protiviti℠
Independent Risk Consulting

Business Risk | Technology Risk | Internal Audit

Overview of Enterprise Risk Management

Scott Norton

protiviti
Independent Risk Consulting

Agenda

- Current Business Environment
  - Protiviti's U.S. Risk Barometer Findings
  - Increased Focus on ERM as a management and governance tool
- Business Risk Management vs. Enterprise Risk Management
- The COSO ERM Framework
- Common Sense Approach to ERM
- Common ERM Obstacles & Pitfalls
- Case studies in ERM

Protiviti U.S. Risk Barometer

Vulnerability to Business Risk:

Survey Results of C-level Executives with the Nation's Largest Companies

protiviti
Independent Risk Consulting

Risk Barometer Results

According to the Protiviti Risk Barometer (published February, 2006):

- Most senior executives lack a high degree of confidence that their organization's risk management capabilities identify and manage all potentially significant business risks.
  - 38% believe that their organization is "very effective" at identifying and managing potentially significant risk.

- Less than half of large companies deploy proven risk management practices.
  - 38% utilize ERM

- 65% of companies plan to make changes in risk management capabilities in the next two years

- The CFO is most likely to be the primary individual responsible for risk management policy (32% of companies).

protiviti
Independent Risk Consulting

Risk Barometer Results

- To identify and prioritize risk, the only frequently used practice is incident reporting and loss measurement.
  - About 30% of companies use techniques such as risk mapping, risk metrics or risk modeling
  - The most common risk management practice (80%) is the internal audit department

- Companies do not have just one predominant risk today – rather, they face a range of risks.
  - The most significant risks cited were:
    - Customer satisfaction (Internal)
    - IT security (Internal)
    - Competition (External)
    - Current regulatory environment (External)

protiviti℠
Independent Risk Consulting

Other Current Risk Environment Factors

FEI Study	60% of senior executives "lack high confidence" that their company's risk management practices identify and manage all potentially significant business risks.
NACD	"It is the board's responsibility to ensure that management has instituted processes to identify major risks and has developed plans to deal with such risks…Boards will be held accountable for any failures to provide adequate risk oversight."
NYSE	Requires audit committee charter to include reference to the committee's responsibility to "discuss risk assessment and risk management."
McKinsey	About a third of directors do not understand the organization's major risks; nonfinancial risk only receives "anecdotal treatment" in the boardroom.

protiviti
Independent Risk Consulting

Agenda

- Current Business Environment
  - Protiviti's U.S. Risk Barometer Findings
  - Increased Focus on ERM as a management and governance tool
- Business Risk Management vs. Enterprise Risk Management
- The COSO ERM Framework
- Common Sense Approach to ERM
- Common ERM Obstacles & Pitfalls
- Case studies in ERM

Business Risk Management Defined

What is Business Risk Management?

A continuous process and an element of Corporate Governance. It promotes efficient and effective assessment of risk, increases risk awareness and improves the management of risk throughout an organization. This includes anticipating and avoiding threats and losses as well as identifying and realizing opportunities.

protiviti
Independent Risk Consulting

Common Weaknesses in Risk Management Approach

- Risks are managed in “silos” leading to decisions that are not always well coordinated.
- Clear assignment and accountability for management of specific risks is not evident.
- Potential risks are identified and managed on an ad hoc basis leading to a reactive approach and the potential for short-term solutions.
- Risk awareness is low due to limited communication between management levels (Execs vs. Line Management) and across business/functional units. Risk is viewed as a negative topic and is not actively discussed.
- Risk management is focused on physical losses (insurable risks) and/or on meeting regulatory requirements.
- Risk management activities are not prioritized and are not linked to strategy and/or the company’s sources of value.

Enterprise Risk Management Defined

What is Enterprise Risk Management?

A process, effected by an entity's board of directors, management, and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

protiviti
Independent Risk Consulting

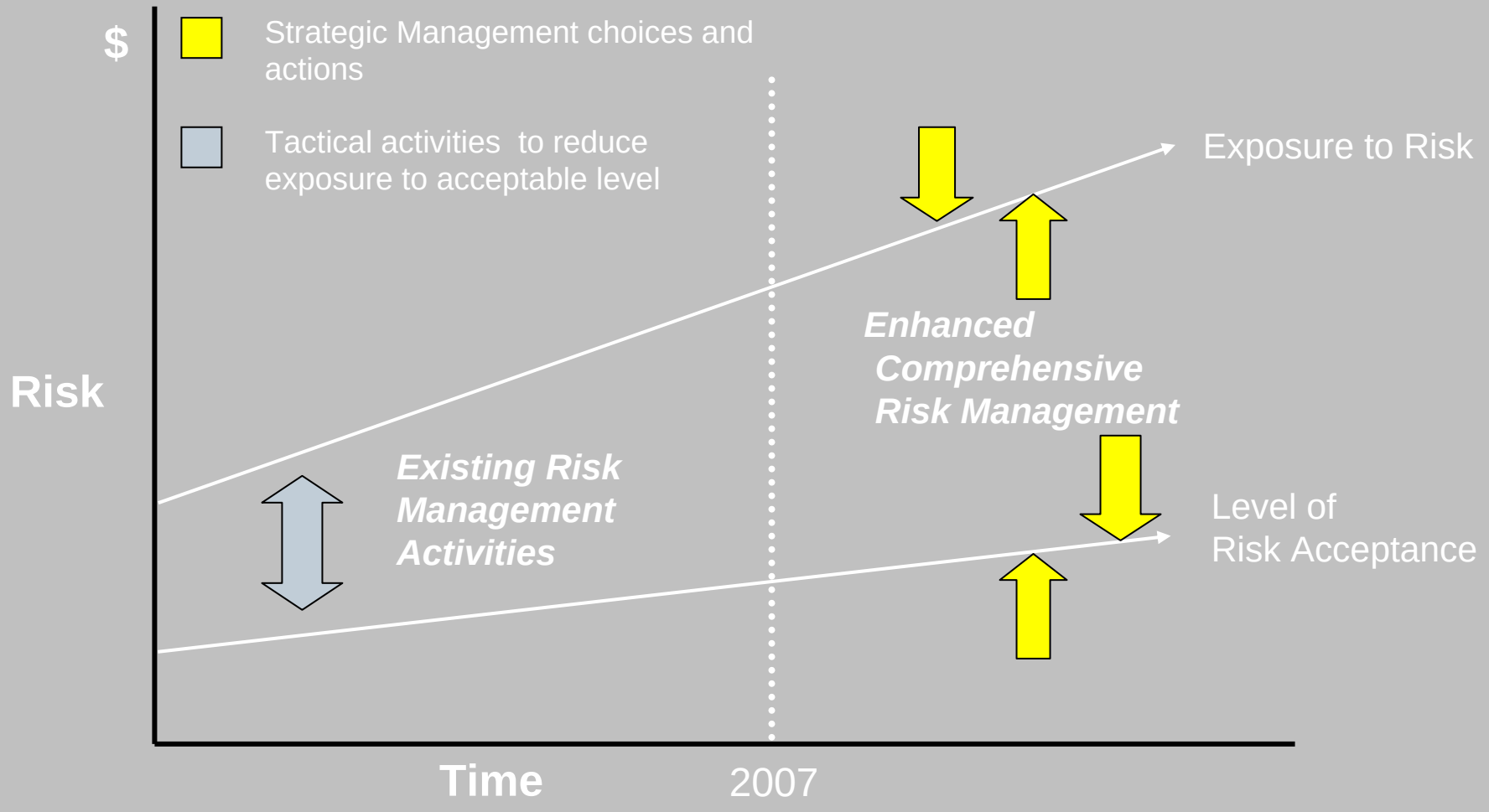
Evolution of Risk Management

	Risk Management	Business Risk Management	Enterprise Risk Management
Focus	Financial and hazard risks and internal controls	Business risk and internal controls	Business risk and internal controls
Objective	Preserve enterprise value	Preserve enterprise value	Create and preserve enterprise value
Scope	Treasury, insurance and operations involved	Business managers accountable (risk-by-risk)	Strategy, people, process, technology and knowledge aligned to manage risk on an enterprise-wide basis
Emphasis	Financial and operations	Management	Strategy
Application	Selected risk areas, units and processes	Selected risk areas, units and processes	Enterprise-wide

"CURRENT STATE" CAPABILITIES ***"FUTURE STATE" VISION***

protiviti
Independent Risk Consulting

Enterprise Risk Management Defined



protiviti
Independent Risk Consulting

Agenda

- Current Business Environment
  - Protiviti's U.S. Risk Barometer Findings
  - Increased Focus on ERM as a management and governance tool
- Business Risk Management vs. Enterprise Risk Management
- The COSO ERM Framework
- Common Sense Approach to ERM
- Common ERM Obstacles & Pitfalls
- Case studies in ERM

protiviti
Independent Risk Consulting

The COSO ERM Framework

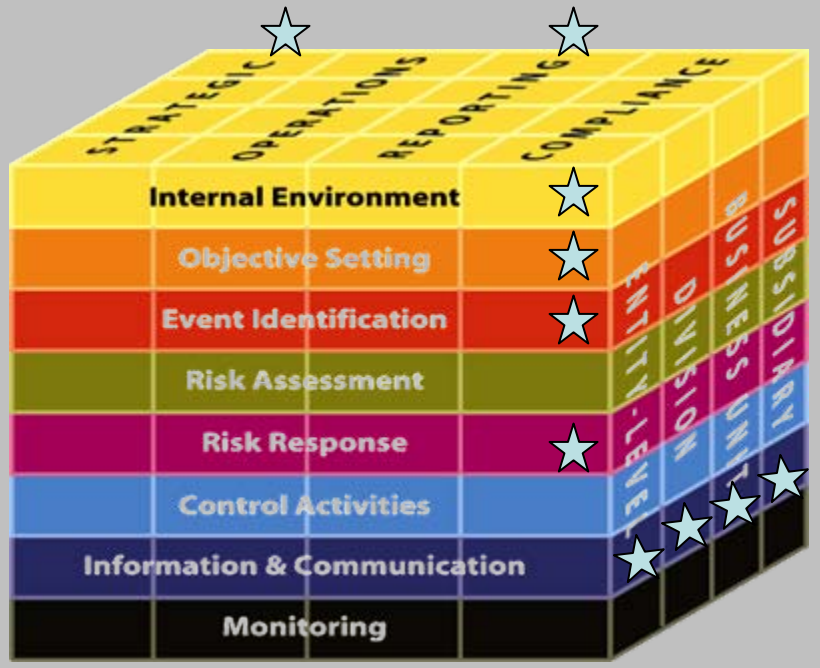
- Introduced in September 2004
- COSO concluded a broadly recognized common structure for ERM is needed
- Framework developed through input from many sources, including members of the five COSO organizations
- Authored by PwC
- COSO-appointed advisory council provided input and guidance to the process

protiviti
Independent Risk Consulting

The COSO ERM Framework

COSO Internal Control Framework

COSO ERM Integrated Framework



☆ = New or Enhanced COSO Component

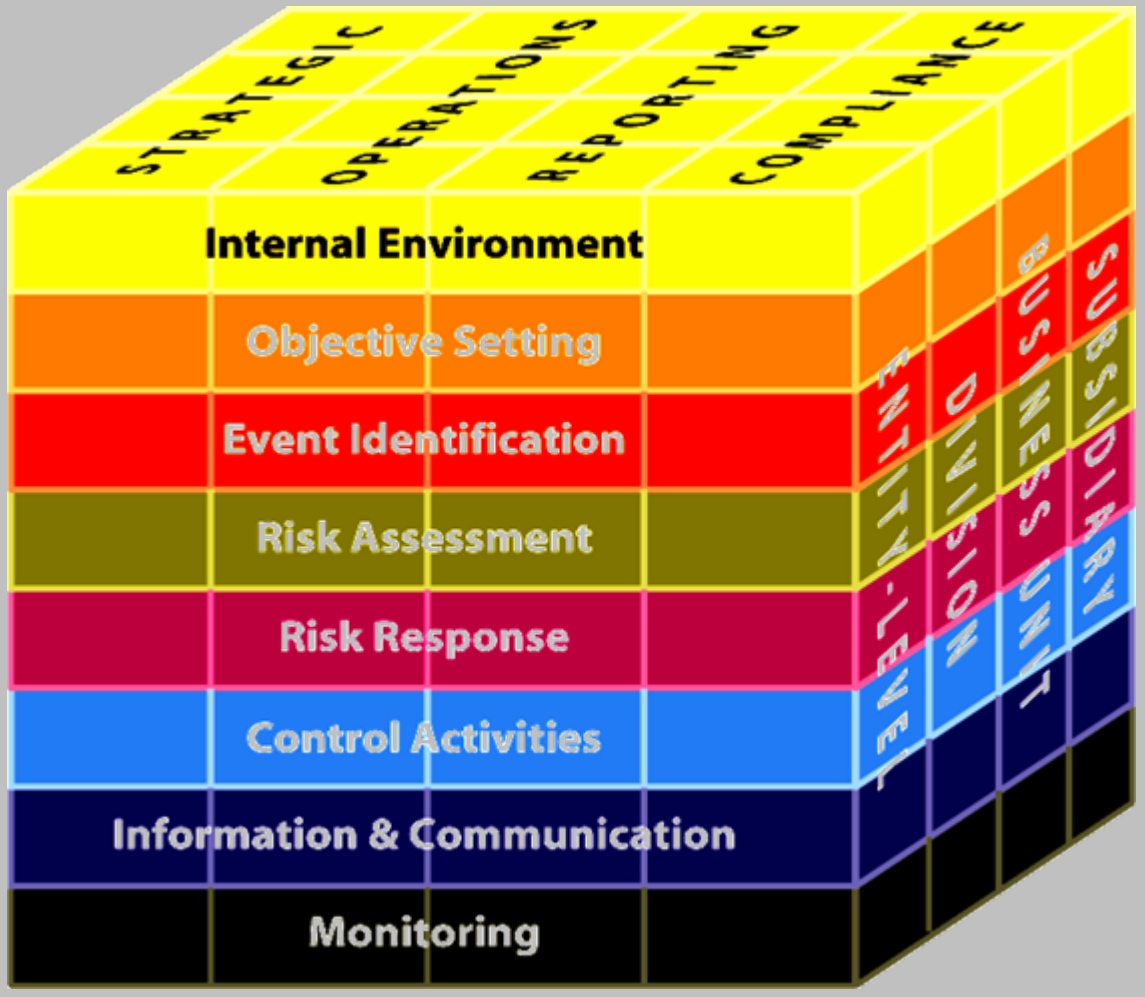
protiviti
Independent Risk Consulting

The COSO ERM Framework

The framework provides:

- A definition of risk and enterprise risk management; common language.
- Concepts, categories, principles and other elements of a comprehensive risk management framework.
- Direction for enhancing risk management.
- Criteria for determining risk management effectiveness.

Application techniques will link directly to the framework.



The COSO ERM Framework

- There are many possible elements that make up an ERM solution – the COSO framework lists many of these elements
- Companies have different objectives, strategies, structure, culture, risk appetite and financial wherewithal -- no two ERM solutions are alike
- The specific policies, processes, skillsets, reports, methodologies and systems comprising the elements defining the solution for one company may differ from another company
- Companies looking for off-the-shelf ERM solutions are setting themselves up for disappointment – in terms of what they find or the results they get….remember, one size done not fit all

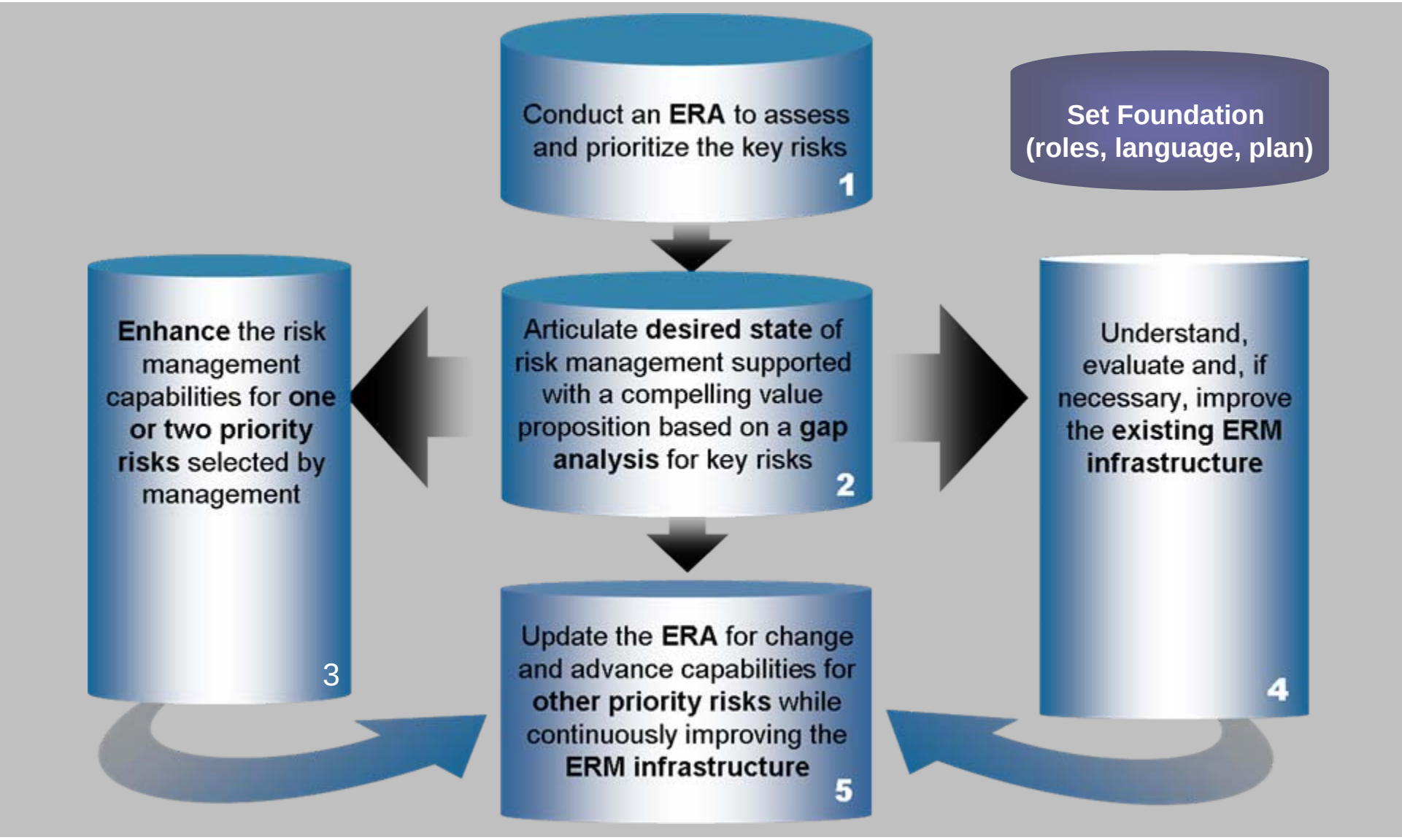
protiviti
Independent Risk Consulting

Agenda

- Current Business Environment
  - Protiviti's U.S. Risk Barometer Findings
  - Increased Focus on ERM as a management and governance tool
- Business Risk Management vs. Enterprise Risk Management
- The COSO ERM Framework
- Common Sense Approach to ERM
- Common ERM Obstacles & Pitfalls
- Case studies in ERM

protiviti
Independent Risk Consulting

Five Practical Steps to ERM Implementation



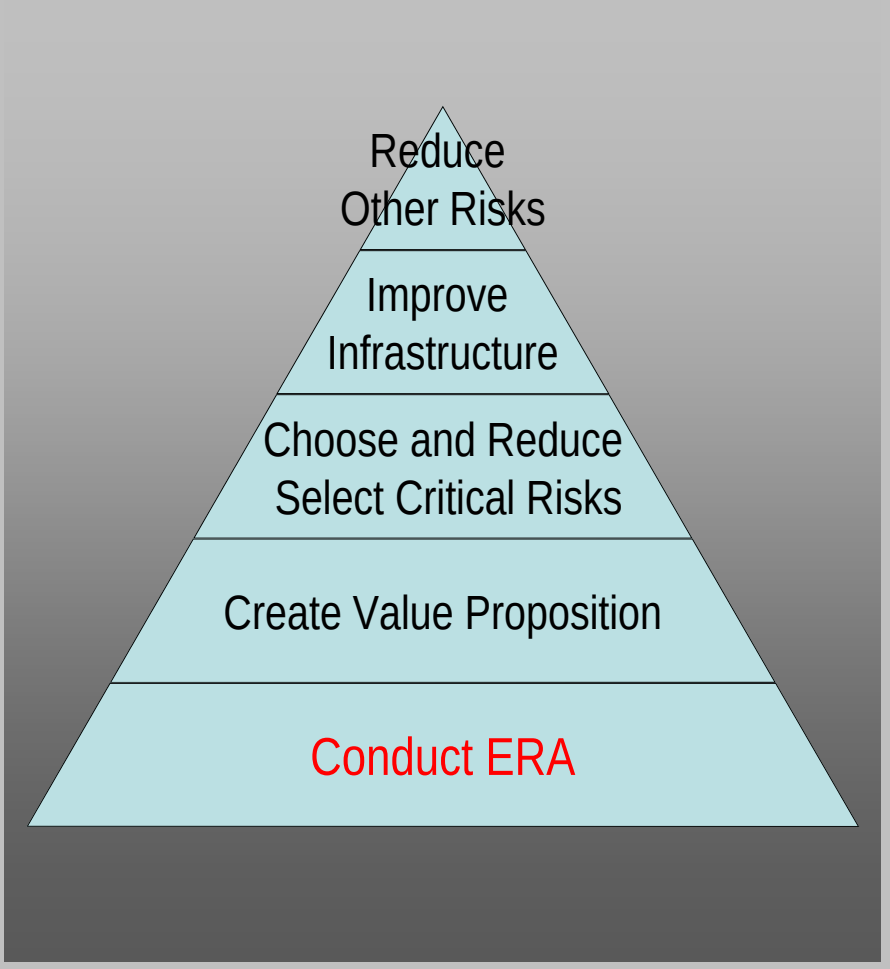
protiviti
Independent Risk Consulting

Five Practical Steps In ERM Implementation

Step 1:

Conduct an Enterprise Risk Assessment to identify and prioritize critical risks.

- Uses the business strategy as context
- Includes information about current risk management capabilities
- Encompasses COSO framework
- May encompass initial identification of gaps as the basis for improvement



protiviti
Independent Risk Consulting

Risk Assessment Data Gathering

- Executive and management interviews
- Management surveys
- Facilitated Risk Assessment Sessions
- Internal Audit Risk Assessment
- Review of 10-K and other Company Information
- Review of Industry and Risk Publications

protiviti℠
Independent Risk Consulting

Protiviti's Business Risk Model

EXTERNAL RISK

- Competitor
- Customer Wants
- Technological Innovation
- Sensitivity
- Shareholder Expectations
- Capital Availability
- Sovereign / Political
- Legal
- Regulatory
- Industry
- Financial Markets
- Catastrophic Loss

PROCESS RISK

FINANCIAL

Price
- Interest Rate
- Currency
- Equity
- Commodity
- Financial Instrument

Liquidity
- Cash Flow
- Opportunity Costs
- Concentration

- Credit
- Default
- Concentration
- Settlement
- Collateral

EMPOWERMENT
- Leadership
- Authority / Limit
- Outsourcing
- Performance Incentives
- Change Readiness
- Communications

INFORMATION TECHNOLOGY
- Integrity
- Access
- Availability
- Infrastructure

GOVERNANCE
- Organizational Culture
- Ethical Behavior
- Board Effectiveness
- Succession Planning

REPUTATION
- Image & Branding
- Stakeholder Relations

INTEGRITY
- Management Fraud
- Employee Fraud
- Third Party Fraud
- Illegal Acts
- Unauthorized Use

INTEGRITY

Customer Satisfaction	Scalability	Compliance
Human Resources	Performance Gap	Business Interruption
Knowledge Capital	Cycle Time	Product / Service Failure
Product Development	Sourcing	Environment
Efficiency	Channel Effectiveness	Health & Safety
Capacity	Partnering	Trademark/Brand Erosion

INFORMATION FOR DECISION MAKING RISK

STRATEGIC
- Environmental Scan
- Business Model
- Business Portfolio
- Investment Valuation / Evaluation
- Organization Structure
- Measurement (Strategy)
- Resource Allocation
- Planning

Public Reporting
- Financial Reporting Evaluation
- Internal Control Evaluation
- Executive Certification
- Taxation
- Pension Fund
- Regulatory Reporting

OPERATIONAL
- Budget & Planning
- Product/Services Pricing
- Contract Commitment
- Measurement (operations)
- Alignment
- Accounting Information

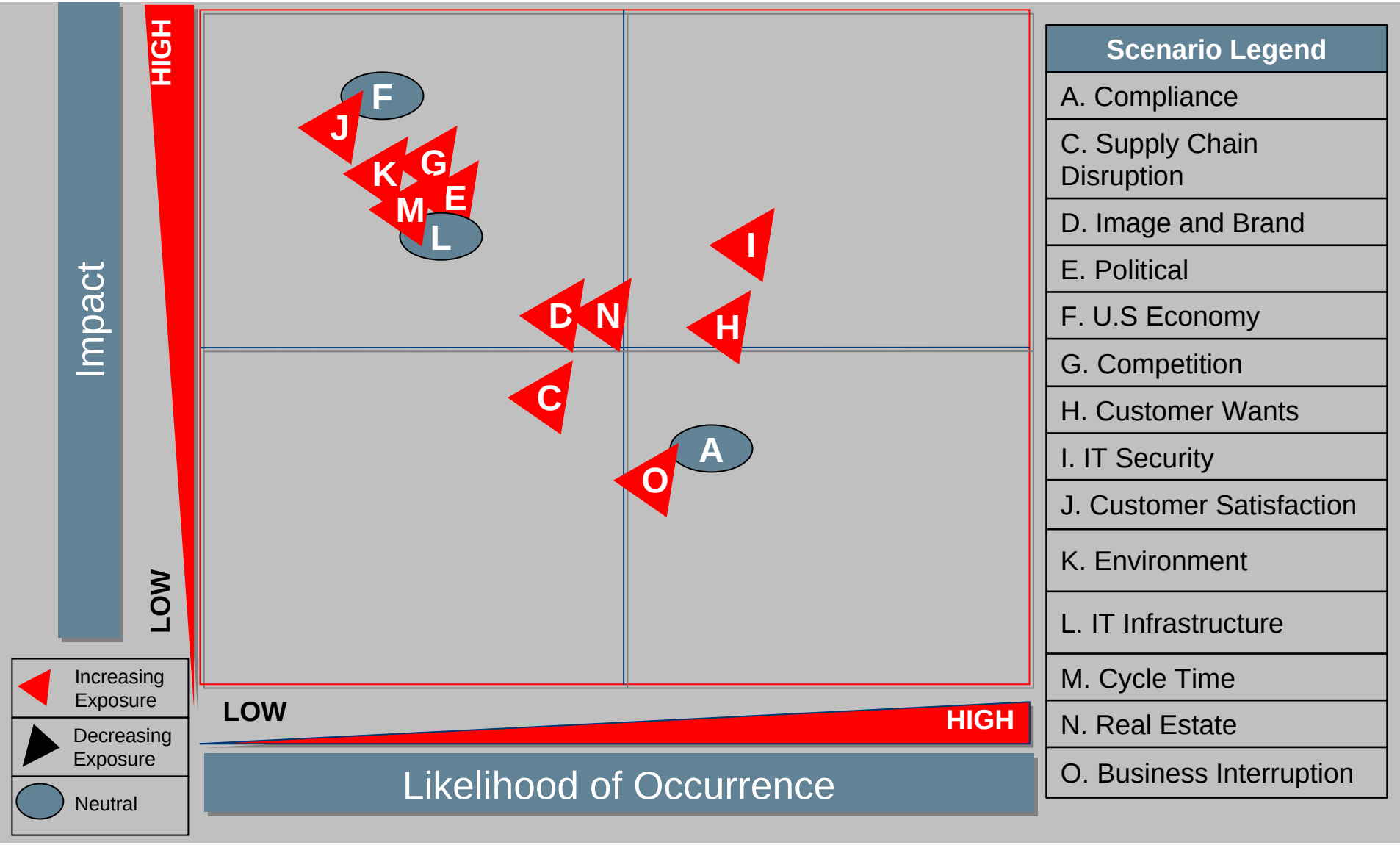
protiviti
Independent Risk Consulting

Risk Levels

Risk Level	Risk Discription
Level 1: Risk Area	External Risk
Level 2: Risk Type	N/A
Level 3: Risk Category	Catastrophic Loss
Level 4: Risk Events	• Hurricane impacts significant company assets • **Fire impacts significant company assets** • Bomb impacts significant company assets •Sustained blackout impacts significant company assets
Level 5: Detailed Risk Scenarios	• A fire originates in Corp HQ data center significantly damages computer hardware, but is contained. • Severe fire condemns Corp HQ and destroys data center. • Fire destroys Eastern distribution center

protiviti
Independent Risk Consulting

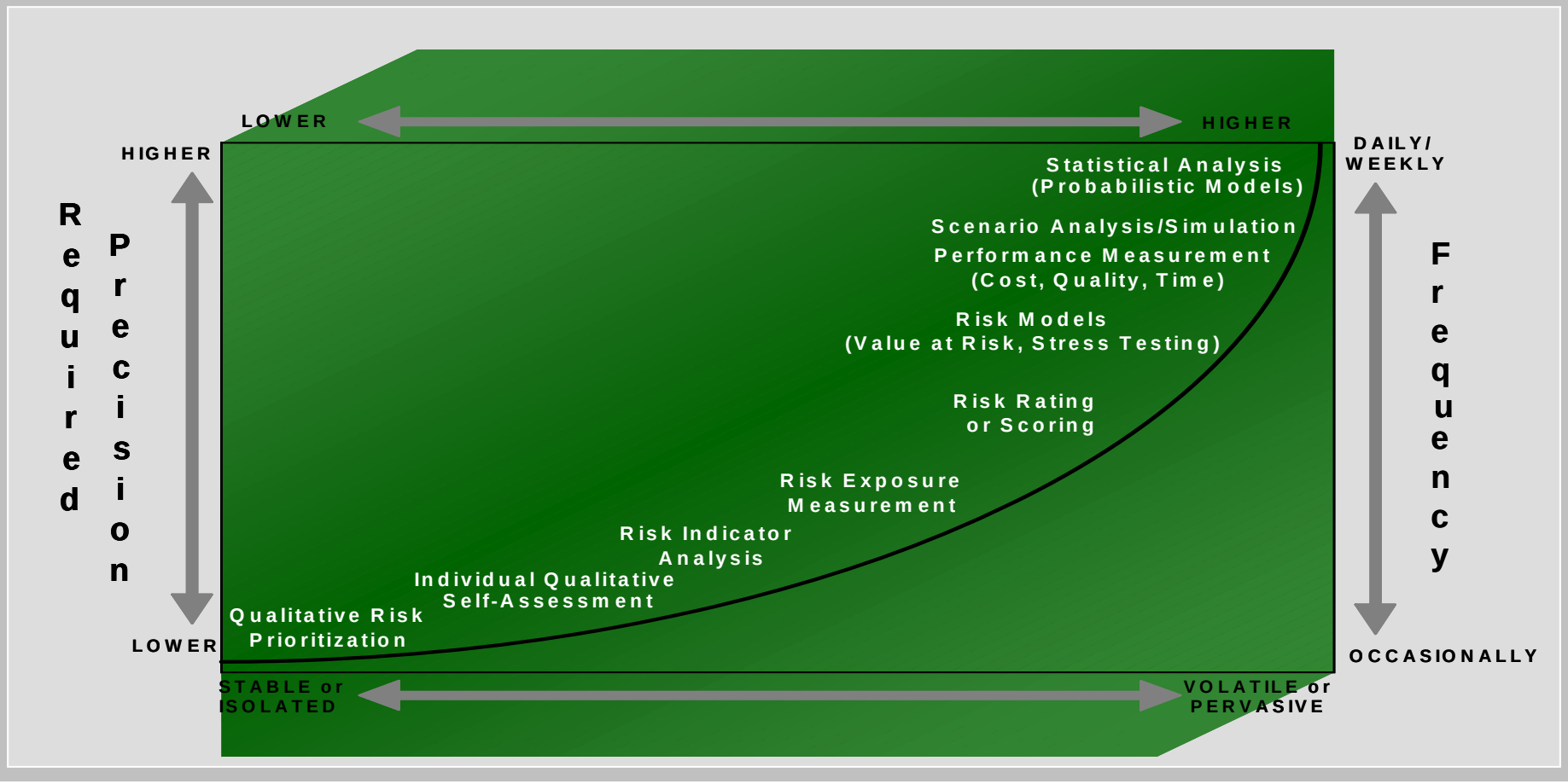
Protiviti's Business Risk Model



Scenario Legend
A. Compliance
C. Supply Chain Disruption
D. Image and Brand
E. Political
F. U.S Economy
G. Competition
H. Customer Wants
I. IT Security
J. Customer Satisfaction
K. Environment
L. IT Infrastructure
M. Cycle Time
N. Real Estate
O. Business Interruption

protiviti
Independent Risk Consulting

Risk Measurement Alternatives

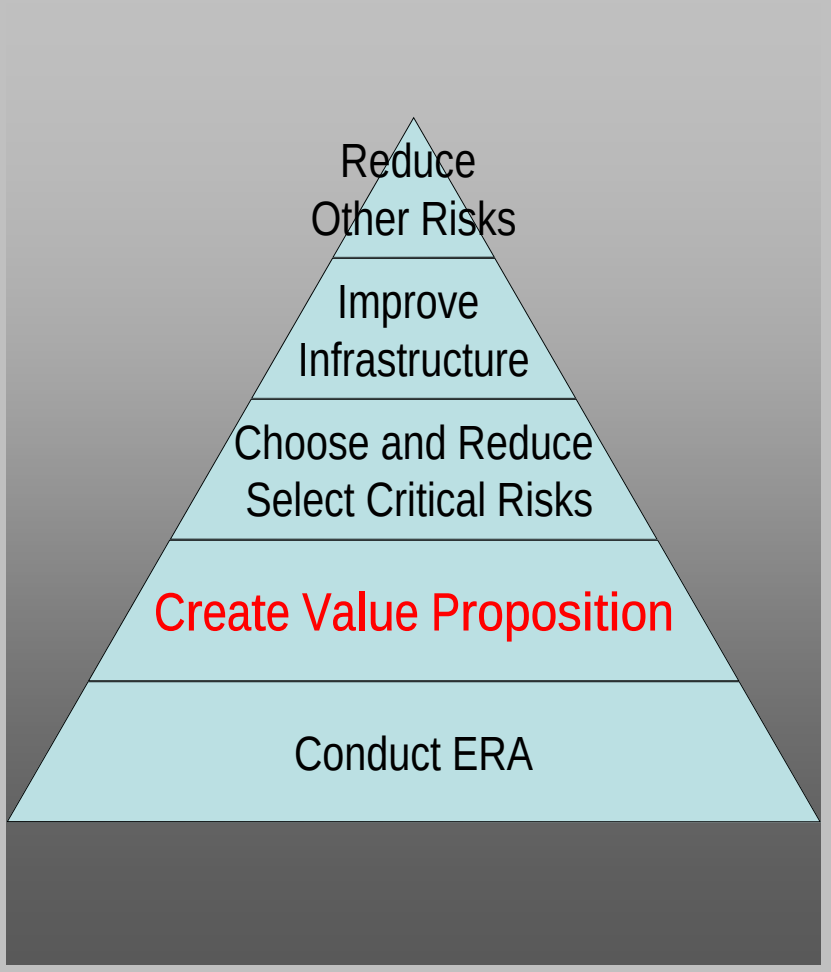


Five Practical Steps In ERM Implementation

Step 2:

Articulate the risk management vision and support it with a compelling value proposition.

- Create economic value proposition
- Identifies the organizational capabilities required to improve performance
- Defines the ERM Infrastructure
  - Policies
  - Processes
  - Oversight



protiviti
Independent Risk Consulting

What is the Value Proposition of ERM?

Sustain competitive advantage

- Expand or improve corporate governance
- Improve strategic management and business planning
- Better understand risks
- Improve risk management capabilities
- Improve capital budgeting decisions
- Better manage mergers and acquisitions

Optimize costs

- More efficiently allocate capital
- Eliminate unnecessary controls

Improve business performance

- Manage KPI shortfalls and tightened margins
- Avoid unexpected earnings-related surprises
- Respond effectively to catastrophic risks

There is no one-size-fits-all approach to ERM. Customize the approach and timing to your culture.

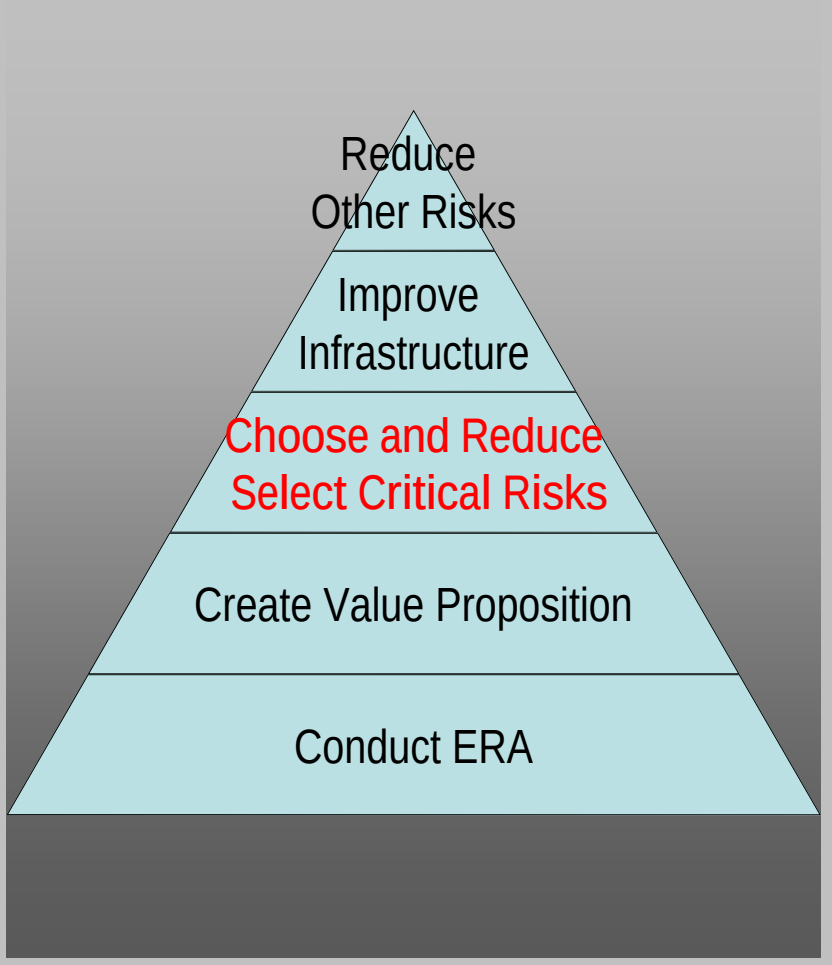
Five Practical Steps In ERM Implementation

Step 3:

Advance the risk management capability of the organization for one or two priority risks.

- Often companies look at financial reporting, then branch out
- Identify priority risks and current gaps to identify initial targets
- Integrate ERM with the management processes that affect priority risks
  - Build knowledge in laying the infrastructure for further ERM

It is important to make the milestones achievable and clear.



protiviti℠
Independent Risk Consulting

Gap Identification

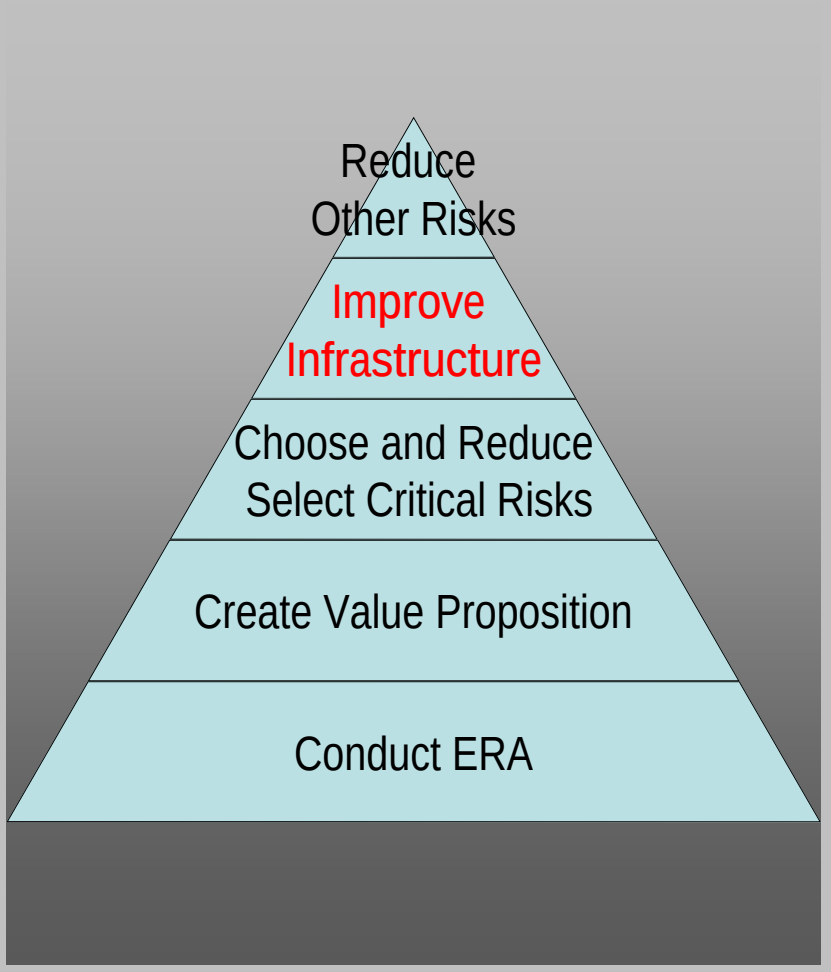
	Business Policies & Procedures	People & Organization	Data Analysis & Management Reporting	Systems and Data
Very Capable	• Enterprise-wide risk strategies are in place and enforced with a focus on continuous improvement • Risk & Strategic management are fully integrated and organized efforts are made to remove inefficiencies. Formal cost/benefit analysis are effectively applied. Best practices are shared across the organization.	•Risk management is fully aligned with company processes and individual performance measures. Process & individual performance incentives are linked to enterprise risk strategies. Risk management knowledge and skills are upgraded continuously.	•"What If" scenarios are identified and tracked, "wind tunneling" testing of risk strategies is in place and special reports are defined for key risk areas. •Risk diversification is exploited competitively. Risk quantification is fully integrated into business decisions. Quality management concepts are applied to all risk management capabilities.	•Integrated risk measurement systems are continuously improved. Special purpose systems quantify pools or portfolios of risk.
Capable	•Revised risk tolerance limits are in place based on improved analysis processes and experience. Aggregate risk tolerance limits are allocated to operating units. Business & risk strategies are aligned. •Process benchmarks are achieved. Cost and cycle time are lower. Risk management is fully integrated with line management activities. Corrective actions are taken when limits are exceeded.	•Strong teamwork is in place and role models are evolving. The enterprise is prepared for contingencies and the requisite knowledge, expertise and experience are fully in place. Experienced personnel apply judgment to quantified results.	•Integrated risk reporting is in place as are risk-adjusted profitability measures. Risk measures are linked to Key Performance Indicators (KPIs). Risks are quantified versus tolerance levels and limit violations are reported. •Integrated physical and financial risk models are defined. Risk measures are applied to performance goals. Early warning systems and risks are measured quantitatively and aggregated. Exposures are anticipated through time-tested models and analytics. Capital allocation techniques are applied.	•Enhanced functionality and expanded risk coverage are in place. Risk analytics are built into decision support systems. Risk analysis systems collect data as part of normal business routines. Database systems support management of risk & risk portfolios.
Somewhat Capable	•Enterprise-wide policies and guidelines are documented. Enterprise-wide risk tolerance limits are allocated.. •Uniform risk management processes are in place across the company. Risk mitigation and oversight are documented and applied. A disciplined modeling process exists.	•Accountabilities are clearly stated. Integrated teams, backup capabilities, standard roles, training and a central function that coordinates efforts.	•Risk reports (multi-unit; multi-risk) are in place. Senior management is comfortable with the consistent format and content of reports. Exceptions and "near misses" are reported. Audit reports include key risks. Status of improvement initiatives is reported. •Improved, consistent measures of performance variability exist. A systematic approach to loss exposures is defined and implemented. Risk coverage is expanded based on formal risk assessment processes. Alternatives are rapidly analyzed.	•Data is captured at its source and a stable client server application is leveraged to assist decision making. The architecture is scalable and reliable. •Improved functionality and web-enabled processes for data organization, extraction, analysis and reporting exist.
Limited Capability	•Business plans and risk policies are articulated. Policies are being followed and risk tolerance limits are established. •Documented, stable policies are in place. Process gaps are identified & corrected.	•Risk owners clearly defined & supported. Roles and commitments clearly defined and understood and people are trained.	•Regular actionable reports are available and some key metrics are defined and reported on. Reports generally have a consistent format and content. •Improved risk measures are in development including consistent risk related assumptions. Risk measurement methods are specified.	•Systematic data collection exists for some risks. Independent spreadsheet models are used as opposed to a centralized application. Improved system security/data integrity exists, fostering improved confidence in models. Costs are still high.
Low Capability	•Policies are undocumented or vague. Risk tolerance limits are vague or not established. •No formal processes are in place and few processes are stable. Responses to evens are reactionary and ad hoc. A "Just do it" mentality is prevalent.	•Individual heroics are relied on for the execution of processes. Firefighting and crisis management are the norm. Coordination is a challenge and accountability is weak.	•Management reports are sporadic and/or ad hoc and are often incomplete or inaccurate. The reporting process is informal, inconsistent and untimely. •Rough risk measures are defined. An over-simplification of risk may be prevalent and key risk characteristics may be missed in the methodology.	Spreadsheet are used to manage risk related information. Unstable, unscable data collection techniques are in place. Data quality poor and costs are high.

Five Practical Steps In ERM Implementation

Step 4:

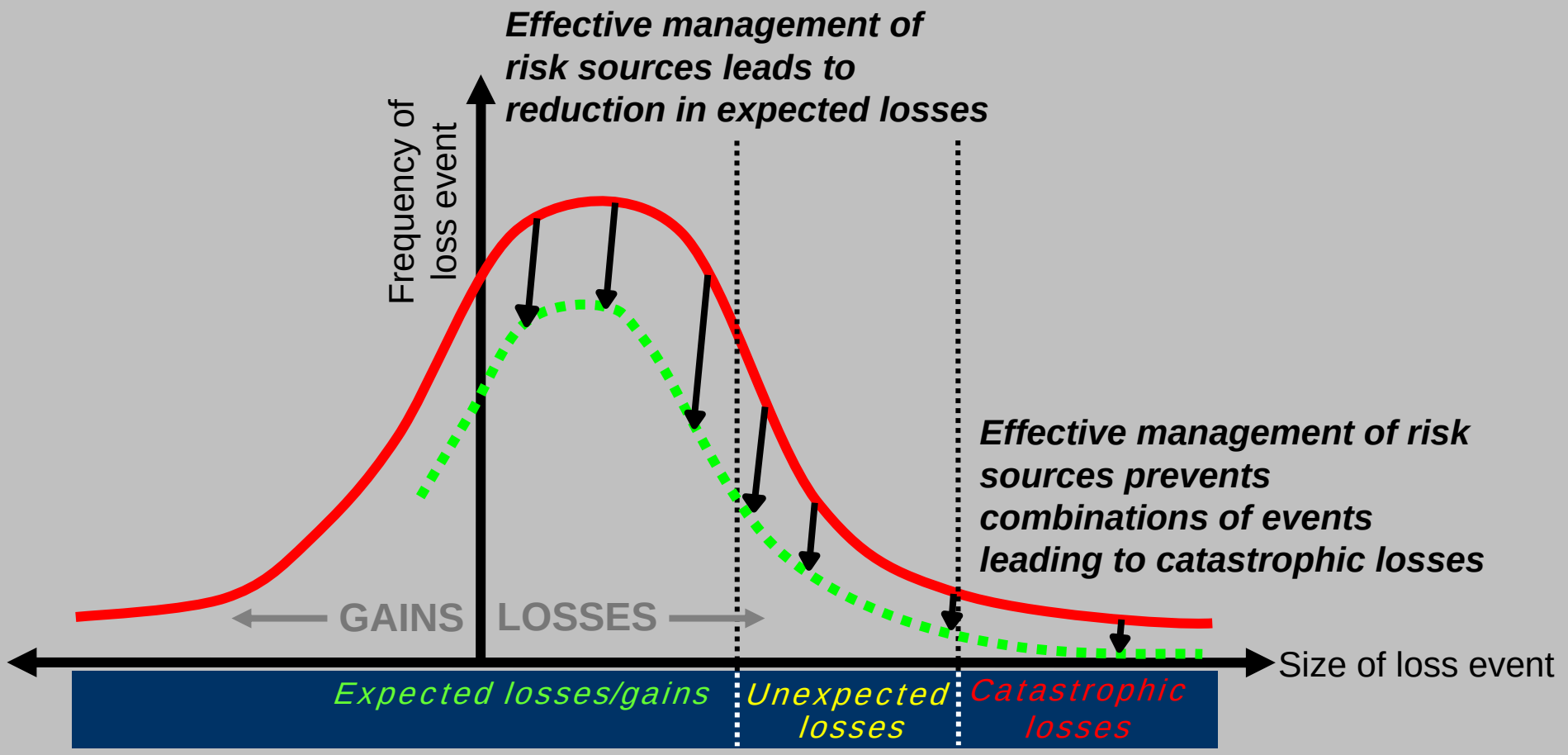
Evaluate the existing ERM infrastructure capability and develop strategy for advancing it.

- Identify integration points with existing risk management activities
- Enhance the ERM infrastructure
  - A common risk language
  - Training
  - Knowledge sharing
  - A risk champion (like a chief risk officer)
  - Define risk appetite and tolerances
- Recognize organizational uniqueness in ERM infrastructure development



protiviti
Independent Risk Consulting

Risk Appetite and Tolerance

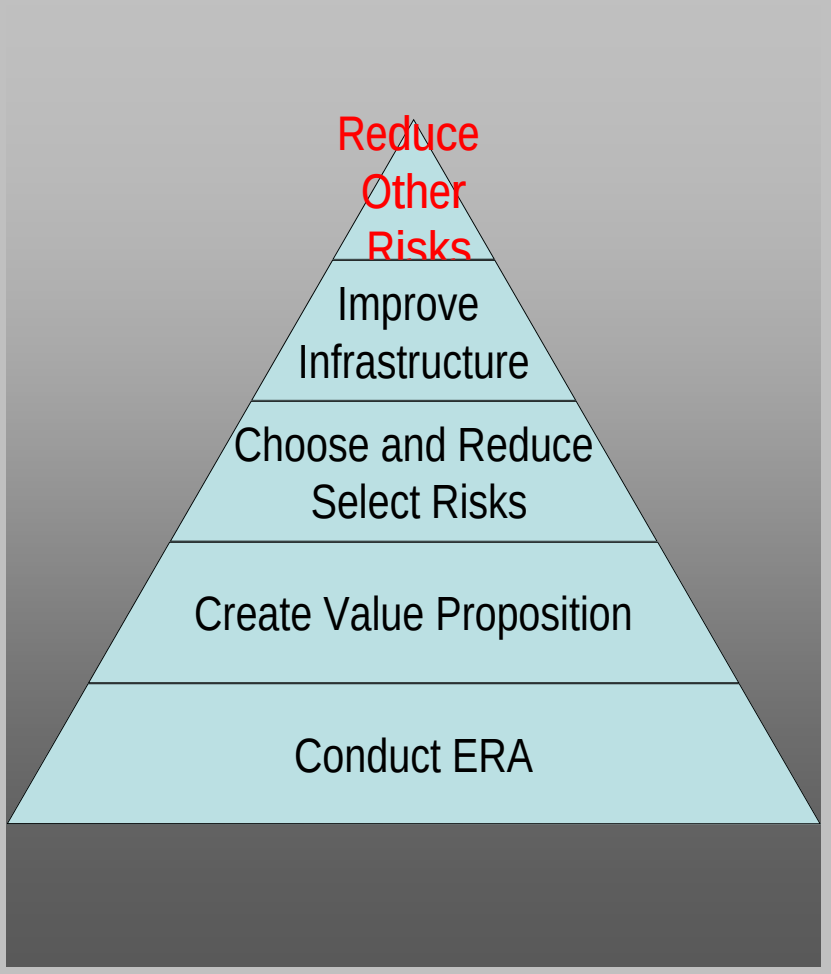


Five Practical Steps In ERM Implementation

Step 5:

Update the ERA and improve the risk management capabilities for key risks.

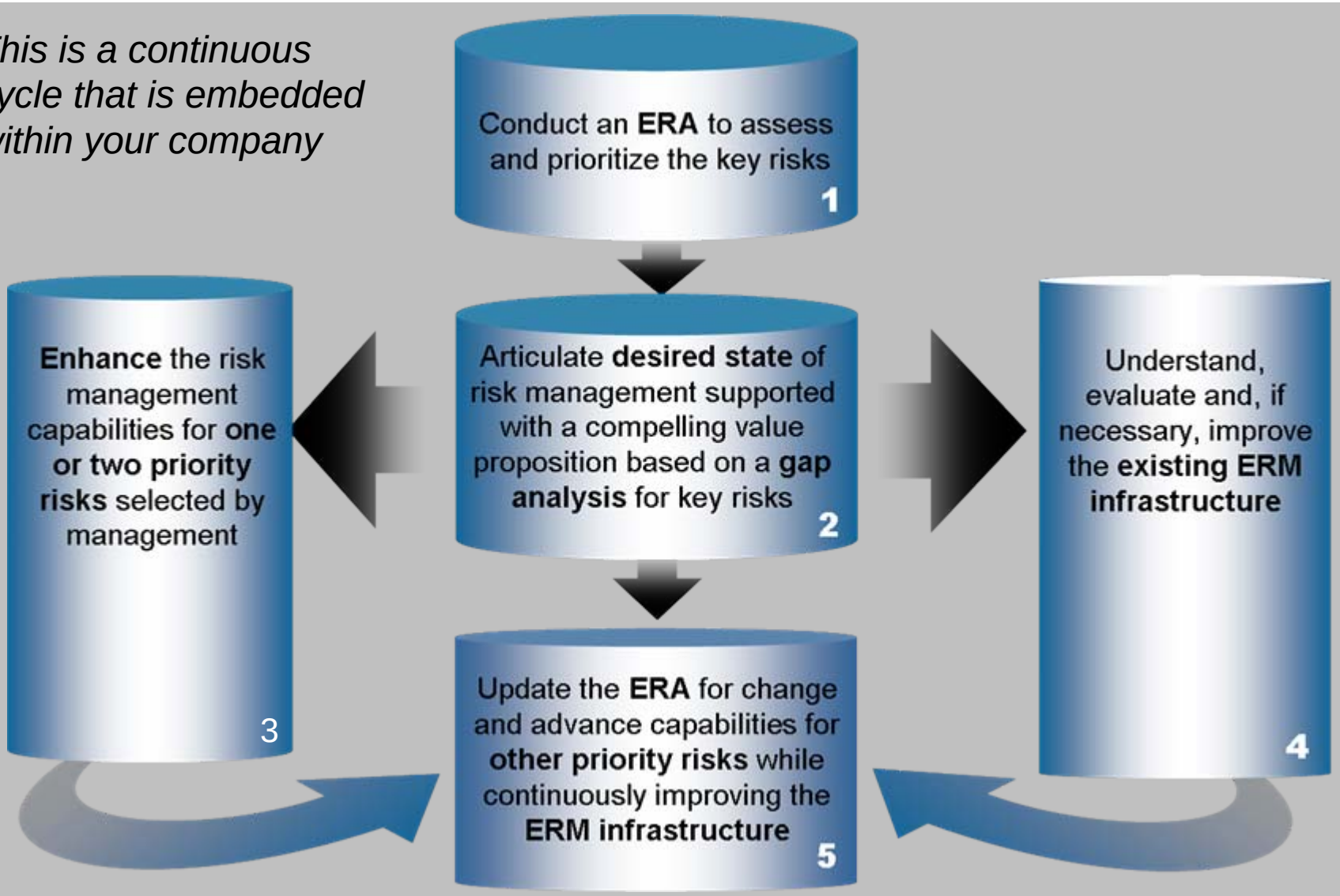
- Expand risk analysis beyond the initial (one or two) priority risks
- Identify Key Risk Indicators (KRI's) and develop executive dashboard reporting
- Consider the costs and benefits of expanding risk management capabilities
  - Which risks should be managed?
  - What is the most beneficial method of addressing these risks?



protiviti
Independent Risk Consulting

Five Practical Steps to ERM Implementation

This is a continuous cycle that is embedded within your company



protiviti
Independent Risk Consulting

Agenda

- Current Business Environment
  - Protiviti's U.S. Risk Barometer Findings
  - Increased Focus on ERM as a management and governance tool
- Business Risk Management vs. Enterprise Risk Management
- The COSO ERM Framework
- Common Sense Approach to ERM
- Common ERM Obstacles & Pitfalls
- Case studies in ERM

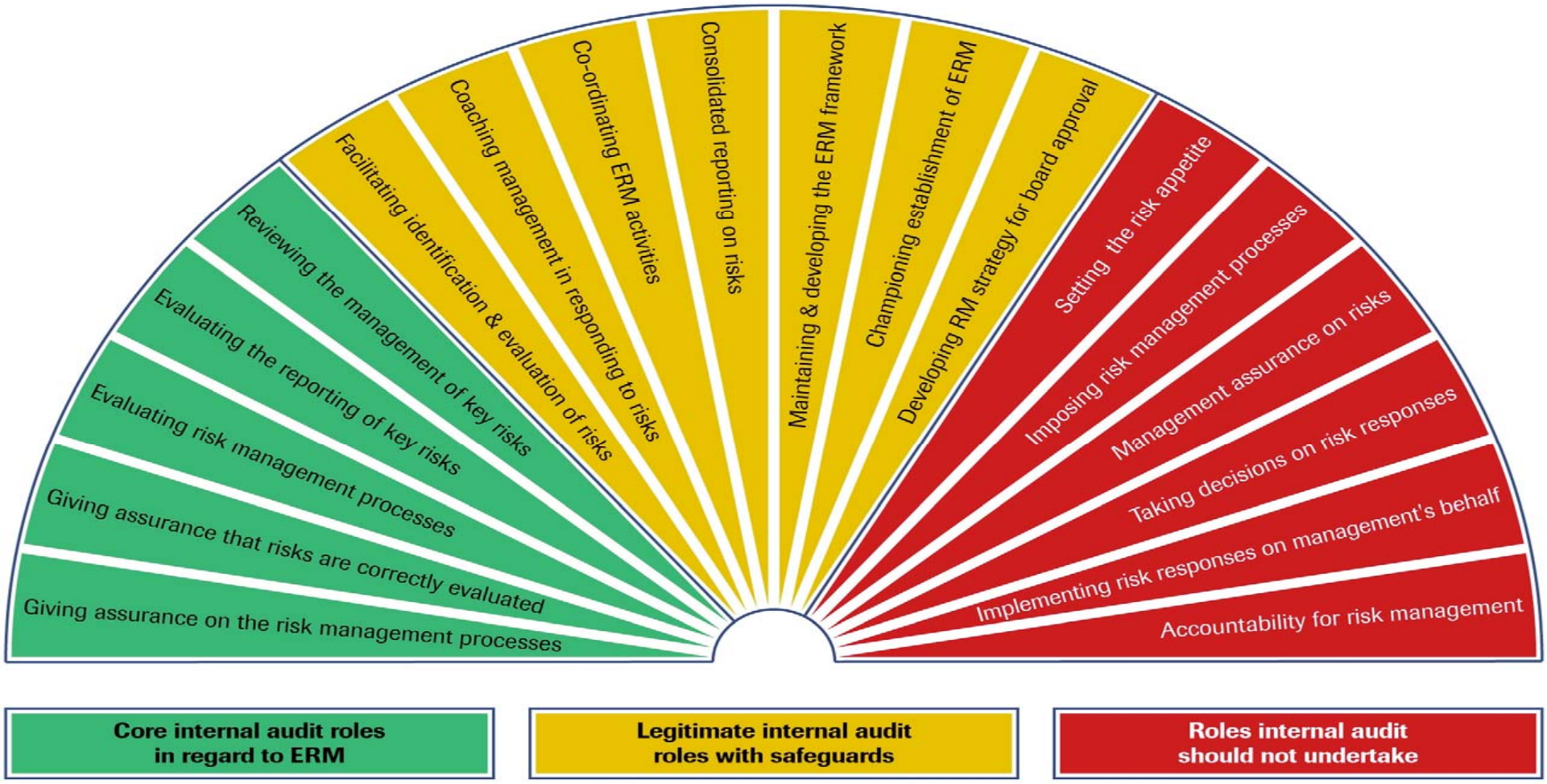
protiviti
Independent Risk Consulting

Common ERM Obstacles & Pitfalls

- Failure to get “buy-in” and support from Executive Management (CEO)
- Inability to demonstrate value to operational personnel and risk owners
- “Enterprise List Management”
- Lack dedicated resources with appropriate background
- Inability to capture, summarize and manage information
- Inefficient or ineffective risk identification techniques
- Risk responsibility not linked to rewards
- General counsel concerns over risk documentation
- ERM not integrated with other activities and functions within the organization

protiviti
Independent Risk Consulting

Role of Internal Audit in ERM



This diagram is taken from "Position Statement: The Role of Internal Audit in Enterprise-wide Risk Management", reproduced with the permission of the Institute of Internal Auditors – UK and Ireland. For the full Statement visit www.iia.org.uk.

protiviti
Independent Risk Consulting

Summary: The ERM Journey

Different companies are at different stages of maturity

Summary: Benefits of ERM

- Promoting a better understanding of risks
- Putting in place a process to highlight the key risks, what is being done, and by whom
- Bringing to light emerging risks earlier
- Enabling organizational alignment to manage the risk and control the cost of compliance
- Allowing organizations to take on and effectively manage risks that their competitors cannot
- Strengthening corporate governance, to increase the confidence of stakeholders, including regulators

protiviti
Independent Risk Consulting

Agenda

- Current Business Environment
  - Protiviti's U.S. Risk Barometer Findings
  - Increased Focus on ERM as a management and governance tool
- Business Risk Management vs. Enterprise Risk Management
- The COSO ERM Framework
- Common Sense Approach to ERM
- Common ERM Obstacles & Pitfalls
- Case studies in ERM

Case Study: ERM Company Profiles

Newell Rubbermaid ($7 billion in revenues, 26 decentralized business units)

- *Goal in Implementing ERM*: To comply with NYSE listing requirements and SOX. Decentralized organization resists centralized initiatives, so focus is on "Comprehensive Risk Management".
- *Began ERM:* 2005
- *Approach to ERM:*
  - No fully dedicated resources, but VP of IA and one auditor work on risk management effort
  - Business Unit roles include: identify, prioritize and quantify downside risk/upside reward; put mitigation plans in place; collect and report data to be aggregated at Corporate
  - Corporate roles include: approve risk management policies; provide technical expertise and support; imbed risk management considerations into corporate processes (strategic planning, budgeting, etc.); aggregate business unit exposures; communicate risk management to Board of Directors
- *How is Risk Management different from good management?*
  - Defined approach that is integrated with strategy to outline exposures, issues and problem areas. Allows management to examine what is missing and why that creates risk
  - Better up front planning including alignment of policies and capabilities to strategy
  - Improved monitoring of planned improvements to ensure they occurred
- *Benefits Anticipated:*
  - Proven anticipation of outcomes
  - Better resource and capital allocation
  - Improved budgeting

protiviti
Independent Risk Consulting

Case Study: ERM Company Profiles

Harrah's Entertainment Inc. ($7 billion in revenues, operate nearly 40 casinos)

- *Goal in Implementing ERM*: To eliminate "silo mentality".
- *Progress in adopting ERM:* Still early in the ERM journey – "We are in our late freshman year"
- *Began ERM:* 2004/2005
- *Approach to ERM:*
  - Fully dedicated ERM department reporting to CFO
  - Began with a comprehensive risk assessment
  - ERM department works with management to determine best case and worse case scenarios for key risks
    - Use risk modeling, actuarial science, forensic accounting and other tools to understand risk and determine the appropriate response
  - Slowly embedding ERM in key corporate business processes (sourcing, M&A, strategic planning). Beginning to role out to individual properties/casinos
- *Biggest ERM challenge:* Defining and producing performance measurement for ERM
- *Benefits Recognized:*
  - Reduction in claim volume and severity
  - More educated business decisions
  - Greater return on investment

protiviti
Independent Risk Consulting

Case Study: ERM Company Profiles

Ameritrade ($16.5 billion in total assets; 5 primary locations)

- *Goal in Implementing ERM*: "To stretch risk management across all departments and business units so that it would penetrate the company and establish a common risk language in everything we do."
- *Began ERM:* 2001
- *ERM Structure:*
  - Corporate Risk Officer (CRO) facilitates ERM
  - Corporate Risk Committee – executive management of the company
  - 8 Risk Subcommittees – representatives across the organization – "imbedded in operations"
- *ERM Approach:*
  - Corporate Risk Committee participates in Strategic Risk Assessment Workshops (Top Down Assessment)
  - Risk Subcommittees assess detailed risks (Bottom Up Assessment)
  - Risk assessments facilitated by CRO and Corporate Audit
    - Utilize frequency, severity, probability and likelihood as metrics in assessing risk
  - Risk matrices used to organize risks, assign key ownership and identify gaps
  - Developed a scorecard approach to monitor the effectiveness of ERM
    - "Cost of Risk" is quantified – includes insurance premiums, claims, litigation, discontinued operations, and other events that occur as a result of risk taking
- *Benefits of ERM:*
  - Significant increase in risk awareness, ownership and accountability. All 2,100 associates have risk management responsibility.
  - Reduced insurance premiums – deeper discounts due to risk management activities

protiviti℠
Independent Risk Consulting

Who We Are

Business Risk	Technology Risk	Internal Audit
• Enterprise Risk Management • Supply Chain Management • Financial Process Effectiveness • Fraud and Event Response • Governance and SOX Compliance • Discovery Risk Management and Litigation Consulting	• Security & Privacy • Continuity & Disaster Recovery • Change Management • IT Asset Management • Program Management • Application Effectiveness	• Outsourcing/Co-Sourcing • Transformation • Quality Assessment • IT Audit • Audit Committee Advisory Services

Protiviti's clients include more than 25% of the Fortune 500 companies; and more than 35% of the Fortune 100 companies.

protiviti[SM]
Independent Risk Consulting

Business Risk | Technology Risk | Internal Audit

All those who need to know their potentially significant business risks are identified and effectively managed…

Say i

Scott Norton

Scott.Norton@Protiviti.com