iWaves
evolve innovate grow

Pragmatic Guide to Enterprise Risk Management

September 2008

PRODUCTS | CONSULTING | DEVELOPMENT | TRAINING

Disclaimer

Confidentiality

This document including any files contained herein is confidential information of iWaves and should not be disclosed to third parties. Any unauthorized use of this document including, but not limited to, copying, reproducing, modifying, republishing, uploading, posting, transmitting, distributing, selling, creating derivative works from, displaying on in any other way exploiting any of its content, in whole or in part, is expressly prohibited and could subject such third party using this document to substantial civil liability.

No Reliance:

This document is subject to change without notice, iWaves cannot guarantee completion of any future products or product features / enhancement described in this document, and no reliance should be placed in their availability.

Disclaimer

The logos and other trademarks wherever used in the presentation belong to their respective owners.

Who we are

- Paisley is an independent software vendor for providing innovative solutions for governance, risk and compliance
- The Paisley GRC software solution supports
  - Financial controls management
  - Internal Audit management
  - Operational risk management
  - Compliance
  - IT governance
  - Enterprise Risk Management

Paisley GRC Solutions

- Paisley Enterprise GRC
  - Complete GRC solution for large enterprise clients
  - Scalable, proven
  - Easy to implement – 45 day implementation gaurantee
  - Single applicaton and single database schema provide unmatched levels of integration
- GRC on demand
  - Complete GRC solution delivered via software as a service
  - Lowest total cost of ownership
  - Get started in days
  - Start small and grow into enterprise adoption
  - Single application and single database schema provide unmatched levels of integration

History, Success, Leadership

- History
  - 12 years dedication to the governance, risk and compliance space
  - Recognized domain experts in GRC process disciplines
- Success
  - Largest GRC customer base, including 140 of fortune 500
  - 100,000 + users representing more than 1300 companies
  - Recognized by leading analyst firm as leader in the GRC space
- Product Leadership
  - Mature products leveraging industry best prsctices

Infowaves

- Paisley partner since 2005
- One of the five partners worldwide
- Part of the team that implemented several GRC solutions with Paisley worldwide
- Exclusive end to end solution provider for the Paisley GRC solution
- Operate from 5 centers across the ASEAN and Middle East region
- Team size of 35 dedicated to this space

Definitions of Risk Management

- The methodical management of all material risks
- The culture, processes and structures that are directed towards realizing potential opportunities whilst managing adverse effects
- ERM is the process by which organizations in all industries assess, control, exploit, finance, and monitor risks from all sources for the purpose of increasing the organization's short and long term value to its stakeholders

Focus on Risk

- Corporate governance standards vide legislations
- “Unanticipated" events are more frequent and larger
  - Business interruptions
  - Sub-prime mortgages
  - Data losses
  - Significant deficiencies
- Convergence of compliance activities
  - Risk provides a common discipline across silos
- Cost effectiveness of control-based assessments
  - AS2 vs. AS5
- ERM is factored into financial stability
  - Credit rating agencies beginning to assess

Need for ERM

"76 percent of internal audit executives and managers reported that they intend to expand Sarbanes-Oxley Compliance into enterprise risk management (ERM) or were already in the process of doing so."

- Compliances worldwide – more stringent
- Organizations operate in more diverse fields then before
- Operations are across continents

ERM is Core to the Finance Discipline

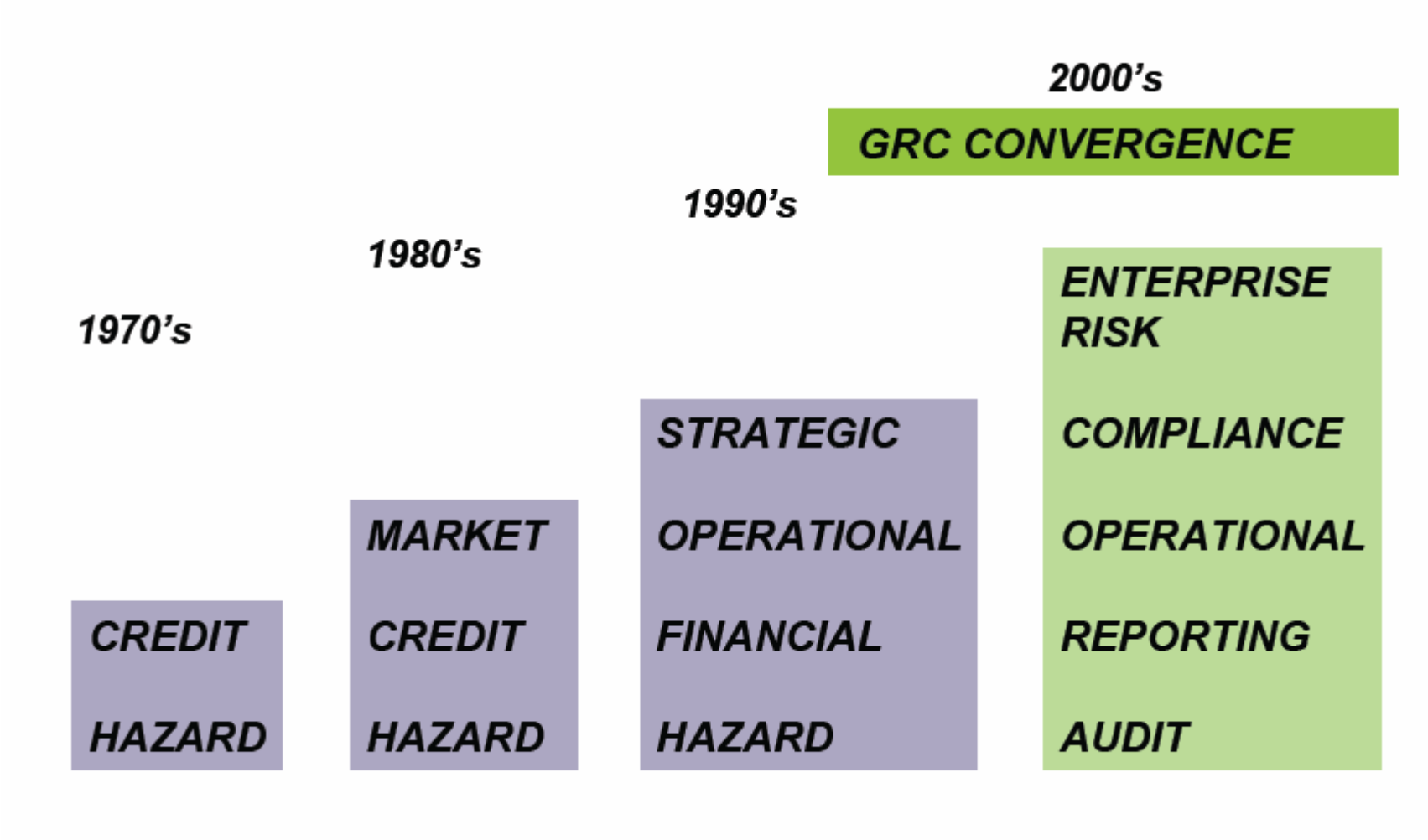
- Strategic Planning
  - ERM is required for making informed risk-based decisions from a top-down, risk-based corporate planning process
  - ERM is a top-down strategy to identify the main organizational objectives and risks to meet those objectives
  - ERM is a systematic and structured way of aligning an organization's approach to risk with its strategy
- Sarbanes-Oxley Compliance
  - A top-down, risk-based approach is the most effective way to sustain SOX compliance under AS5
- Internal Audit
  - ERM is a best practice of the leading internal audit departments

ERM Defined - COSO

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

– **COSO Enterprise Risk Management –Integrated Framework, 2004, COSO**

The Evolution of ERM: GRC Convergence



iWaves
evolve innovate grow

ERM and Sarbanes-Oxley

Risk Orientation: ERM vs. SOX

Word Count Comparison		
	Risk	**Control**
Basel II	1,500	67
ANZ 4360	307	7
AS2	79	1203
AS5	168	635

Strategy: Shift focus from control to risk identification and assessment for ERM

Why is ERM Important?

- Can help safeguard businesses against losses, earnings surprises and reputation damage by:
  - Strengthening the management of credit, market and other financial risks
  - Designing effective controls over fraud, systems and compliance failures
- Enhance the basis for decision-making
  - Clear and aligned businesses objectives
  - More focused management information
  - Better understanding of the trade-offs between r and reward

COSO ERM Risk Assessment Process

- **Objective Setting:** Enterprise risk management ensures that management has in place a process to set objectives and that the chosen objectives support and align with the entity's mission and are consistent with its risk appetite.

- **Event Identification:** Internal and external events affecting achievement of an entity's objectives must be identified, distinguishing between risks and opportunities.

- **Risk Assessment:** Risks are analyzed, considering likelihood and impact, as a basis for determining how they should be managed. Risks are assessed on an inherent and a residual basis.

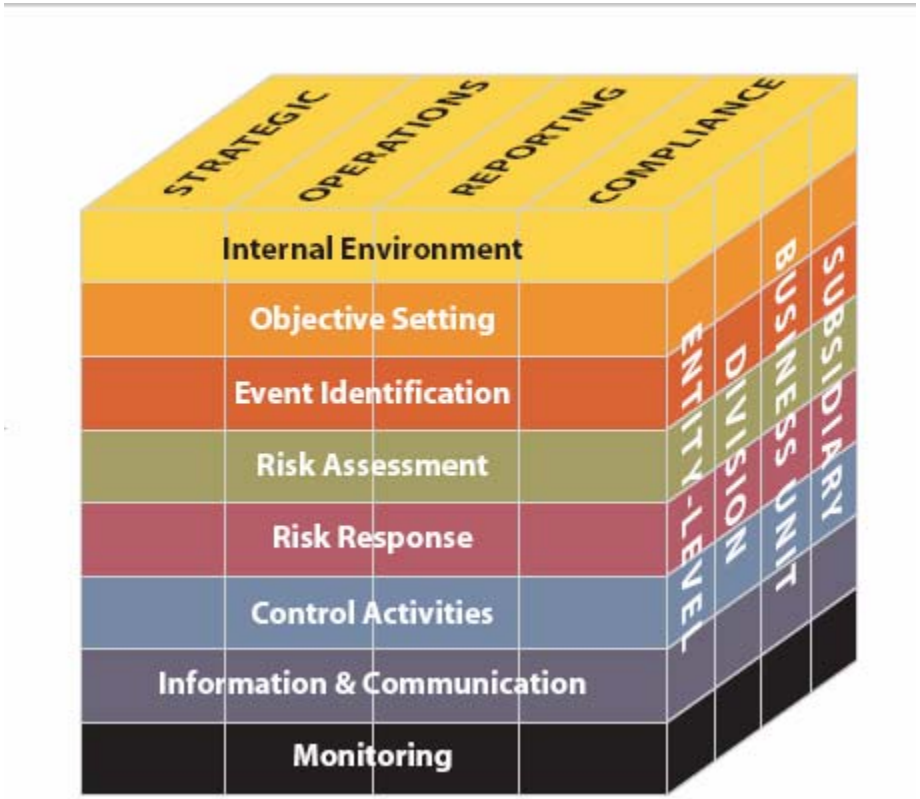
- **Risk Response:** Management selects risk responses–avoiding, accepting, reducing, or sharing risk –developing a set of actions to align risks with the entity's risk tolerances and risk appetite.

- **Assess Supporting Business Processes:** How do existing processes support objectives? Assess their performance. What gaps exist?

Relationship of Objectives and Components

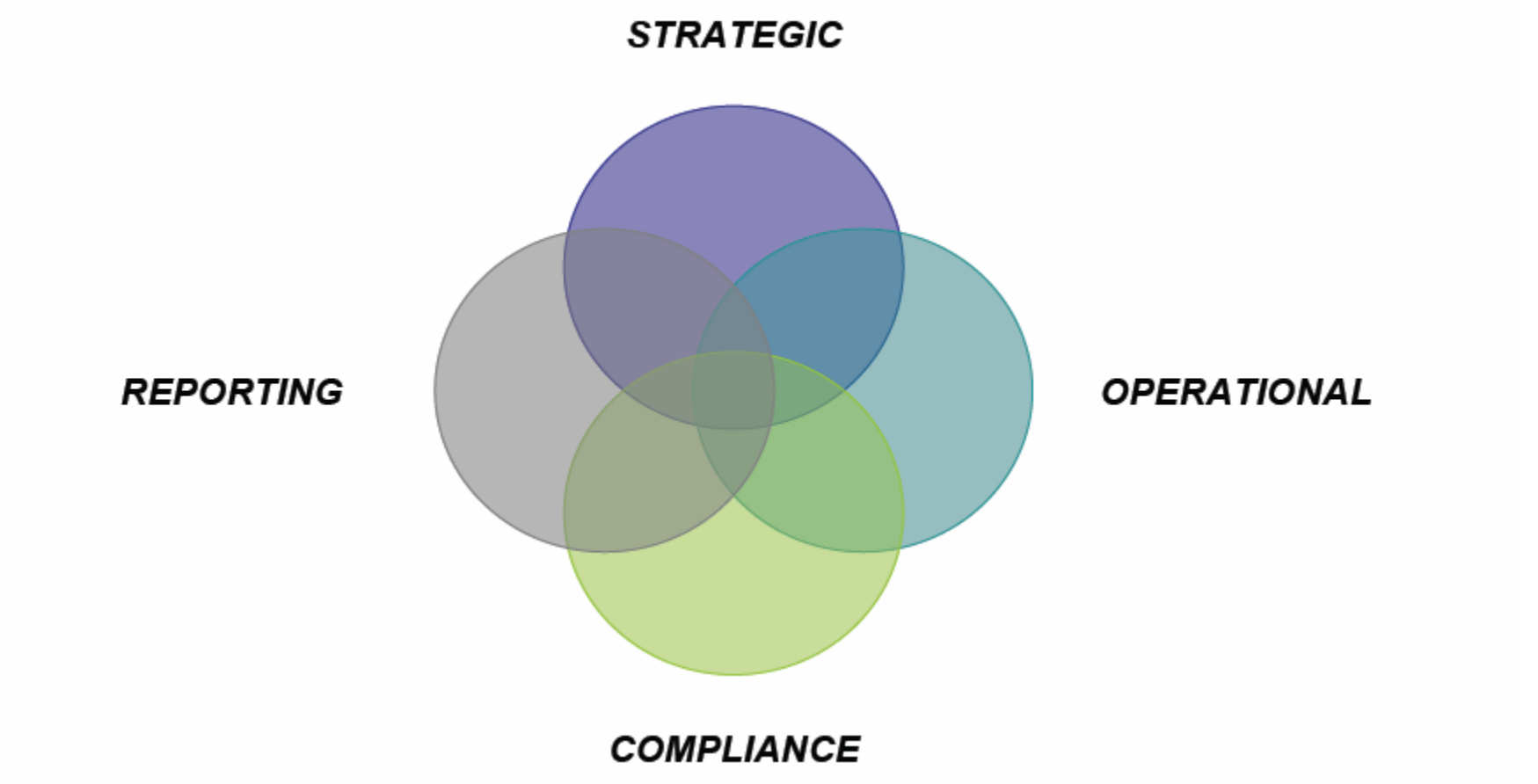
- There is a direct relationship between objectives, which are what an entity strives to achieve, and enterprise risk management components, which represent what is needed to achieve them.
- The relationship is depicted in a three-dimensional matrix, in the form of a cube.

The four objectives categories – strategic, operations, reporting, and compliance – are represented by the vertical columns, the eight components by horizontal rows, and an entity's units by the third dimension. This depiction portrays the ability to focus on the entirety of an entity's enterprise risk management, or by objectives category, component, entity unit, or any subset thereof.



Seeking Opportunity –Top-Down Risk Assessment

COSO ERM Identifies on Four Broad, Overlapping Objective Categories



Aligning Opportunity –Bottom-Up Risk Assessment

In Practice it is Essential to Identify Specific End Result Objectives

- Product Quality
- Customer Service
- Minimizing Unnecessary Costs
- Revenue/Profit Maximization
- Reliable Business Information
- Asset Safeguarding
- Safety
- Regulatory Compliance
- Fraud Prevention/Detection
- Continuity of Operations
- Unintentional Risk Exposure
- Internal Compliance
- External Financial Disclosures

iWaves
evolve innovate grow

ERM: Aligning Opportunities

ERM Should Align and Focus on Existing Key Corporate Objectives and New Opportunities

Business Unit A	*Importance*		*Performance Status*
	Work Unit	*Corporate*	
1.Product Quality (PQ)	H	H	Exceeds
1.Minimize Unnecessary Cost	H	L	Underperforms
1.Reliable Financial Reporting	L	H	Acceptable

Seeking and Aligning Opportunity -Benefits

- Opportunities Will Appear as:
  - "Gaps" in the objective template
    - Are revenue maximization objectives missing?
    - Do cost centers rate cost minimization importance low?
  - Unacceptable performance
    - Is performance low on high rated corporate objectives?
    - Is performance above target in low rated corporate objectives?
  - Misaligned objectives
    - Is there misalignment in importance between business units and corporate?
    - Do business units see opportunity where corporate does not?
- Never Underestimate the Knowledge Work Groups Have About Their Objectives and How They Align with Corporate Goals

Roles and Responsibilities

- Everyone in an entity has some responsibility for enterprise risk management.
- The chief executive officer is ultimately responsible and should assume ownership.
- Other managers support the entity's risk management philosophy, promote compliance with its
  - risk appetite, and
  - manage risks within their spheres of responsibility consistent with risk tolerances.
  - A risk officer, financial officer, internal auditor, and others usually have key support responsibilities.
  - Other entity personnel are responsible for executing enterprise risk management in accordance with established directives and protocols.
  - The board of directors provides important oversight to enterprise risk management, and is aware of and concurs with the entity's risk appetite.

Roles and Responsibilities

- *Board of Directors* – The board should discuss with senior management the state of the entity's enterprise risk management and provide oversight as needed. The board should ensure it is apprised of the most significant risks, along with actions management is taking and how it is ensuring effective enterprise risk management. The board should consider seeking input from internal auditors, external auditors, and others.
- *Senior Management* – This study suggests that the chief executive assess the organization's enterprise risk management capabilities. In one approach, the chief executive brings together business unit heads and key functional staff to discuss an initial assessment of enterprise risk management capabilities and effectiveness. Whatever its form, an initial assessment should determine whether there is a need for, and how to proceed with, a broader, more in-depth evaluation.

Roles and Responsibilities

- ***Other Entity Personnel*** – Managers and other personnel should consider how they are conducting their responsibilities in light of this framework and discuss with more senior personnel ideas for strengthening enterprise risk management. Internal auditors should consider the breadth of their focus on enterprise risk management.
- ***Regulators*** – This framework can promote a shared view of enterprise risk management, including what it can do and its limitations. Regulators may refer to this framework in establishing expectations, whether by rule or guidance or in conducting examinations, for entities they oversee
- ***Professional Organizations*** – Rule-making and other professional organizations providing guidance on financial management, auditing, and related topics should consider their standards and guidance in light of this framework. To the extent diversity in concepts and terminology is eliminated, all parties benefit.
- ***Educators*** – This framework might be the subject of academic research and analysis, to see where future enhancements can be made. With the presumption that this report becomes accepted as a common ground for understanding, its concepts and terms should find their way into university curricula.

ERM: Ranking the Opportunities

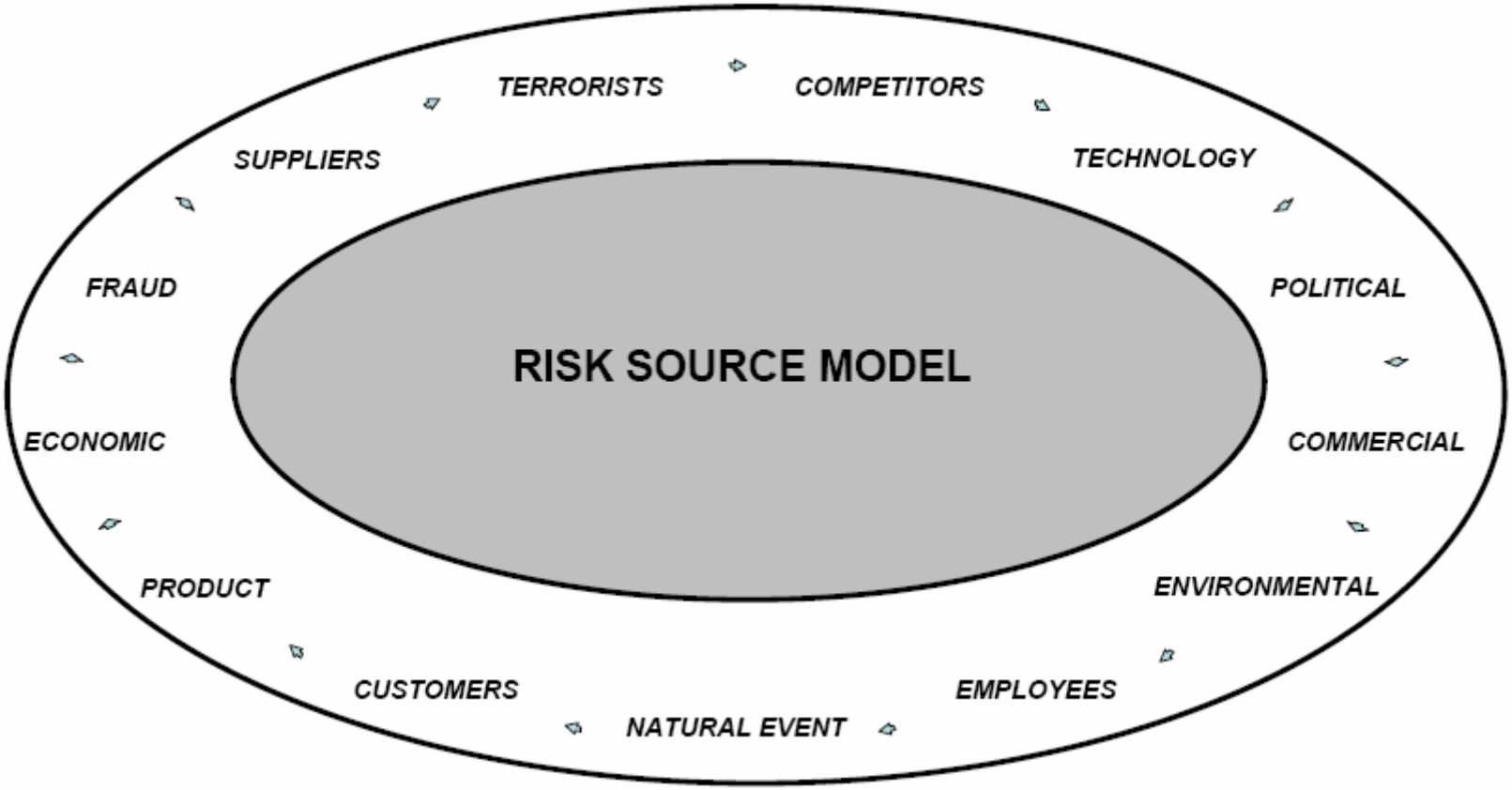
Event Identification –Exactly What is a Risk?

RISK CAUSE/ISSUE	RISK EVENT	CONSEQUENCE
BROKEN SHOELACE	TRIP AND FALL	SPRAINED WRIST
INSUFFICIENT STAFF	PRODUCTION TARGETS AND DEADLINES MISSED	CUSTOMERS INVOKE PENALTY CLAUSE

Significant Risk Management Effort Has Been Spent Fixing “Broken Shoelaces. ”Does Fixing the Shoelace Solve the Problem?

Issues and Action plans dashboard

Risk Models Help Ensure All Types of Risks are Considered



Risk Models Must be Event-Based to be Useful For ERM

ERM: Ranking the Opportunities

- Benefits of Complete Risk Identification
  - Ensures all objectives are identified and prioritized
    - If missed production deadlines are a risk, ensure an objective exists to meet the deadlines
  - Consider all possible solutions
    - Is outsourcing a better solution for production problems than hiring
  - Drive improved business performance
    - Understand and assess cause effect relationships
  - Better resource allocation
    - Factor real risk into budgets and plans

ERM –Allocating Resources

- **Risk Assessment**: Risks are analyzed, considering likelihood and impact, as a basis for determining how they should be managed. Risks are assessed on an inherent and a residual basis
  - **Inherent Risk:** The risk to an entity in the absence of any actions management might take to alter either the risks impact or likelihood (COSO ERM)
  - **Residual Risk:** The risk to an entity after taking into account the impact of the risk response

ERM –Allocating Resources

Standard Qualitative Risk Tables are Used to Assess Inherent and Residual Risk

Significance						
	Extreme 5	Significant	Major	High	Severe	Severe
	Very High 4	Moderate	Significant	Major	High	Severe
	Medium 3	Low	Moderate	Significant	Major	High
	Low 2	Trivial	Low	Moderate	Significant	Major
	Negligible 1	Trivial	Trivial	Low	Moderate	Significant
		Rare 1	Unlikely 2	Moderate 3	Likely 4	Almost Certain 5
				Likelihood		

Consistent Assessment of Risk Across the Entity is Critical

ERM: Allocating Resources

Benefits of Consistent Risk Assessment

- Focus Resources on Significant Inherent Risk
  - What are the top risks that could have a significant impact on the entity's critical business objectives?
  - Can the inherent risk be quantified?
  - Will quantification add credibility?
  - Have we considered the risk in the planning and resource allocation process?

- Focus Resources on Critical Risk Response
  - Where do we believe we have sound risk response measures in place? (e.g. high inherent/low residual risk)
  - Have we allocated resources to ensure those risk responses are effective?
  - What is the cost of our risk response?

ERM: Linking to Business Processes

- Selecting a Risk Response -Making Conscious Choices

  - **Avoid: Is** there a business/region/product we should exit? Can we outperform competitors?
  - **Reduce:** Can we gain unique competitive advantage with the right strategy? Are there compelling reasons to reduce the risk?
  - **Accept:** Is the risk reward equation balanced now? Is risk acceptance a sound economic strategy? How high is residual risk?
  - **Share:** Is it there a business case for sharing or financing a risk, e.g. hedging or other contractual tactics? Are we sharing risks we should not be sharing?

ERM: Linking to Business Processes

- Benefits of Careful Risk Response
  - Cost reduction
    - Link response strategy to budget -don't allocate resources if there is no significant inherent risk
    - Compare the cost of risk reduction to risk sharing
  - Focus on value-adding opportunities
    - Focus resources on strategic objectives where value is added
    - Aim for low cost compliance strategies –achieve compliance but optimize cost of control/mitigation
  - Look for business process performance improvement
    - Will risk response improve process performance

Business Benefits of ERM

- Provide the assurance that enables companies to take more controlled risks and manage uncertainty more effectively
- Gain understanding of risk appetite and consistent measures of risk
- Align risk appetite with strategic objectives and capital needs
- Capitalize on understanding risk from the top down
- Identify, quantify and manage cross enterprise risks
- Potential to provide competitive advantage

Building Blocks for ERM

ERM Context	ERM Objectives	ERM Risks	Business Ops Processes
2007 US Operations	Increase Sales by 15%	Competition	Procurement
	Minimize Unnecessary Costs	Control Design	Manufacturing Flow Mgt
	Reduce Customer Churn 10%	Environmental Liability	Customer Relationship Mgt

7 Steps to Implementing ERM

- 1. Define “key" contexts for ERM

  a) Critical BUs, regions, LOB, processes
  b) Assess criticality and current performance
  c) Where are our strengths? Where must we improve? Where are the opportunities?

- 2. Start with top-down, risk identification in critical “contexts”

- a) Use participative processes to identify risks (via facilitated sessions or surveys)
- b) Use a risk model, industry experience, etc.
- c) No “broken shoelaces”

Steps to Implementing ERM

3. Rank risks by severity
   a) Assess significance and likelihood (Inherent/Target/Residual)
   b) Use a standard risk model
   c) Are you spending resources in the “green zone”

4. Develop strategies and objectives from risks
   a) Significant risks should become opportunities/objectives. (e.g. of high cost is a risk, an objective must be directed at high cost risk)
   b) Look for opportunities
   c) Align objectives horizontally and vertically across the entity

Steps to Implementing ERM

5. Link to business processes
   a) Identify key business processes supporting critical objectives
   b) Conduct process level risk identification and assessment

6. Develop risk response for
   a) Avoid
   b) Transfer
   c) Accept
   d) Reduce

7. Develop performance measures, KPIs
   a) Assign accountability
   b) Track incidents/performance and audit results

iWaves
evolve innovate grow

Case Study

Company Profile:

Quintiles Transnational Corp. Quintiles Transnational Corp. aims to power the next generation of healthcare by providing a broad range of services in drug development, financial partnering and commercialization for the pharmaceutical, biotechnology and health-care industries.

From its headquarters in Research Triangle Park, North Carolina, Quintiles oversees more than 19,000 employees in over 50 countries. The privately held company operates three major groups.

Quintiles' product development division provides a full range of services, from early development through late-phase trials, aimed at regulatory approval and post-launch research and consulting on product safety and value.

Innovex, Quintiles' commercialization group, is responsible for sales-force and medical communications services, including the promotion of physician education.

And the company's NovaQuest strategic solutions help pharmaceutical and biotech firms optimize their portfolio development, company growth and profits through a range of tailored partnering and financial options.

Case Study – Challenges

- Quintiles left behind the many regulatory filing requirements demanded under the Sarbanes-Oxley Act of 2002 when the company decided to go private in 2003, and then eliminated its public debt a year and a half ago. But the compliance systems and infrastructure that Quintiles had built proved too valuable to dismantle because they helped the company identify areas in which it could improve operations. Thus Quintiles, on the recommendation of its audit committee, kept the compliance processes and systems in place to bolster the company's corporate governance, allow it to monitor and maintain financial and operational controls, and ensure the accuracy and validity of its financial statements.

Case Study

- “Once a company’s culture has accepted the requirements and accountability of a compliance structure, it’s much easier to continue and improve upon such culture instead of dismantling it only to reestablish it at a later point and time,” said Karl Deonanan, Executive Director, Finance for Quintiles. “At the end of the day, we benefit from a level of comfort derived from the local level up through the consolidated level and thus, our compliance program is an effective support mechanism for our executive team and finance colleagues around the world.” The company’s initial compliance tool was very rigid and did not offer all of the functionality Quintiles desired. When the compliance software vendor was sold and product support eliminated, Quintiles decided to investigate the many new solutions that had emerged following their implementation of Sarbanes-Oxley.

The Solution

- **The Solution**
  - Quintiles' approach was to cast a wide net in its search for potential compliance software vendors.
  - The company wanted vendors, and their products, to perform in several categories, including: reporting capabilities, security, performance and data storage, and training and support.
  - Quintiles also wanted a system that could easily transfer data from its existing system to the new one, and allow them to customize the way the information is organized.
  - Our comprehensive solution provided Quintiles the complete solution it was looking for with a robust reporting feature that was both flexible and customizable.
  - Users are enabled to grab any data component, extract it into a customizable report from a range of standard software such as Microsoft Excel® or Word®, and manipulate the information as needed.

Seven Steps to Effective ERM

- **INTRODUCTION**

  Managing enterprise risk in a consistent, efficient, sustainable manner has become a critical boardroom priority as CEOs, CFOs and other members of the senior leadership team face unprecedented levels of business complexity changing geopolitical threats, new regulations and legislation, and increasing shareholder demands.

The recognition that business success depends on striking a balance between enhancing profits and managing risk and the investment in the discipline of enterprise risk management is now top of mind for most business leaders

Defining ERM

Enterprise risk management is sometimes viewed as a way of aggregating managing and reporting on all of the risks facing an organization – a way to consolidate the information within the individual risk silos. That is a necessary and desirable goal, but it is not specifically enterprise risk management. While there are many different definitions of enterprise risk management, many organizations have standardized on the definition outlined in COSO's *Enterprise Risk Management—Integrated Framework,* published in 2004.

Enterprise risk management is defined by COSO as a process designed to:

- Identify potential events that may affect the organization
- Manage risk to be within the organization's risk appetite
- Provide reasonable assurance regarding the achievement of the organisation's objectives organization's objectives

COSO definition

The COSO definition goes on to outline eight interrelated components of enterprise risk management. These disciplines are derived from the way management runs an enterprise and are integrated with the management process. These components are:

- **Internal Environment:** The internal environment encompasses the tone of an organization, and sets the basis for how risk is viewed and addressed by an organization's people, including risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate.
- **Objective Setting:** Objectives must exist before management can identify potential events affecting their achievement. Enterprise risk management ensures that management has in place a process to set objectives and that the chosen objectives support and align with the organization's mission and are consistent with its risk appetite.
- **Event Identification:** Internal and external events affecting achievement of an organization's objectives must be identified, distinguishing between risks and opportunities. Opportunities are channeled back to management's strategy or objective-setting processes.

COSO definition

- **Risk Assessment:** Risks are analyzed, considering likelihood and impact, as a basis for determining how they should be managed. Risks are assessed on an inherent and a residual basis.
- **Risk Response:** Management selects risk responses – avoiding, accepting, reducing or sharing risk – developing a set of actions to align risks with the entity's risk tolerances and risk appetite.
- **Control Activities:** Policies and procedures are established and implemented to help ensure the risk responses are effectively carried out.
- **Information and Communication:** Relevant information is identified, captured, and communicated in a form and timeframe that enable people to carry out their responsibilities. Effective communication also occurs in a broader sense, flowing down, across, and up the entity.
- **Monitoring:** The entirety of enterprise risk management is monitored and modifications are made as necessary. Monitoring is accomplished through ongoing management activities, separate evaluations, or both.

In practice, enterprise risk management is not strictly a serial process, where one component affects only the next. It is a multidirectional, iterative process in which almost any component can and does influence another.

IF IT'S SO GOOD WHY ISN'T EVERYONE DOING IT?

- Enterprise risk management has been promoted for years as an important activity. Boards insist they want more information on enterprise risk, but examples of successful enterprise risk management implementations, sustained over time, and across all business functions, are elusive. The problem with most risk management initiatives to date is that they have been conducted primarily in silos and usually for defensive purposes. While they may, at best, have identified hazards, prevented value erosion and reduced compliance violations, they have seldom added real economic value. Value is added by seeking and exploiting opportunities and improving business performance.
- Many organizations found it difficult to create a solid business case for enterprise risk management, in part due to the difficulties of quantifying the full range of benefits. According to the study, "...only 13% of executives said that their firms quantify ERM costs and just 4% said they quantify ERM value." An estimate of the human resources, technology and corporate energy investment required to fully implement risk management across an organization is elusive.
- Most business cases for comprehensive risk management focus on cost savings and efficiencies and fail to make a compelling case for adding value. By just focusing risk management on these traditional areas, practitioners ignore about half of the organization's potential uncertainties. Unfortunately these are the uncertainties with a positive impact – the value adding exploitable

FROM RISK TO OPPORTUNITY

- Enterprise risk management must focus on risks and opportunities at the strategic level. The strategic risks that companies face can be classified into seven broad categories.

STRATEGIC RISK	COUNTERMEASURE
Industry margin squeeze	Shift the compete/collaborate ratio (Seek collaboration opportunities – sharing back office functions, co-production, asset sharing etc.)
Technology shift	Double bet (Invest in two or more versions of a technology simultaneously).
Brand erosion	Redefine the scope of brand investment Reallocate brand investment
One of a kind competitor	Create a new, non-overlapping business design (Establish a position in an adjacent space)
Customer priority shift	Create and analyze proprietary information Conduct quick and cheap market experiments
New project failure	Engage in smart sequencing Develop excess options Employ the stepping stone method
Market stagnation	Generate "demand innovation" (Redefining the market by looking at it through the lens of customer economics)

FROM RISK TO OPPORTUNITY

- Within the existing silos of risk management in an entity, such as audit, compliance, IT governance and financial management, the concept of risks as threats predominates, and the result is a focus on controls that prevent or minimize the threat. Enterprise risk management must focus on opportunities and provide insight into overcoming obstacles to realizing those opportunities on both a strategic and tactical level.

Seven Steps to Effective Risk Management

Step 1

- **Management's Role**

  Management's role, often executed in a structured workshop setting, is to engage in risk assessment and prioritization through purely qualitative assessment and "gut feel" based on experience.
- Although simpler, the results must stand up to scrutiny from knowledgeable experts and experienced practitioners.
- Qualitative screening of risks is also useful in making an initial assessment of the level of risk. More detailed quantitative analysis may follow.

Step 2 : Establish Context

- Enterprise risk management begins with establishing the context of the risk assessment.
- In the risk management literature, the “context” is commonly

  thought of as the
  - opportunity,
  - strategy,
  - outcome or
  - process

  on which stakeholders want formal analysis and assurance.

What have standards to say

- AS/NZS 4360: 2004, a widely accepted risk management standard published by Standards Australia, suggests that the strategic context, the organizational context, and the risk management context must all be considered.
- The assessment of the strategic context links the organization's mission and strategic objectives to the management of risks to which it is exposed.
- Defining the risk management context involves setting the scope and boundaries of the risk assessment process, including the time frame and specific project or activity.
- A context could include the entity as a whole, a business unit, a line of business, a geographic area or all of the above.
- The context is the level at which management feels the need to set strategy and assess risk.
- Whatever the context, it will usually be the basis for formal board reporting and will usually include a variety of existing business activities and functions.
- Whatever the context identified for an enterprise risk management assessment, it must be sufficiently important to be visible to the senior officers and the board. Its importance may be due to its current significance or its potential significance.

iWaves
evolve innovate grow

Step 3: Identify and Prioritize

- The goal of risk or event identification is to produce a list of risks or events categorized into each of the seven areas.
- Risks in this context are potential events that, if they occur, will adversely affect the ability of the entity to achieve its objectives.
- By definition, managing risks is necessary to achieve the organization's strategies and objectives.
- The way in which risks are managed will affect the value they add and provide competitive advantage.
- Some events may have a positive impact. These represent opportunities in the struggling airline industry, one of the biggest risks is operating costs and the squeeze on margins. Some independent airlines have turned cost risk to a competitive advantage by minimizing fleet diversity, maximizing aircraft utilization and reducing turnaround times.
- Completeness in risk or event identification is critical. Risks and events left unidentified are excluded from further analysis. Unidentified risks represent unidentified opportunities.
- Strategic risks should be explicitly identified even and some would say especially) if they are apparently outside the control of the entity. For the risks or events identified, management should consider the severity, the probability and the impact of time on the event.

Step 4: Tools of Relevance

- AS/NZS4360 suggests the use of checklists or risk source models to promote consideration of all risks.
- COSO ERM – Integrated Framework suggests a range of event identification techniques ranging from facilitated workshops with senior management to studies of the use of event category tables.
- While quantitative approaches to risk assessment are attractive for their apparent precision, the variables involved in enterprise risk management are seldom sufficiently accurate.
- Qualitative risk tables are often used to provide a consistent assessment of severity and probability.

Step 5 : Look at the End Result

- Consider the potential positive outcomes from events and the impact of risks that do not occur. enterprise risk management should add value at the strategic level and the value must come from strategic decisions based on a careful analysis of and response to risks and events.

Step 6 : Evaluate existing processes

- Enterprise risk assessment identifies areas where management systems and processes are required to support the achievement of objectives.
- Linking enterprise risks to the processes or systems that support the management of those risks creates alignment within the organization.

  For example, fast growing technology companies may identify delays in product development or poor product quality as significant risk areas.
- Enterprise risk management connects these risks with the actual processes or organization elements that are accountable for new product development and product quality.
- The significance of those processes or divisions is then understood and managed in the context of the enterprise risk identified. The value adding potential from timely product development and product quality initiatives are maximized.
- Conversely, if an assessment of enterprise risk identifies a gap in the management framework, that gap can be addressed more quickly and effectively.
- Enterprise risk management may identify raw material shortages as a significant risk. As a result, the company may choose to put processes in place to hedge against future price increases, to seek alternative sources of supply or to redesign products to consume less of the scarce resource.
- Finally, enterprise risk management will identify business processes and locations whose value to the business is low or indirect.

Step 7: Link ERM to GRC

- Enterprise risk management sits above the elements of integrated governance, risk and compliance but must be linked to them.
- The common denominator linking enterprise risk management with existing risk silos is the risk-based approach established in the enterprise risk management initiative, including the language, tools and technology for storing and managing the information produced.
- The organization should have one single framework for managing risk and a common language and tools for implementation across the organization.
- Effective operational risk management ensures the tactics necessary to support the strategies are in place and functioning at an acceptable level of risk. Operational risk management focuses on the reliable performance of processes deemed critical to strategy.
- Compliance programs are essential to operate within management's discretionary boundaries and the law. More than ever before, business is expected to operate within the boundaries of safety, environmental, supply chain and consumer protection laws that change from one jurisdiction to another.
- Financial control management provides assurance that the information management uses to run the business and report to stakeholders is reliable. Stakeholders rely on complete, accurate and timely financial reporting and failures can have an immediate and negative impact on value.
- IT governance provides assurance that the technology management relies upon is operating effectively and reliably. Information technology is more than a source of cost savings; it is a source of strategic advantage. Sound IT governance practices are essential to achieving strategic goals.
- Audit is an essential element of GRC, and provides assurance and recommendations to management and the board. Audit is relied upon to ensure all the pieces of GRC are working together effectively.

ENTERPRISE RISK MANAGEMENT – ITS TIME HAS COME

One study by Mercer Management Consulting found that 10 percent of the Fortune 1000 lost 25 percent of their value within a one month period. Another study, by Booz Allen Hamilton, suggested that of 1,200 firms with market capitalizations greater than $1 billion, the primary events triggering the loss of shareholder value were strategic and operational failures.

The evidence is compelling that strategic failure can cause enormous, irreversible and sometimes sudden value loss.

Are these losses predictable and avoidable? Can strategy be made more resilient by enterprise risk management? Clearly, many companies do avoid strategic failure and thrive in adverse circumstances.

Proving that enterprise risk management will prevent or mitigate strategic failure may be difficult. But the tools for implementing enterprise risk management are readily available, implementation is not complex and the cost is not high compared to the cost of failure. It is easier to argue that the time has come when enterprise risk management should be a standard management practice.

Effectiveness

- Determining whether an entity's enterprise risk management is "effective" is a judgment resulting from an assessment of whether the eight components are present and functioning effectively. Thus, the components are also criteria for effective enterprise risk management. For the components to be present and functioning properly there can be no material weaknesses, and risk needs to have been brought within the entity's risk appetite.
- When enterprise risk management is determined to be effective in each of the four categories of objectives, respectively, the board of directors and management have reasonable assurance that they understand the extent to which the entity's strategic and operations objectives are being achieved, and that the entity's reporting is reliable and applicable laws and regulations are being complied with. The eight components will not function identically in every entity. Application in small and mid-size entities, for example, may be less formal and less structured. Nonetheless, small entities still can have effective enterprise risk management, as long as each of the components is present and functioning properly.

Limitations

While enterprise risk management provides important benefits, limitations exist.

In addition to factors discussed above, limitations result from the realities that human judgment in decision making can be faulty, decisions on responding to risk and establishing controls need to consider the relative costs and benefits, breakdowns can occur because of human failures such as simple errors or mistakes, controls can be circumvented by collusion of two or more people, and management has the ability to override enterprise risk management decisions.

These limitations preclude a board and management from having absolute assurance as to achievement of the entity's objectives.

Encompasses Internal Control

- Internal control is an integral part of enterprise risk management. This enterprise risk management framework encompasses internal control, forming a more robust conceptualization and tool for management. Internal control is defined and described in
- *Internal Control – Integrated Framework*. Because that framework has stood the test of time and is the basis for existing rules, regulations, and laws, that document remains in place as the definition of and framework for internal control. While only portions of the text of *Internal*
- *Control – Integrated Framework* are reproduced in this framework, the entirety of that framework is incorporated by reference into this one.

Thank you

For more details contact us on

KN Bhat
knbhat@infowavesindia.com

Tel - 91 22 6636 6575
Mobile - 91 98922 07296 / 91 99672 19323

http://www.infowavesindia.com

Mumbai | Delhi | Poona | Bangalore | Chennai | UAE | USA