of risk)?

Low	Moderately Low	Moderate	Moderately High	High
0–20%	21–40%	41–60%	61–80%	81–100%

Level of Risk



Prioritize Risks

- First, consider impact and likelihood (level of risk).
  - Check those close to "borders"
  - Consider management's tolerance levels
- Evaluate whether other risk assessment criteria would cause a change in priorities.
- Determine risk profile (those risks from the universe that the organization should formally treat).

Other Risk Criteria Example

Risk	Impact	Likelihood	Factor A	Factor B	Priority
AAA	High	High			1
BBB	High	Medium			2
CCC	Medium	High			3
DDD	High	Low			4
EEE	Medium	Medium			5
FFF	Low	High			6
GGG	Medium	Low			7
HHH	Low	Medium			8
III	Low	Low			9

Other Risk Criteria Example

Risk	Impact	Likelihood	Factor A	Factor B	Priority
AAA	High	High	↑		1
BBB	High	Medium			3
CCC	Medium	High	↓		5
DDD	High	Low		↑	2
EEE	Medium	Medium	↑		4
FFF	Low	High			6
GGG	Medium	Low		↓	8
HHH	Low	Medium	↑		7
III	Low	Low		↓	9

Consider Upside Risks

- Determine actions or initiatives necessary to achieve objectives / create value; should also consider the barriers to success (risk identification).
- Identify the possible outcomes from those actions or initiatives, and their sources and interdependencies (risk analysis).
- Determine desired impacts and likelihood of those impacts occurring, and whether those will achieve the objectives (risk evaluation).
- Understand how the organization's risk attitude and risk appetite may impact these actions and initiatives (risk criteria).

Case Scenario: How Much "Moore" Is Enough? Part 4

Internal Audit's Role in Risk Assessment

- Document and communicate the ERM context.
- Facilitate risk universe development.
- Assist in risk analysis.
- Facilitate the risk evaluation.
  - Determination of impact and likelihood scales.
  - Assessment of risk impact and likelihood.
  - Prioritization based on levels of risk.
  - Consideration and evaluation of other risk assessment criteria.
  - Consideration of how risk appetite and risk tolerance may justify changes in levels of risk.

Treating Risks

Risk Treatment

- The risk portfolio – the outcome of risk assessment – is the input for risk treatment.
- Risk treatment – "a process to modify risk" (ISO 31000)
- Management must decide:
  - Which risks warrant the allocation of treatment resources.
  - How risk treatment resources will be deployed.

Risk Treatment Options

- **Avoid** – Decide not to start or continue the activity that gives rise to the risk, or remove the source of the risk.
  - Appropriate when it is not possible to reduce the risk to a tolerable level, or the cost of doing so is prohibitive.
- **Mitigate** – Reduce the level of risk.
  - Appropriate when the cost of implementing controls or taking other actions to reduce the risk is less than the expected reduction in risk exposure.

Risk Treatment Options

- **Share** – Portion the management of the risk with one or more outside parties.
  - Appropriate when the cost of partnering with others to treat the risk effectively is less than the cost of treating the risk effectively in-house.
- **Accept** – Retain the risk at its current level.
  - Appropriate when the current level of risk is tolerable.

Risk Treatment Options

- **Exploit** – Take or increase risk to pursue an opportunity.
  - Appropriate when the organization must take on more risk to obtain desired outcomes and achieve its strategic objectives.

Develop a Risk Treatment Plan

- Select a treatment approach.
  - Evaluate the costs and benefits of different treatment options for each risk.
  - Focus the treatment options on the risk sources to treat the root causes.
  - Ensure that the treatment options address the range of possible outcomes, not just a single point estimate.

Develop a Risk Treatment Plan

- Construct an integrated treatment plan.
  - Understand the risk interdependencies that were identified in the risk analysis phase of risk assessment.
  - Consider treatment options that can address multiple risks.
  - Incorporate activities that are already part of day-to-day management.

Develop a Risk Treatment Plan

- Assign accountability.
  - Designate treatment owners and clearly define their responsibilities.
  - Provide treatment owners the resources they need to successfully fulfill their responsibilities.
  - Establish and communicate performance expectations and reporting requirements.

Develop a Risk Treatment Plan

- Establish a monitoring approach.
  - Determine that the risk treatments employed are operating effectively.
  - Periodically assess the overall risk treatment plan.

Case Scenario: How Much "Moore" Is Enough? Part 5

Internal Audit's Role in Risk Treatment

- Help management research and analyze risk treatment options, including their costs.
- Provide advice pertaining to risk sources and causes to help management evaluate the appropriateness of chosen risk treatments.
- Provide assurance that the integrated risk treatment plan is comprehensively communicated and understood.
- Provide assurance regarding the overall effectiveness of monitoring activities.

Monitoring the ERM System

ERM Monitoring

ERM monitoring is the assessment of the organization's context, ERM system, and business performance over time.

Why ERM Monitoring is Important

- ERM monitoring:
  - Provides assurance that the ERM system continues to operate effectively over time, i.e., that deficiencies in design adequacy or operating effectiveness are identified and rectified timely.
  - Facilitates timely identification of changes in the organization's external and internal context, performance objectives, strategies, and risks.
  - Expedites appropriate ERM alterations in response to changes identified.
  - Provides assurance that the organization's strategic, operations, reporting, and compliance objectives continue to be achieved.

What is Monitored

- Monitoring the organization's context:
  - The context is where risks originate; changes in the context may cause new risks to surface or existing risks to increase or decrease.
  - Changes in the context may prompt management and the board to make changes in the organization's performance objectives and strategies.
  - As the organization's performance objective and strategies change, its risks will change.
  - Therefore, the external and internal context must be monitored to ensure that changes that may affect the risk portfolio and ERM system are identified timely.

What is Monitored

- Monitoring the ERM system:
  - Monitoring is imbedded in both the process component and framework component of ERM.
    - Each step in the ERM process, and the specific elements of each step, must be monitored.
    - Each key element of the ERM framework must be monitored.
  - In addition, it is important to periodically take a step back and assess the entire system from a big-picture perspective.

What is Monitored

- Monitoring the organization's business performance:
  - Improved business performance is an expected outcome of an effective ERM system.
  - Therefore, monitoring the organization's business performance provides evidence regarding the performance of the ERM system.

What is Monitored

- Monitoring throughout the organization:
  - The ERM system operates in all functional areas and at all levels – entity level, business unit level, process level, and transaction level – of the organization.
  - Each segment of the organization is affected by its own external and internal context.
  - The ERM system for each segment affects both the performance of that segment and the performance of the organization as a whole.
  - Accordingly, ERM monitoring must occur in all functional areas and at all levels of the organization.

How Monitoring is Performed

- Integrated assessments:
  - Are imbedded among the risk management activities being monitored.
  - Are most effective when conducted as soon as possible after the risk management activities occur.
  - Vary in terms of specificity.
- Separate assessments:
  - Are detached from the business activities being monitored.
  - Complement integrated assessments.
  - Vary in terms of specificity.

How Monitoring is Performed

- ERM monitoring procedures are used to:
  - Track developments in the external and internal context that may foretell risk events that pose threats to the organization.
  - Provide direct feedback about the effectiveness of the ERM system.
  - Provide direct feedback about business performance, which in turn provides indirect feedback about ERM system performance.

Who Monitors

- ERM monitoring includes:
  - Self-assessments (least impartial).
  - Peer assessments.
  - Supervisory assessments.
  - Objective assessments (most impartial).

Who Monitors

- The board's role:
  - As the owner of the governance system, the board oversees senior management's risk management activities, including its ERM monitoring activities, in a supervisory capacity.
- Management's role:
  - As the owner of the ERM system, senior management has primary responsibility for monitoring the system. Its monitoring responsibilities include supervisory assessments, peer assessments, and self-assessments.

Who Monitors

- Process owners' and employees' roles:
  - Process owners' and employees' monitoring responsibilities include supervisory assessments, peer assessments, and self-assessments.
- Independent parties' roles:
  - In many organizations, functions other than internal audit provide separate, objective monitoring assessments. Such functions include, for example:
    - Quality assurance.
    - Corporate responsibility.
    - Corporate security.
    - Health and safety.

Case Scenario: How Much "Moore" Is Enough? Part 6

Internal Audit's Role in ERM Monitoring

- Internal auditors perform separate, objective ERM monitoring assessments in their everyday role as assurance providers.
- The impartiality of internal audit's ERM monitoring assessments is what distinguishes these assessments from the supervisory, peer, and self-assessment monitoring procedures performed by management.
- The most effective way to ensure impartiality is to position internal audit's role in ERM monitoring as one of governance.

Internal Audit's Role in ERM Monitoring

- "Organizational independence is effectively achieved when the chief audit executive reports functionally to the board." (IIA Standard 1110)
- The internal audit activity must also be objective.
  - Any direct involvement in ERM decision-making or participation in ERM activities will impair internal audit's capacity to remain objective as they monitor ERM.
  - To maximize their value as impartial ERM evaluators, Internal auditors must be as far removed from day-to-day ERM decision-making and activities as possible.

Reporting on Risks

Types of Reporting

- Reporting to the Board
- Other Internal Reporting
- External Reporting

Reporting to the Board

- Board must be able to evaluate how successfully management is:
  - Operating within established governance risk criteria.
  - Identifying, analyzing and evaluating existing and emerging risks.
  - Treating risks in pursuit of upside opportunities and mitigation of downside exposure, within tolerance levels.
  - Conducting monitoring activities, adjusting risk treatments and evaluating the overall ERM system.
- Board should establish a reporting/escalation protocol.
  - Immediate communications
  - Periodic written communications
  - Periodic presentations

Other Internal Reporting

- Status Reporting
  - Updates and changes in the organization's context.
  - Effectiveness of the ERM system.
  - The organization's business performance.
- Risk Event Escalation
  - Escalation protocol
  - Authority to act during a risk event

External Reporting

- Due to regulatory requirements:
  - In securities filings (e.g., key risk factors).
  - To regulatory agencies (required filings or in response to an event, such as a toxic spill).
  - In response to requests from credit rating agencies.
- Voluntary disclosures:
  - Reports on corporate social responsibility.
  - Press releases or postings on website to manage public perception.

Internal Audit's Role in Reporting on Risks

- Assurance to management re: the accuracy and timeliness of key risk reports.
- Assurance to the Board re: the completeness and accuracy of key risk management information.
- Assurance that those receiving key risk management reports are taking appropriate actions.
- Assurance on the accuracy, relevance and timeliness of reports to external parties.
- Advice on sources of data to monitor changes in the organization's external context.
- Advice on processes and systems that provide reports.

Sustaining ERM Success

Sustaining ERM Success

- Embedding ERM in the internal audit plan.
- Embedding ERM in the internal audit methodology.
- Assessing the ERM system.

Embedding ERM in the Audit Plan

- Develop an audit plan that's ERM-based.
  - Ensure internal audit's risk assessment is the same as, or linked to, the organization's risk portfolio and assessment.
  - Include key components of ERM in the audit universe.
- Provide assurance and consulting services.
  - Assurance reports reference enterprise risks and risk management activities.
  - Consulting services improve ERM.
- Coordinate other assurance and consulting activities.
- Document internal audit's ERM responsibilities.
- Involve internal audit in strategic planning.

Embedding ERM in the Methodology

- Primary outcomes of ERM-based auditing are to:
  - Assess design adequacy and operating effectiveness of risk treatments for the risks applicable to the area under review.
  - Validate the reasonableness of the overall residual risk assessment for applicable risks.
- Plan audits around relevant objectives, risks, treatments, tolerance levels and monitoring.
- Conduct audits to provide support for an assessment of applicable risk management activities.
- Communicate results so that recipients understand the assessment in terms of risk management effectiveness.

Assessing the ERM System

- To be successful, organizations must find ways to:
  - Create new value
  - Protect existing value
- This requires good strategic planning and managing the risks to the strategic plan.
  - Intelligently take on risks that create value and enable success
  - Mitigate risks that can destroy value and inhibit success
- Effective risk management helps an organization achieve and sustain success!
- Therefore, assurance helps enable sustained success.

What Types of Assurance?

- Designed Adequately
  - Aligned with organization's objectives
  - Consistent with ERM objectives
  - Aligned with risk criteria (i.e., capacity, attitude, appetite and tolerance levels)
  - Relevant to the organization's external and internal context
- Operating Effectively
  - Operating as designed
  - Sustainable

What Types of Assurance?

- ERM system as a whole
  - Shortly after implementation
  - As the system matures
- Components of the ERM system
- ERM within a discreet business area
- Reaction to a risk event

How to Provide Assurance?

- Comprehensive Assessment Approach
- Maturity Assessment Approach

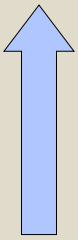
Comprehensive Assessment

- Evaluates all aspects of the ERM system.
- Assess whether sound (not leading) practices are operating in all key areas.
- Involves answering a series of questions related to all key areas.
- Organized around ISO 31000:2009(E), but could mirror COSO ERM or other approach.

Maturity Assessment

- Effectiveness is not necessarily binary – you don't magically go from ineffective to effective.
- Not all areas need to be mature – it's a cost/ benefit decision.
- Focus should be on closing largest gaps between current and desired state.
  - Management determines desired state, with board input.

ERM Maturity Stages



Value Creation Stage	
Maturity Stages	***Innovative Level***
	Proficient Level
	Foundational Level
Implementation Stage	

ERM Maturity Criteria

- ERM Mandate and Commitment
- Framework Design
- Risk Criteria
- Risk Assessment
- Risk Treatment
- Risk Monitoring and Reporting

Summary

- Achieving ERM success is an evolution, not a revolution.
  - ISO 31000 provides a roadmap for achieving success, but it's a long road.
  - Every organization must customize the path to fit their own needs and culture.
  - Internal audit can have a role every step of the way.
- Internal audit also plays a key role in helping to sustain success.
  - Embed ERM concepts into the audit plan and methodology.
  - Periodically assess the ERM system.

Questions?

paul.sobel@gapac.com
kurt.reding@wichita.edu