Enterprise Risk Management Leads to Strategic Alignment and Value Creation

Presented by: Alyssa Martin, Risk Advisory Services

Alyssa G. Martin, CPA

Risk Advisory Partner with 25 years of experience. Practice emphasis in the areas of risk management, internal audit, IT audit, business management consulting, strategic planning, and technology consulting.

- Member of the Executive Advisory Committee of the Accounting and Information Management Area of the University of Texas at Dallas' School of Management
- Chair of the Baker Tilley International Corporate Governance and Risk Management Committee
- Frequent author on Risk Management, Internal Audit, IT and Governance topics

1

Agenda

- **ERM Basics:**
  - Defining Enterprise Risk Management
- **Approach and Methodology:**
  - Putting Theory into Practice
- **Steps to Accomplish ERM:**
  - How to Implement ERM in Your Organization
- **ERM as an Ongoing Process:**
  - Document Results and Plan for Ongoing Progress

2

ERM Basics

Defining and differentiating ERM from other risk management approaches

3

Audience Question

- ***Have you completed a Risk Assessment?***
- ***Have you embarked on Enterprise Risk Management?***

4

What is Risk?

- The IIA defines risk as the possibility of an event occurring that will have an impact on the achievement of an organization's objectives.
  - Risk is measured in terms of probability and impact
- ISO 31000 defines risk as "the effect of uncertainty on objectives."

5

Defining Risk Management

COSO-ERM and the ISO define Risk Management in the following ways:

COSO-ERM Framework:	ISO 31000:
"Enterprise Risk Management is a structured and coordinated entity wide governance approach to **identify**, *quantify*, **respond** to, and *monitor* the consequences of potential events. Implemented by Management"	The Risk Management Process is a "systematic application of" "policies, procedures and practices" for "communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, monitoring and reviewing risk"

We combine the best of both definitions into one Risk Management strategy

6

Defining Enterprise Risk Management

- Enterprise Risk Management (ERM) is:
  - A process
  - Effected by people
  - Applied in strategy setting
  - Applied across the enterprise
  - Designed to identify potential events (both positive and negative)
  - Manages risk within risk appetite
  - Provides "reasonable assurance"
  - Supports the achievement of key objectives

7

Defining Risk Management

Risk Management is not the same as Risk Assessment:

- Risk Assessment: The process of identifying and evaluating individual risks for the purpose of determining risk responses
- Risk Management: A comprehensive set of risk management activities that includes Risk Assessment and incorporates all components of the COSO Framework

Effective, Strategic Risk Management:

- Focuses on value creation and linking risks to business strategy
- Embeds risk management in business processes in order to systematically ensure that processes are designed to achieve strategic objectives
- Identifies positive events (opportunities) upon which to capitalize, in addition to identifying risks

8

Did you know?

- According to a recent study:
  - 91% of companies surveyed plan to reorganize their approach to risk management over the next three years
  - Why?
    - Increased volatility across 11 risk areas surveyed which included:
      - Strategic risk
      - Reputational risk
      - Operational risk

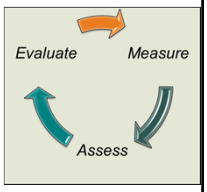
Source: Deloitte, "Aftershock: Adjusting to the New World of Risk Management"

9

Defining Risk Management

Enterprise Risk Management incorporates a broad spectrum of considerations:

- Financial and nonfinancial indicators
  - Intangible assets, like your "brand"
- Enhancing business strategy
- External influences
- Opportunities in addition to risks
- Operational management



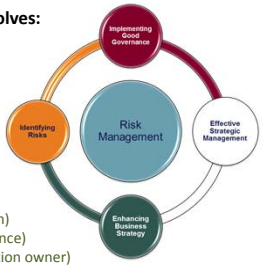
10

Risk Management

Effective Risk Management also involves:

- Implementing Good Governance
- Identifying Risks
- Effective Strategic Management
- Enhancing Business Strategy

- ERM seeks to answer
  - Why (root cause risk)
  - What (risk identification description)
  - Where "we need to be" (risk tolerance)
  - Who (risk owner and mitigation action owner)



11

Differentiating ERM from Compliance

Compliance plays an important role in the Public Sector
ERM is designed to support achievement of objectives

Compliance is merely one of the types of objectives ERM is designed to achieve

Foundation Layer

- **Compliance**
  - Compliance with contracts, laws, regulations
- **Reporting**
  - Reliability of internal and external information reporting
- **Operations**
  - Efficient use of resources
  - Operational effectiveness, performance
- **Strategic**
  - High level value creation choices
  - Support overall mission

12

Why ERM?

ERM necessitates *proactive* identification of risk.

Waiting until a risk becomes a hot button issue can create other risks (i.e., reputational risk), and promotes a reactionary culture.

Proactive identification of risk empowers management to make sound decisions in the strategy-setting phase, prior to implementation. Thus, risk consciousness is baked in to the strategic plan.

13

Anatomy and Lifecycle of a Risk Event

*ERM seeks to identify and address risks **here**...*

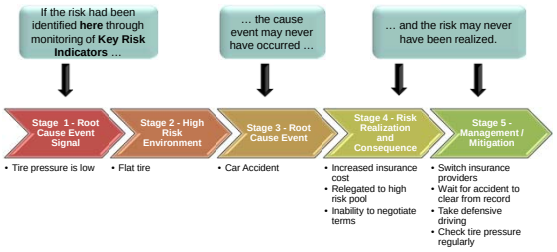
*... instead after they have impacted the company of reacting to risk events **here***

Stage 1 - Root Cause Event Signal	Stage 2 - High Risk Environment	Stage 3 - Root Cause Event	Stage 4 - Risk Realization and Consequence	Stage 5 - Management / Mitigation

• Factors/signals are present that create a high risk environment.
• Can be identified through monitoring of Key Risk Indicators (discussed in Monitoring section).
	• A high risk environment has resulted from the signals identified in Stage 1. High potential for root cause event.	• An event occurs that creates potential for significant risks to be realized.	• A significant risk event occurs, impacting the company.
			• A snowball effect can occur, causing risks to multiply at this stage:
			  • *Reputation risk*
			  • *Fraud risk*
				• Management evaluates outcome and establishes mitigation strategy to avoid future risk.

14

Anatomy and Lifecycle of a Risk Event



15

Theory into Practice: Xerium Technologies

- Senior Executives thought ERM was a compliance exercise like SOX
- Senior Leadership acted reactionary to risk, **putting out fires!**
  - Nobody spent the time to look ahead and get above the curve
- In the initial phases of ERM
  - The CEO, VP of Audit, and CFO sat down and ironed out their top 15 risks
  - After a meeting with the board about 6 more were added
- The ERM process helped the company navigate through bankruptcy
  - What the company wanted to avoid
  - What were some things they wanted out of bankruptcy
  - What did they not want to lose
  - What did they want to maintain? **CUSTOMERS, SHAREHOLDERS….**
- Now the process has evolved through an online Questionnaire directed at various levels of management
- Success of the program relied on getting all risk owners involved

Source: NCSU interview with Fred Caloggero, VP Audit Services of Xerium

16

Approach and Methodology

Putting Theory into Practice

17

Focus on the "Right Risks"

An effective approach to implementing ERM would:

- Start with identification of top critical risks facing the organization
- Refocus decision making on key strategic risks
- Deploy the internal audit plan toward the "right risks"

18

Top Risks on Horizon for 2013

Rank	Risk Issue	
1	Regulatory changes and heightened regulatory scrutiny.	Strategic Risk
2	Economic conditions of the market.	Economic Risk
3	Uncertainty of political leadership in national and international markets.	Economic Risk
4	Organic growth through customer acquisition and/or enhancements.	Strategic Risk
5	Succession challenges and the ability to attract and retain top talent.	Operational Risk
6	Anticipated volatility in global financial markets and currencies.	Economic Risk
7	Cyber threats and the potential of significant disruption to core operations.	Operational Risk
8	Ensuring privacy and information security will require significant resources.	Operational Risk
9	Resistance to change will restrict necessary changes by organizations.	Operational Risk
10	Existing operations may not be able to meet performance expectations.	Operational Risk

Source: UNC Poole College of Management

19

The Key Is Focusing On Strategic Risks To Achieve Objectives

Typical categories of risks that are often considered in creating a risk universe:

- **Financial Reporting Risk:** The risk arising from errors in the financial reporting process, such as specific errors in reporting financial results.
- **Economic Risk:** The risk arising from external macroeconomic changes of the organizations business environment.
- **Fraud Risk:** The risk resulting from any illegal acts characterized by deceit, concealment or violation of trust.
- **Information Technology Risk:** The risk that information systems will fail to ensure confidentiality, integrity, and availability of the storage and processing of the organization's data.
- **Operational Risk:** The risk of effectively executing processes and procedures as designed to support the business functions across the organization.
- **Governance Risk:** The risk that governance processes will fail to provide adequate oversight.
- **Reputational Risk:** The risk that the organizational will suffer damage to its reputation if negative media attention occurs due to failure to prevent or detect misconduct within the organization.
- **Environmental Risk:** The risk that environmental catastrophes could interrupt normal business operations.
- **Strategic Risk:** The risk associated with an organization's chosen business strategy, which includes entering new markets, developing new products, and expanding through mergers and acquisitions.

This is where we want to move the focus

20

Mapping Critical Enterprise-wide Risks

Identify the strategic objectives and major initiatives of the organization.

- Determine critical success factors for each objective
- Understand which KPI's managers are monitoring to meet business results and strategic objectives
- Perform root analysis to identify risk influencers – KRI's, that affect KPI's

21

Key Risk Indicators

KPI's

- Many organizations currently monitor key performance indicators (KPI's) in order to stay up-to-date on potential events
- According to COSO, KPI's may not provide enough advance notice. Often, KPI's alert management to risk events that have *already impacted* the organization

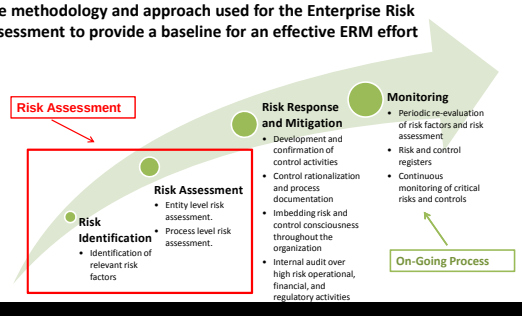
KRI's

- Key Risk Indicators (KRI's): Metrics developed by management to identify potential future shifts in risk conditions
- Using KRI's allows for more timely, strategic, and proactive development of risk mitigation strategies

22

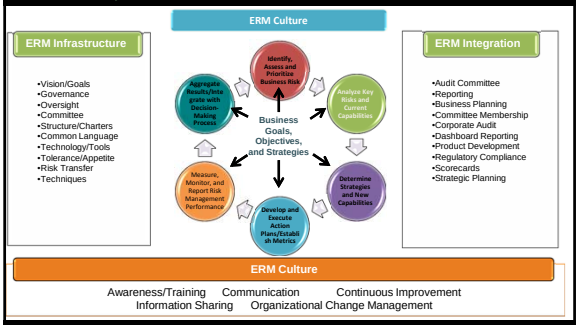
Enterprise Risk Management Approach

The methodology and approach used for the Enterprise Risk Assessment to provide a baseline for an effective ERM effort



23

ERM Overview



24

Determining the Best Approach to ERM

Seek buy-in from Board, Senior Management

- Identify an "ERM Leader" in executive management that can lead the process to begin ERM
- Create a senior-level Risk Management Committee headed by the ERM Leader
- Engage in round table discussions with the Committee to facilitate discussion of risk, risk awareness, and risk culture within the company

Identify organizational goals

- An ERM implementation plan should be adapted to the unique needs and characteristics of your organization
- Risk Management Committee should develop maturity milestones that define where the company wants to be, and when

Conduct Enterprise-wide Risk Assessment

- Conduct enterprise-wide risk assessment with Risk Management Committee's help
- Use knowledge gained about significant organizational risks to develop implementation plan that focuses on most critical risks

25

Theory into Practice: Department of Homeland Security

- The Department of Homeland Security (DHS) operates across sixteen separate agencies
- This diverse and distributed enterprise, presents a daunting challenge to implement ERM
  DHS has outlined five core missions…
  - Preventing Terrorism and Enhancing Security
  - Securing and Managing U.S. Borders
  - Enforcing and Administering U.S. Immigration Laws
  - Safeguarding and Securing Cyberspace
  - Ensuring Resilience to Disasters
- Successes in linking risk management with departmental strategy
  - DHS published a *Risk Lexicon* to establish common, operational useful language related to risk to encourage consistency between agencies.
  - DHS 's risk assessment relies on three factors; threats, vulnerabilities, and consequences. To assess risk at the strategic level, DHS has employed a Risk Assessment Process for Informed Decision-Making (RAPID).
  - In risk identification, DHS management notes the importance of answering "risk from what" and "risk to what."
  - DHS integration of ERM demonstrates the importance of Executive-level support of risk management, which fosters a risk awareness culture.

Risk Management in Non-DoD U.S. Government Agencies and the International Community

26

Public vs. Private Sector

- The Department of Homeland Security conducted a comparative survey to identify risk management efforts taken by both public and private sector organizations, providing a few key observations:
  - Secure consistent support from leadership: Many public sector responses listed that support was tough to gather due to high turnover rates.
  - Manage politically controversial risks: Public sector must deal with this where private sector avoids these more so.
  - Manage risks at an enterprise-wide level: Private sector is doing this more so than public sector.
  - Link risk management and key objectives: Lack of this has caused the public sector to fall behind the private sector in implementing ERM.

Source: Homeland Security: Office of Risk Management and Analysis

27

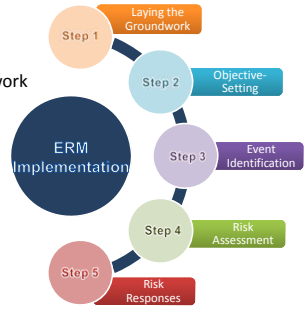
Steps to Accomplish ERM

How to Implement ERM in Your Organization

28

There Are Five Key Steps To Implementing ERM

- Step 1: Laying the Groundwork
- Step 2: Objective-Setting
- Step 3: Event Identification
- Step 4: Risk Assessment
- Step 5: Risk Responses



29

First: Don't Panic!

ERM often seems to be a daunting, complex, expensive effort. COSO offers the following tips to get an effective ERM program launched:

- **Use an incremental approach.** Some organizations have been successful launching an enterprise-wide program over time, rather than all at once
  - Start small, by picking your battles.
  - Progress observed in initial phases of ERM implementation can be used to further champion the cause of ERM in the organization. Build on your success!
- **Leverage existing Risk Management Resources and Activities.** Enhance existing capabilities rather than reinventing the wheel
- **Commit to Continuous Improvement.** Decide where you want to be with Risk Management, and develop a plan to get there. This is discussed in more detail in section four

30

Laying the Groundwork

Set the tone:

Paramount to successful implementation is establishing a Risk-Aware Culture.

31

Key Roles -Who owns ERM?

ERM should be owned and led from the top, with typical roles for the following individuals:

- **Chief Risk Officer, Executive Director, City Manager or Super Intendant**
  - Oversees the organizational risk management function and lead of the risk management framework and implementation
  - Monitors the organization's risk profile and ensures that high risks are identified and reported upward
  - Validates that ERM is functioning in each business unit according to the approved risk management policy and framework
- **General Counsel**
  - Assists in interpreting federal, state, and local law as it relates to the company's risk tolerance
- **Internal Audit**
  - Assists in the implementation process of an ERM process
  - Answers to the Audit Committee that the organization is managing risks in relation to its risk tolerance
  - Assists management in designing and implementing a suitable risk management methodology and regularly reviewing its adequacy and effectiveness.
  - Must be independent from operations

32

Key Roles in Enterprise Risk Management

The Board's responsibilities:

- Determines mission and vision
- Consults with executives to ensure an ongoing risk management process is in place
- Set the "tone at the top" in order to establish sound risk culture that mirrors risk tolerance and appetite

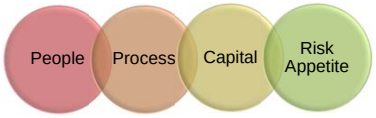
Managements responsibilities:

- Create strategies and tactical plans that are cohesive with the vision and risk appetite of the organization
- Ensures an ongoing effort exists to identify new risks and implement strategies to monitor and mitigate risks
- Evaluates impact to the organization should events occur

33

Step 2: Objective-Setting

- Objective-Setting should link people, process, capital and risk appetite



- Risk Appetite: Level of Risk the Organization is willing to accept in pursuit of value creation
  - Reflects risk management philosophy
  - Influences risk culture
  - A guidepost in strategy-setting
  - Related primarily to business model
- Risk Tolerance: The acceptable level of variation in achievement of objectives – typically measured in same units as related objectives; how much exposure to accept

34

Risk Appetite and Tolerance

Overview of Considerations Affecting Risk Profile

Existing Risk Profile	•The current level of risks across the entity and across various risk categories	Determination of Risk Profile
Risk Capacity	•The amount of risk that the entity is able to support in pursuit of its objectives	
Risk Tolerance	•Acceptable level of variation an entity is willing to accept regarding the pursuit of its objectives	
Attitudes Towards Risk	•The attitudes towards growth, risk, and return	

35

Step 3: Event Identification

Identify all events – positive and negative – that impact achievement of organizational objectives

- Do the events represent threats or opportunities?
- Opportunities should be channeled back into the objective-setting process so that they can be maximized
- Risk will be evaluated in the Risk Assessment phase of the framework
- Determine whether events are internal or external
- During risk Identification, consider risks that will influence achievement of objectives and consider KPI's used to monitor performance

36

Step 3: Event Identification

External Events and the Impact on Goals

37

Step 3: Event Identification

Internal Factors and the Impact on Goals

38

Step 4: Risk Assessment

Methods for Assessing Risk: Choose one of the four effective data collection methods for collecting information about significant risks.

Self-Assessment

- ***Advantages***
  - Participants generally close to the process and can easily identify exposure areas
- ***Disadvantages***
  - Self Assessment may miss key areas due to lack of involvement of others.
  - May not be objective.

Questionnaire

- ***Advantages***
  - Specific questions asked.
  - Works well if decentralized operations
- ***Disadvantages***
  - No opportunity for discussion. Required extra effort for follow up if responses are not clear.

Participatory / Open Forum

- ***Advantages***
  - Involves many perspectives . Creates "buy in" & awareness of RA importance.
  - Discussion format, healthy for the organization.
- ***Disadvantages***
  - Some may hesitate to speak out in a group.

Internal Audit

- ***Advantages***
  - IA has the ability to ask probing questions of participants.
  - IA personnel have expertise.
- ***Disadvantages***
  - IA may have pre-determined opinions based on prior internal audit areas, may miss new areas of exposure.

39

Step 4: Risk Assessment

Rating Risk

- Once key activities and organizational risks are identified, Management from across the organization judgmentally rates the risks
- The risk rating will be based on the profile of the company, considering factors such as organizational structure, customer concentration, economic climate, regulatory environment, etc.
- Example Risk Scale

Rating Scale	
Rank	Risk
1	Low — Very Remote (<10% Chance)
2	Below Avg. — Somewhat Likely (>10% - <50% Chance
3	Moderate — Likely (>50% - <70% Chance)
4	Above Avg. — Probable (>70% - <90% Chance)
5	High — Highly Probable (>90% Chance)

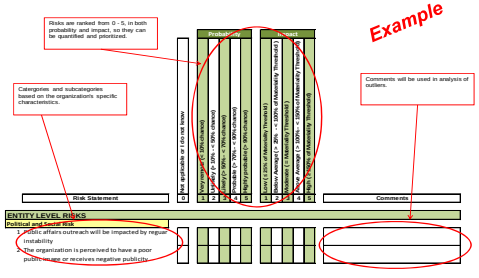
Risk responses are scored, finalized, and plotted on a Risk Map based on the following:

- **Probability** – The likelihood of an error or omission occurring
- **Impact** – The severity (monetary, operational, social, etc.) of that potential

40

Entity-level Risk Questionnaire

Risk Assessment Questionnaire



41

Entity-Level Risk Assessment

RISK CATEGORY	RISK EVENT / INFLUENCERS	Composite Risk Rating
Entity Level		
DEMOGRAPHIC RISK	Population projections, Aging workforce, Life expectancy rates	4.00
ECONOMIC RISK	Consumer behavior, employment indicators, cost of living requirements	3.53
HUMAN CAPITAL RISK	Employee competence, morale, and retention, team cohesion	3.46
GOVERNANCE RISK	Board diversity, leadership effectiveness, organization identity, tone at the top	3.24
POLITICAL RISK	Regulation, public policy, legislative activity	2.96
GROWTH / COMPETITION RISK	New providers, scalability/growth, [illegible] innovation, service expansion	2.90
REPUTATION RISK	Consumer relations, [illegible]ons (internal and external), privacy	2.89
EXTERNAL ENVIRONMENTAL RISK	External technology [illegible] relationships with outside agencies	2.88
SYSTEM / APPLICATION RISK	Adoption of new technologies, application development, deployment, e-commerce	2.87
ORGANIZATION RISK	Staffing [illegible], management practices and continuity, organizational structure	2.81
COMPUTER OPERATIONS RISK	Change management, interruptions, redundancy, maintenance, emerging technology	2.69
ORGANIZATIONAL RISKS	Employee competency, contracts, poor morale, reliance on debt financing, turnover	2.62
OPERATION RISK	Business continuity, project delivery, maintenance, health and safety, security	2.57
FINANCIAL STABILITY RISK	Availability of capital, budgeting, liquidity, debt service, cash management	2.42
SECURITY RISK	External penetration, information security, internal security, privacy, confidentiality	2.22
MISAPPROPRIATION OF ASSETS	Availability of cash, diversion of assets, theft, negligence, collusion	2.08
CORRUPTION RISKS	Kick backs, related party transactions, self-dealing, vendor favoritism	2.02
FINANCIAL REPORTING RISK	Financial statement manipulation, misuse of restricted funds, reporting capabilities	1.96
DATA MANAGEMENT RISK	Data integrity, external data, third party data sharing	1.85

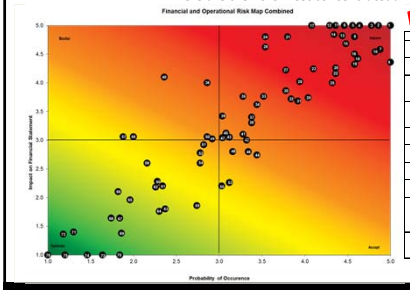
EXAMPLE

42

Entity-Wide Risk Assessment Risk Map

Where are the risks most concentrated?

Example



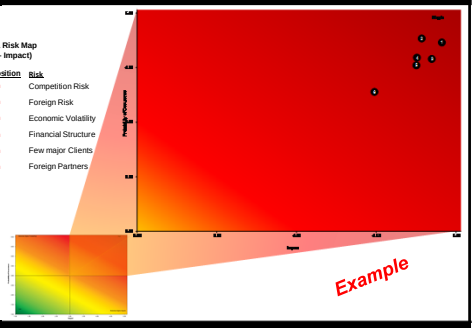
	Top 10 Risks
1	Operates in a highly competitive environment.
2	Has international operations or risk from foreign contracts or currency.
3	The industry is affected by economic trends and volatility in demand for products.
4	The financial function is not appropriately structured to allow time to be spent on relevant issues.
5	Dependent upon one or a few major customers.
6	Dependent upon the stability of foreign countries for products.
7	Has recently made significant acquisitions or plans to.
8	Particularly dependent on certain products.
9	Systems configuration is not standardized among all locations with sufficient user acceptance testing over all changes.
10	Significant product lines are particularly sensitive to changes in consumer tastes.

43

Entity-Wide Risk Assessment High Risk Map

Legend – High Area Risk Map
(P – Probability, I – Impact)

Plot Number	Matrix Position	Risk
1	High	Competition Risk
2	High	Foreign Risk
3	High	Economic Volatility
4	High	Financial Structure
5	High	Few major Clients
6	High	Foreign Partners



Example

44

Risk Mapped to the Process-Level

Risk Rated Audit Universe

Weights as determined by Risk Assessment team

Rating Scale

Translated Rank	Rank	Risk
Low	1	Low
Medium	2	Below Avg.
	3	Moderate
	4	Above Avg.
High	5	High

Risk Scale	Audit Frequency
Low	Every 36 Months to Never
Moderate	Bi-Annually
High	Annually

Significant Activities	Foreign Operations Risk		Product Acceptance Risk		IT Integration Risk		Change Management Risk		Financial Reporting Risk		Regulatory and Compliance Risk		FCPA Risk		Probability Sub-Total	Impact Sub-Total	Risk Map Quadrant
Weight	20%		12%		10%		18%		8%		18%		14%				
	P	I	P	I	P	I	P	I	P	I	P	I	P	I			
Revenue																	
Maintain Pricing Master File	3	5	3	3	5	5	1	2	4	4	1	1	3	5	2.56	3.42	2
Capture Sales Information, PO, Contract, LC	4	4	4	4	4	4	5	4	5	4	5	5	5	5	4.58	4.32	4
Generate and Enter Sales Order in System	3	3	3	3	3	3	4	4	5	4	4	5	3	4	3.52	3.76	4
Pull/Pick Goods for Shipment	4	4	4	4	4	4	5	5	5	4	5	5	5	5	4.58	4.52	4
Ship Goods and Record Shipment	4	5	4	5	5	5	5	5	3	3	5	5	5	5	4.34	4.84	4
Procurement																	
Maintain Vendor Master File	2	3	2	5	2	4	2	2	2	1	2	2	2	2	2.00	3.06	2
Maintain Item Master File	4	4	4	4	4	4	4	4	3	4	4	4	3	3	3.76	3.88	4
Process P						4	2	3	2	1	2	2	2	2	2.00	3.06	2
Receive It						4	4	4	3	4	4	4	3	3	3.78	3.88	4
Record Re						4	4								3.78	3.88	4

Example

Item identified for further assessment

Risk Rating for Heat Map

Step 5: Develop Risk Responses

Steps to Risk Mitigation

- Risk Mitigation is "A systematic reduction in the extent of exposure to a risk and/or likelihood of its occurrence."
  - Prioritize processes and activities based on the critical risk factors
  - Based on the risk rating of the processes and activities, identify the current mitigation and monitoring strategies in place to respond to the risk level.
  - Determine gaps and duplications in coverage.
  - Develop risk mitigation strategies to address gaps in coverage noted.
  - Realign Internal Audit plan to cover gaps, reduce redundancy, and maintain existing coverage, based on revisions to the risk response plan.
  - Review the completed Risk Response and Internal Audit plan to ensure adequate coverage of top risk-ranked areas based on Risk Appetite / Risk Tolerance.

Step 5: Develop Risk Responses

When developing risk responses, Management:

- Considers alternative responses
  - **Reduce:** Implement mitigating controls
  - **Accept:** Take no positive action to mitigate the risk
  - **Avoid:** Stop engaging in any activity that creates the risk
  - **Share:** Share the risk with a third party; e.g., insurance policies
- Evaluates costs/benefits of available risk responses
- Analyzes whether risk responses appropriately reduce risk to tolerable level
- Selects most appropriate risk response based on risk appetite, risk tolerance, and evaluation of portfolio risk

Risk Response Plan

Create Risk Response Plan and Align it with the Internal Audit Plan

Significant Activity	Sub-Process	Impact	Probability	Composite	Risk Map Quadrant	Risk Response
Disaster Recovery / Business Continuity Plan	Information Technology	3.83	3.07	3.44	4	DR/BCP testing is planned for March 2014
Environmental Reporting & Compliance	Facilities	3.55	3.31	3.52	4	Compliance Audit over for Phase I and II Environmental implement for November 2014
Training and Competencies	Human Resources	2.85	2.57	2.65	4	Monitoring of training compliance in performed quarterly by HR. Employee competencies are part of the Annual Employee Evaluation
Emergency Response Plans	Security	3.[illegible]	2.[illegible]	3.07	4	
Physical Security	Security	2.[illegible]	2.48	2.65	3	Included in the 2014 Internal Audit Plan
Incident Reporting and Investigation	Human Resources	2.80	2.48	2.64	3	
Network Security (Encryption, Logical Access, Virus, Internal or External)	Information Technology	3.71	2.85	3.28	4	Network security will be added to the 2014 internal audit plan. Application access is addressed through SOX Compliance procedures. 2014 Internal Audit Plan
Critical Application Access and Controls	Information Technology	3.05	2.65	2.85	4	
Debt Covenant Compliance	Debt and Equity	3.52	3.09	3.28	4	Debt compliance is reviewed annually through the external audit. An internal audit over Long-term Debt and Collateral validation was part of the 2013 Internal Audit Plan
Monitoring Collateral Provisions and Contingencies	Debt and Equity	3.00	1.67	2.33	3	

EXAMPLE

48

Alignment of Strategic Goals & Risk Appetite and Tolerance

- Risk Appetite and Tolerance Strategic Goal Mapping documents the relation of the top risk events to the strategic goals of an organization
- This will document the acceptable and unacceptable thresholds for specified metrics in place to monitor the identified critical risk events

49

What do you think?

What is the biggest challenge companies face in attempting to manage risk?

A. Weakness in risk culture
B. Organization is too complex to manage risk
C. Inadequate information needed to make risk-based decisions
D. People are unaware of what they need to do concerning risk

Source: Deloitte, "Aftershock: Adjusting to the New World of Risk Management"

50

What do you think?

What is the biggest challenge companies face in attempting to manage risk?

A. Weakness in risk culture – 15%
B. Organization is too complex to manage risk – 21%
C. Inadequate information needed to make risk-based decisions – 23%
D. People are unaware of what they need to do concerning risk – 28%

Source: Deloitte, "Aftershock: Adjusting to the New World of Risk Management"

51

Theory into Practice: Duke University

- **Duke has annual revenues of $2 billion, along with $7 billion in endowment and $500 million of federal research grants**
  - Processes need to be in place to address the inherent risks of receiving public funds
- During the beginning phase of ERM, managers and administrators at Duke were able to define who should be responsible for each risk, and how it could affect the strategic mission of the University
- With upper managements involvement, Duke was able to prioritize risk across athletic, academic, research, or medical functions and identifying which risks were most prominent at an enterprise-wide level
  - Duke employed the use of a heat map, which measures likelihood and impact of risks to assist in pin-pointing risk areas.
- **Lessons learned**
  - Don't move too quickly, implementing an ERM process across a university is a daunting task and it is tempting to cut corners
  - Small steps need to be taken to ensure that each is fully completed and done correctly before moving onto the next step

NCSU: Learning from Duke University's Enterprise Risk Management Process

52

Key Takeaways

- ERM can be implemented in five key steps
  - Laying the Groundwork
  - Objective-Setting
  - Event Identification
  - Risk Assessment
  - Risk Response
- Using an incremental approach helps ensure the ERM effort is practical, appropriate, and successful based on the needs of the company.
- Commit to continuous improvement.
  - Use the milestones developed by the Risk Management Committee in the pre-implementation phase as a benchmark for measuring progress.
  - Report results of efforts to the Risk Management Committee

53

ERM as an Ongoing Process

Document Results and Plan for Ongoing Process

54

ERM Documentation and Reporting

Objectives of ERM Reporting:

- Link the "Information and Communication" and "Monitoring" elements of ERM Framework
- Provide Management with enough information to evaluate risk management performance as frequently as the risks dictate
- Obtain actionable information about KRI's and KPI's

Keys to Effective ERM Reporting:

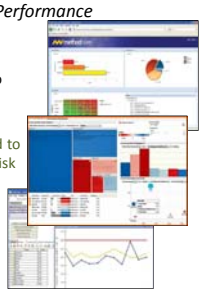
- Keep your risk profile fresh
- Monitor KRI's for critical risks and map to KPI's
- Evaluate critical controls to reduce risk
- Report on the status of risk monitoring and the risk and response plan

55

ERM Documentation and Reporting

Evaluating Progress and Performance

- Dashboard and scorecard reporting are useful in assessing risk management
- Enables executive management and the Board to understand:
  - Progress toward goal achievement
  - Status of Key Risk Indicators (KRI's) compared to performance standards for various types of risk
  - How internal performance compares to competitive benchmark information



56

Monitoring and Communicating

Internal Audit – Evaluating Progress and Improvement

- Provide a focused, independent evaluation of the adequacy of design of the risk responses developed by management, as well as the extent to which mitigating controls are operating effectively.
- Contain detailed, actionable findings that help improve effectiveness and efficiency of the risk management process.

57

ERM as an ongoing Process

Start small and document victories/successes

Consider implementing on a small scale, such as in a single department.	Use successes (i.e., reduced exceptions or increased cost savings) to obtain buy-in from skeptical managers.

Have formal or informal discussions with executive management.

What keeps executive management up at night?	What can go wrong to impact achievement of business objectives?	Identify where key controls should be and recommend that these controls be added.

Communicate effectiveness of monitoring and reporting mechanisms

Out of sight, out of mind: If people don't see the progress being made, they might lose sight of implementation goals and fail to the effort.	Implement effective / efficient reporting of KRI's / KPI's. This is critical to strategic risk management and planning.	Results of monitoring and reporting mechanisms provide feedback to measure success of ERM implementation and are vital to Continuous Improvement.

58

Theory into Practice: Bank of America

- Bank of America's is in the business of taking risks!
- The bank deployed ERM as a strategic management tool
- Their definition of operating excellence centers around the critical buy-in of the CEO.
  - Key operating elements for achieving organic growth are:
    - Innovation,
    - Using scale as a strategic advantage,
    - Building a strong brand,
    - Improving the customer experience,
    - Managing risk and reward for consistent growth.
- They approach risk and reward management as an enabler of growth by:
  1. Establishing a culture of performance management and accountability
  2. Implementing processes that are both comprehensive – taking into account all four risk categories (Credit, Market, Operational, Strategic)
  3. Taking a forward-looking view of risk

Source: "Perfect Storms, White Knuckles and the Most Challenging Job You'll Ever Have

59

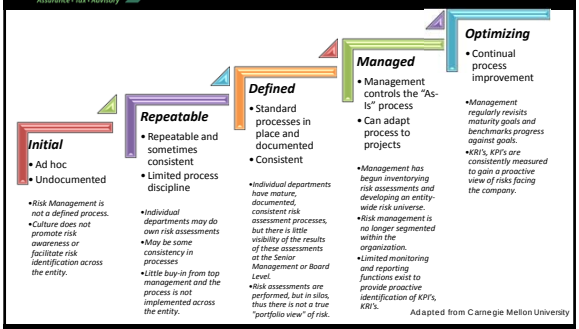
ERM as an ongoing Process

Regularly measure progress toward established maturity goals.

- Revisit the Capability Maturity Model and determine:
  - Where are we with respect to our stated goals?
  - At what rate do we want to improve?
  - What resources are we willing to commit to risk management to ensure continuous attainment of objectives?
- Make a plan to meet with key stakeholders in the process (Management, Internal Audit, etc.) to periodically monitor progress towards established goals.

60

The Capability Maturity Model



Adapted from Carnegie Mellon University

61

Thank you!

62

Disclaimer of Liability

Weaver provides the information in this presentation for general guidance only, and it does not constitute the provision of legal advice, tax advice, accounting services, investment advice or professional consulting of any kind. The information included herein should not be used as a substitute for consultation with professional tax, accounting, legal or other competent advisers. Before making any decision or taking any action, you should consult a professional adviser who has been provided with all pertinent facts relevant to your particular situation. Tax information is not intended to be used and cannot be used by any taxpayer for the purpose of avoiding accuracy-related penalties that may be imposed on the taxpayer. The information is provided "as is," with no assurance or guarantee of completeness, accuracy or timeliness of the information, and without warranty of any kind, express or implied, including but not limited to warranties of performance, merchantability and fitness for a particular purpose.

63