



Deloitte.

The Risk Intelligent Internal Auditor

Presented to the ECIIA

Eric Hespenheide

Rick Funston

September, 2006

This presentation is incomplete without the accompanying discussion

Audit. Tax. Consulting. Financial Advisory.

Outline

- Why is risk management such a hot topic?
- What is wrong with risk?
- The value proposition for improving risk intelligence
- The evolution of risk assessment
- A new paradigm for risk assessment
- The implications for the enterprise and internal audit

Where Would We Be Without Risk?

- How many of your jobs depend on risk?
- How many of your companies would prosper if they didn't take risk?

"A ship is safe in a harbor - but that's not what ships are for." **John A. Shedd**

Why Is Risk Management Such a Hot Topic?

- **Unanticipated Losses**

- Stakeholder activism
- Changes in customer preferences
- Commodity price spikes
- Adverse changes to laws and regulations
- Cyber security & privacy protection
- Business discontinuities / supplier disruptions
- Technology obsolescence
- Failed acquisitions

- **Regulation**

- NYSE listing requirements
- Sarbanes-Oxley assertions
- SEC reporting requirements
- Federal sentencing guidelines
- Kontra G
- Turnbull
- King
- Euronext
- Basle

- **Market Expectations**

- Shareholder activism
- Increased pressure by rating agencies

- **Public Image**

- Highly visible litigation
- Growing media attention
- Company reputation risks
- Executive compensation

- **Corporate Governance**

- Board and Audit Committee responsibilities
- Executive Management responsibilities
- External risk reporting responsibilities

The Role of the Audit Committee

NYSE Listing Requirement

- *"While it is the job of the CEO and senior management to **assess and manage the company's exposure to risk**, the audit committee must discuss guidelines and policies to govern the process by which this is handled."*
- *The audit committee should discuss the **company's major financial risk exposures and the steps management has taken to monitor and control such exposures.***

Major Financial Risk Exposure

"It seems reasonable that the risk factors you disclose in your financial statements should be included in the risk analysis."

Janice O'Neill
Senior Vice President Corporate Compliance
New York Stock Exchange
March 16, 2006

Rating Agency ERM Criteria

Moody's

- Risk Governance
- Risk Management
- Risk Analysis & Quantification
- Risk Infrastructure & Risk Intelligence

Standard & Poor

- Policies
 - Governance & Risk Culture
 - Risk Appetite & Strategy
 - Risk Control
 - Risk Disclosure
- Methodology
 - Valuation Techniques
 - Model Vetting & Back Testing
- Infrastructure
 - Risk Architecture
 - Operations

What is Risk?

- Risk is the potential for loss of value or the sub-optimization of gain
- Risk may be caused by an event (or series of events) that can adversely affect the achievement of your objectives.
- The objectives of the enterprise are to:
 - protect the value of its existing assets
 - create new or future value.

What's Wrong With Risk?

Two Schools of Thought

- Risk taking is bad and needs to be avoided
- Risk taking is good and needs to be managed

Value Preservation

The market severely punishes failure to **protect existing assets** (some risks are bad)

- Traditional domain of risk management
- Bottom-up and focused on operations, reporting and compliance
- Vast majority of current risk specializations focus on risks to existing assets yet do so in isolation
- Traditional risk assessment is probabilistic and quantitative
 - does not typically address risk at the extremes
- Unrewarded risk i.e., no premium for taking these kinds of risks when compared to the severity of the punishment when detected

Value Creation

The market rewards the ability to **create and sustain future growth** (some risks may be good)

- The new domain is managing risks to future growth
- Without risk, there is no reward. This is the basis of capitalism i.e., putting capital at risk and making profitable bets.
- Better understanding the profitability of big bets, risks to success and how to overcome them
- Probabilities don't apply
- Top down focus on mission critical risks to strategy and execution
- Rewarded risk-taking i.e., company can receive a premium for successfully taking and managing risks associated with new products, new markets, new business models, alliances, acquisitions etc.

10 Most Frequently Publicly Disclosed Risks*

Grow

Protect

Rank	Disclosed Risk	Frequency
1	Economic Conditions / Trends	294
2	Adverse Legal / Regulatory / Environmental Changes	288
3	Competitors & Competitive Actions	281
4	Business Interruption (e.g., supply Interruption and Natural Disasters/Severe Weather	277
5	Litigation / Intellectual Capital Issues	213
6	M&A Strategy / Execution / Integration	192
7	Political Stability / Country Risk	189
8	Unanticipated changes in Consumer Demands/Preferences	187
9	Inability to Develop / Market New Products	156
10	Terrorist Activities / War / Civil Unrest	149

*Unpublished research of 10Q, 10K and 20F's Deloitte 2005

What is your organization's current level of "shock resistance" to these kinds of risks?

Understanding Risks to Value

Management is responsible for creating and preserving value in the enterprise

- 1. How can the enterprise fail to achieve its value objectives?**
- 2. What would cause the enterprise to fail?**
- 3. What would be the effects of the failure?**
- 4. What is currently being done to prevent, detect, correct or escalate such failure?**
- 5. What is our vulnerability to such failure?**
- 6. What further actions are required to cost-effectively mitigate value at risk?**
- 7. How do we get reasonable assurance existing mitigation is reliable & effective?**

ENTERPRISE VALUE

Revenue Growth

Operating Margin

Asset Efficiency

Expectations

ROOT CAUSES / FAILURE MODES

People

Processes

Systems

External Factors

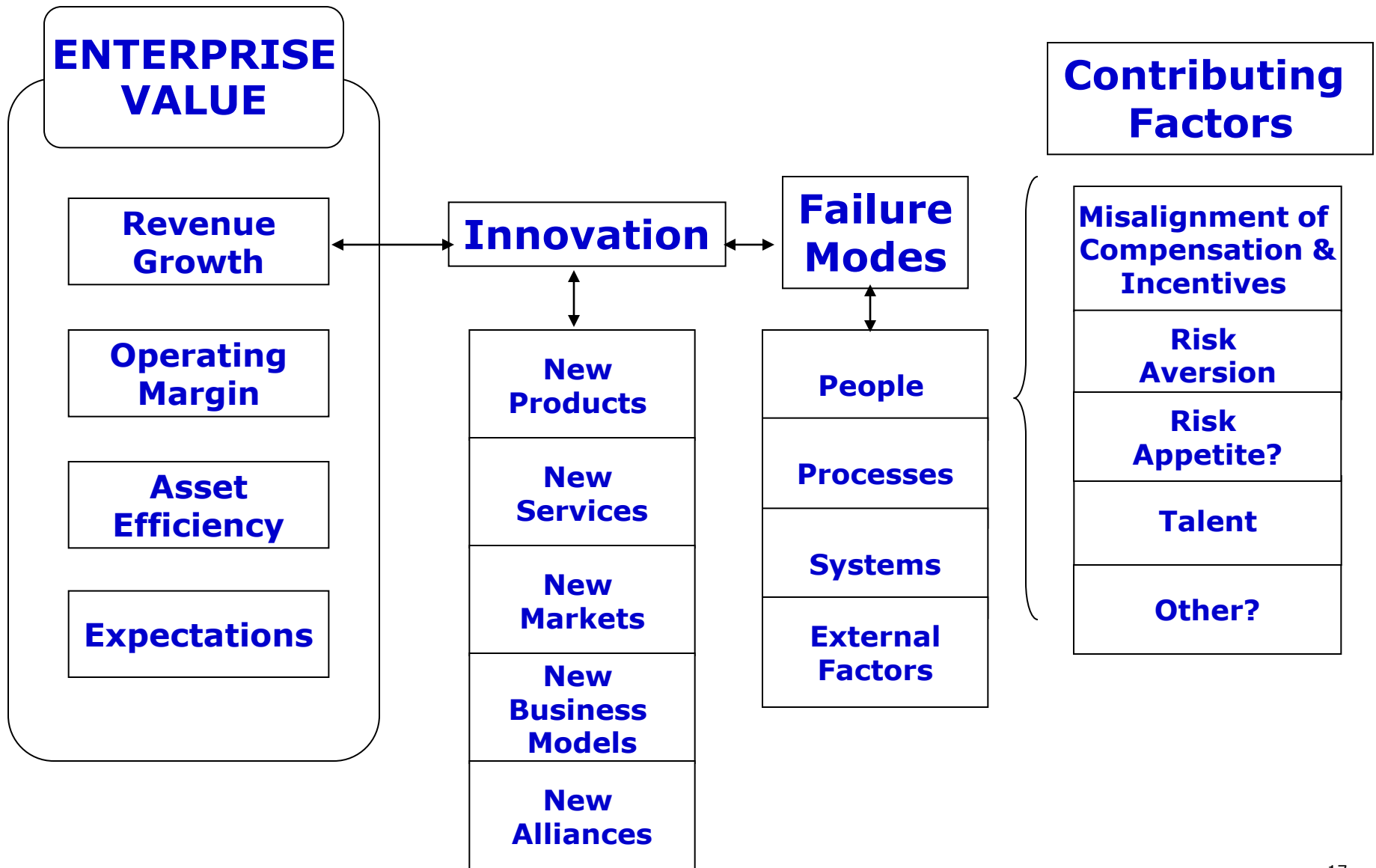
Innovation & Risk Management



When It's Risky –
Complacency Can Kill!!!

But When You Are Very Good at
Managing Risk –
You Can Take More Risk!!!

Innovation & Risk



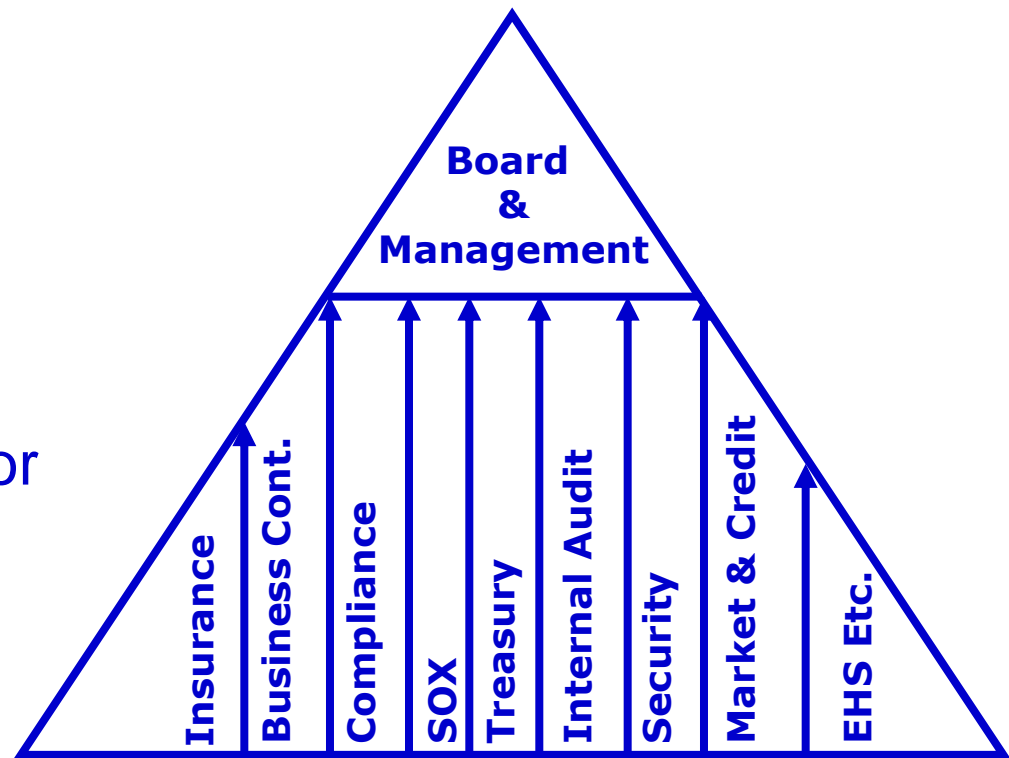
No One is Immune to Value Killers and No One is Perfect

- Almost 50% of global 1000 companies lost 20% or more in share price in less than a month during the past 10 years – some never recovered
- 80% of losses were due to interaction of multiple risks
- Almost all organizations have risk management located in specialist silos
- Most major losses were as the result of a series of high impact but low likelihood events

The Value Killers
Deloitte Research, 2005

Today's Typical Risk Silos

- Deep specialization
- Bottom Up
- Inefficient (no commonality)
- Hard to get portfolio view
- Ineffective response to major value losses that cut across functions
- Focus is on risks to control and existing assets

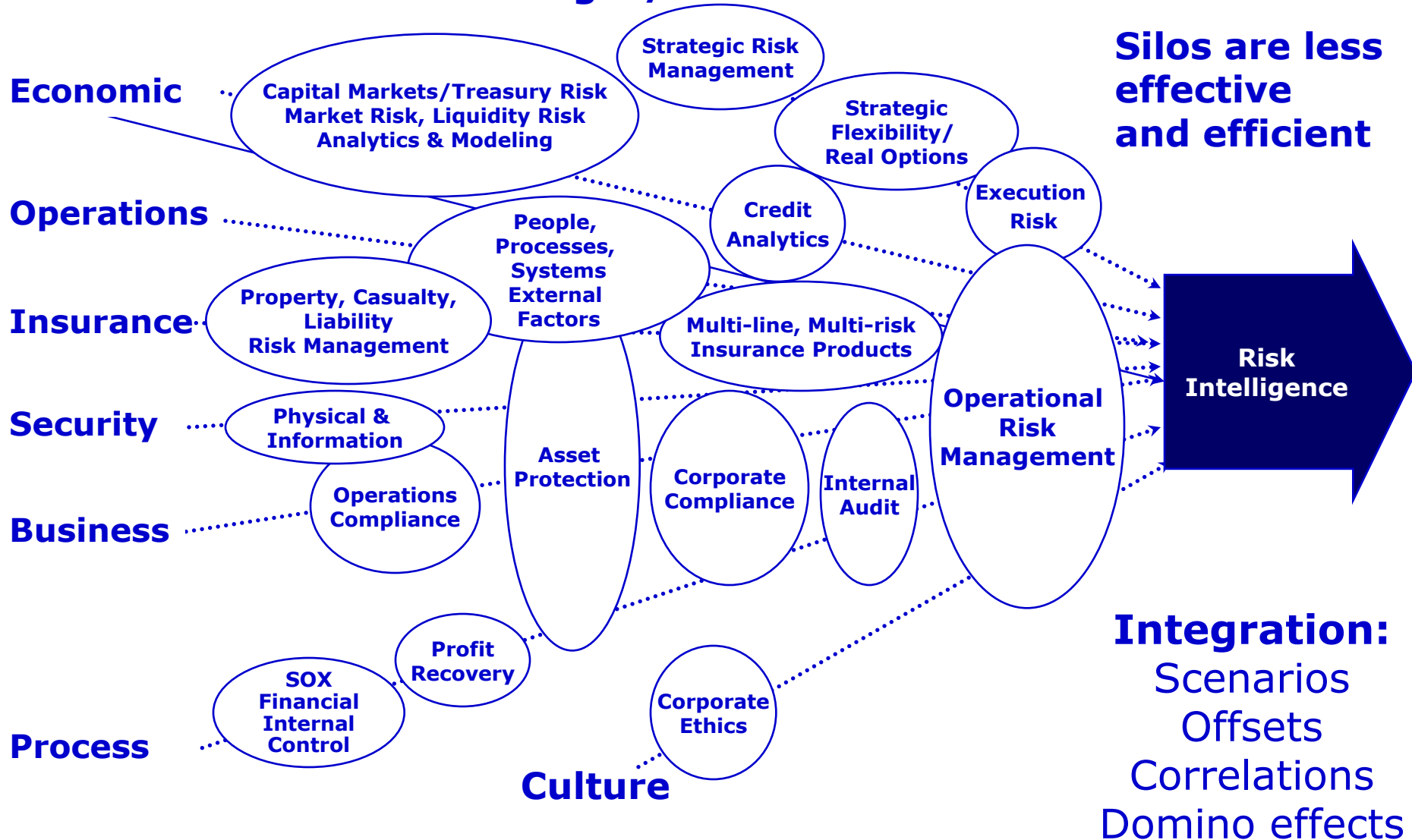


Focus of action is deep specialization within the wider organization

- ~ 20% of benefit from top management effort and implementation
- ~ 80% of benefit from full organizational effort and implementation

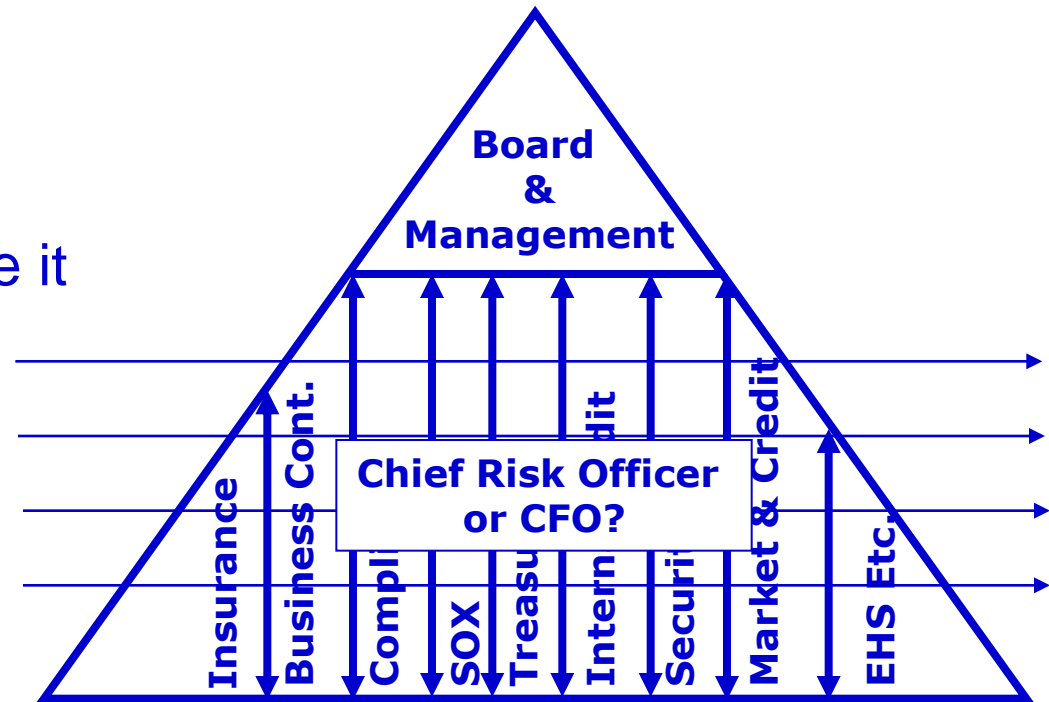
From Silos to Integrated

Strategic / Execution



The Risk Intelligent Enterprise

- Top Down & Bottom Up
- Maintain deep specialization
- Improve cross-functional efficiency (commonality where it makes sense)
- Easier to get portfolio view
- More effective response to major value losses that cut across functions
- Focus is on risks to value (existing assets and future growth)



Focus of action is risks to value, top down & alignment across the risk specializations

~ 20% of effort to get 80% of benefit from top management implementation

Harmonization, Synchronization and Rationalization

1. Harmonize

- Establish common language
- Standardize policies, practices and reports
- Clarify roles and responsibilities (gaps and overlaps)
- Produce a portfolio view to better understand and manage risk interactions
- Improve ability to rely on one another's work

2. Synchronize

- Coordinate cross-functionally for improved anticipation, preparedness, response and recovery
- Coordinate timing of requests for information
- Smooth workload demands

3. Rationalize

- Eliminate gaps / redundant structures, processes & controls
- Reduce / eliminate duplication of effort related to assessment, testing, reporting, etc.
- Reduce burden on the business and related expense growth

What is Risk Intelligence?

Rewarded Risk Taking

All Enterprise Risks

Consistent

Forward-looking

Risks to Value

Gross & Net Risk

Assurance of Mitigated Value

Scenarios

Speed of Onset is Critical Variable

Integrated (Built In)

Risk Management can be Free

Effective & Efficient

Sustainable Capability

**N
O
T

J
U
S
T**

Risk Aversion

Financial Statement Risk

Ad Hoc

Historical

Risks to Control

Impact & Likelihood

Assume Effectiveness

Single Events

Speed is Constant

Bolted On

Increased Costs

Specialist Silos

“One Off” Assessments

The Value Proposition for Improving “Risk Intelligence”

“Brakes actually help cars go faster”

- Enterprises that are most effective and efficient in managing risks to future growth and existing assets will, in the long run, outperform those who are less so.
- Competitive advantage requires calculated risk taking for reward.
- Calculated risk taking and protection of existing assets requires risk intelligence in an uncertain environment.

But Have Our Risk Assessment Models Kept Pace?

The Role of Internal Audit

“Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations.

It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.”

Source: *The International Standards for the Professional Practice of Internal Auditing (Standards)* The Institute of Internal Auditors

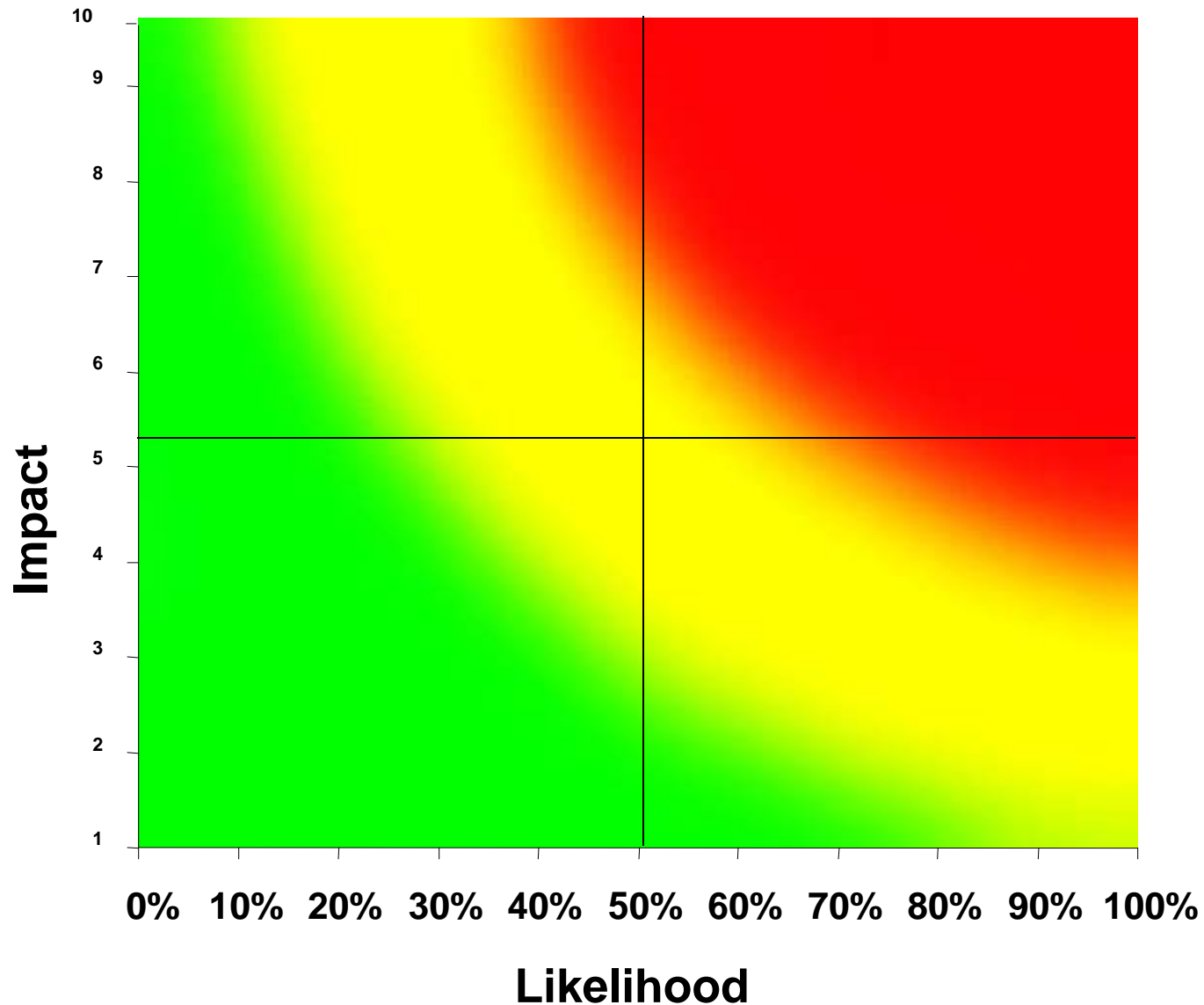
Balancing IA Roles

Internal Audit's Role	Major ERM Activities
<p>Core/Safe – consistent with Standards</p>	<ul style="list-style-type: none"> • Giving assurance on the risk management process
	<ul style="list-style-type: none"> • Giving assurance that risks are correctly evaluated
	<ul style="list-style-type: none"> • Evaluating risk management processes
	<ul style="list-style-type: none"> • Evaluating the reporting of key risks
	<ul style="list-style-type: none"> • Reviewing the management of key risks
<p>Should be performed with certain safeguards</p>	<ul style="list-style-type: none"> • Facilitating identification and evaluation of risks
	<ul style="list-style-type: none"> • Coaching management in responding to risks
	<ul style="list-style-type: none"> • Coordinating ERM activities
	<ul style="list-style-type: none"> • Consolidated reporting on risks
	<ul style="list-style-type: none"> • Championing establishment of ERM
	<ul style="list-style-type: none"> • Developing risk management strategy - BOD approval
<p>Should not be performed by internal audit</p>	<ul style="list-style-type: none"> • Setting risk appetite
	<ul style="list-style-type: none"> • Imposing risk management processes
	<ul style="list-style-type: none"> • Providing management assurance on risks
	<ul style="list-style-type: none"> • Making decisions on risk responses
	<ul style="list-style-type: none"> • Implementing risk responses on management's behalf
	<ul style="list-style-type: none"> • Assuming accountability for risk management

A Quick Self-assessment of Your Current Internal Audit Risk Assessment Model. Do You:

1. Assess primarily risks, entities, processes or systems or all of these?
2. Differentiate between rewarded and unrewarded risk?
3. Assess impact and likelihood?
4. Allocate audit resources to highest impact and most likely risks?
5. Clearly differentiate between inherent and residual risk?
6. Provide assurance on mitigated value?
7. Evaluate inherent and residual risk simultaneously?
8. Address high impact / low likelihood events?
9. Address scenarios and series of events not just individual events?
10. Support harmonization, synchronization and rationalization of risk intelligence?

Impact and Likelihood



Current IA Risk Assessments

Typically:

- Start with a blank sheet of paper
- Audit individual entities, processes and systems
- Audit those with highest impact and probability
- Do not differentiate between inherent & residual risk
- Address risks as separate, unrelated events
- By their nature, audit plans avoid dealing with risks that are outside of their scope
- So what happens to the rest of the risks?

Inherent and Residual Risk

- Inherent (Gross) risk is the risk to an entity in the absence of any actions management might take to alter either the risk's likelihood or impact.
- Residual (Net) risk is the risk that remains after management's response to the risk.
- Risk assessment is applied first to inherent risks. Once risk responses have been developed, management then considers residual risk.
- Effective enterprise risk management requires that risk assessment be done both with respect to inherent risk and also following risk response.

COSO ERM 2004

Probabilistic Modeling

Suitable

Recurring situations

Large body of data

Subject to known rules

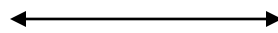
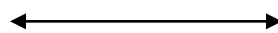
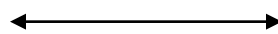
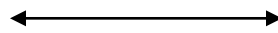
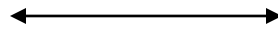
Stable

Patterns Observable

Controllable

Limited range of outcomes

Combinations lead to known results



Unsuitable

Rare/Non-recurring situations

Small body of data

Rules are unknown/forming

Unstable / rapid change

Patterns not readily observable

Uncontrollable (External) Factors

Unlimited range of outcomes

Combinations lead to unknown results

Predictability is a Thing of the Past

“Predictions about the likelihood of multi-causal losses actually depend on sound understanding of cause-and-effect relationships or on a detailed loss history, and the risks of the future have neither of the two.”

Swiss Re “ The Risk Landscape of the Future”

The Fallibility of Probability

- Little or no predictive value
- Major value losses are often high impact / low likelihood

9/11

Dot com bubble

Oil / commodity price spikes

Danish cartoons

1997 Asian Financial crisis

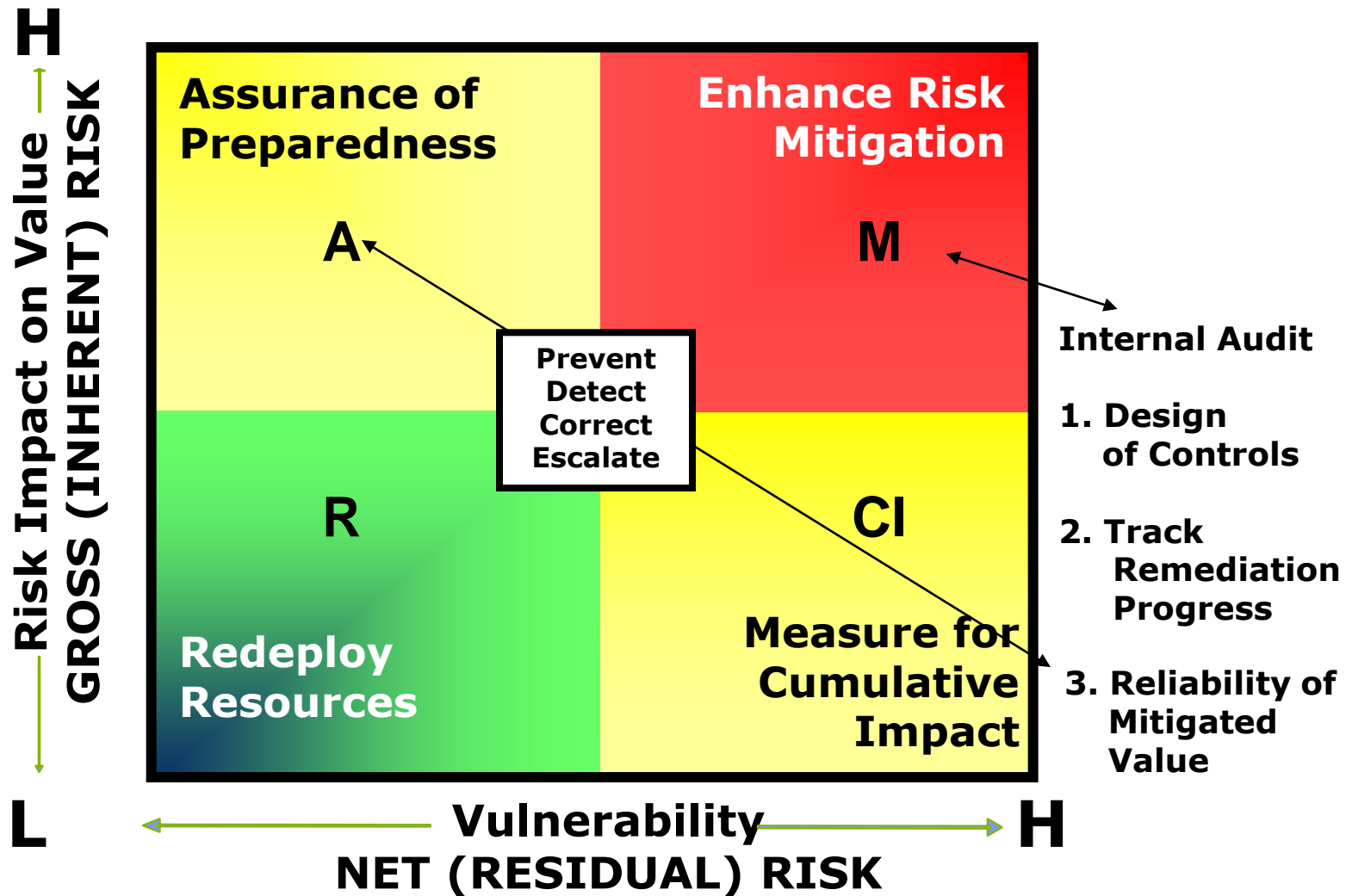
Financial scandals

Natural disasters

???

- Biases management to direct resources to high impact / high likelihood events
- Typically focuses on single events rather than a series of events or domino effects
- Audit activities are often mis-directed to the red zone

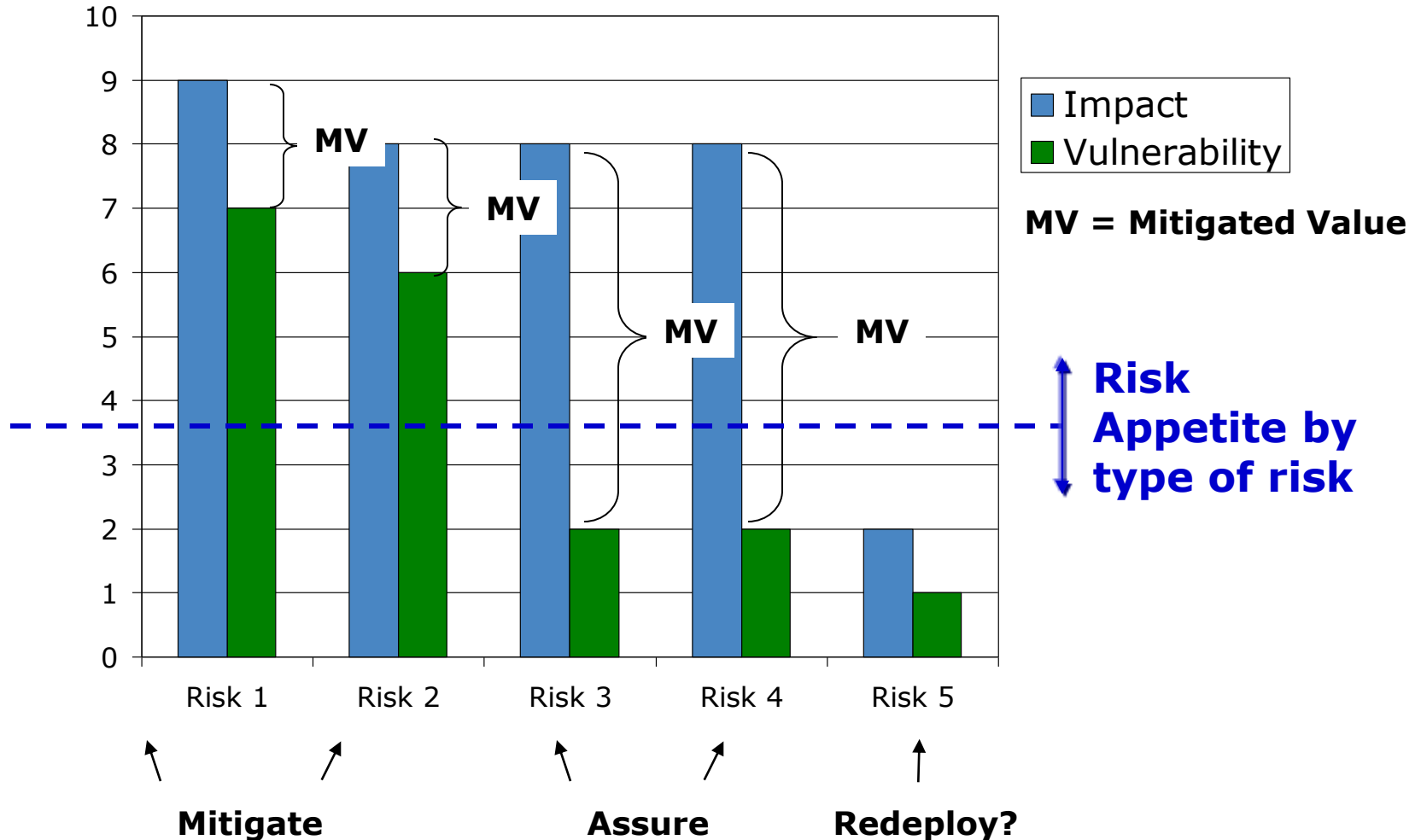
The New Paradigm



Risk Assessment Model

Illustrative

Gross Risk – Net Risk = Mitigated Value



Mitigated Value Example

Gross (Inherent) Risk \$100MM	Mitigated Risk Value \$35MM	RISK MITIGATION <ul style="list-style-type: none"> • Management Reviews • Functional Responsibility • Risk Transfer (Insurance) • Disaster Recovery Plans • Performance Metrics • Inventory Buffer 	ASSURE <ul style="list-style-type: none"> • Assurance Plan prioritized by Mitigated Risk Value • Criticality • Effectiveness and efficiency of mitigated value plan
	Net (Residual) Risk \$65MM	<ul style="list-style-type: none"> • Data Center Vulnerable • Environmental Liability • Contract Penalties • Contract Weaknesses • Market share loss • Reputation loss • Litigation 	MITIGATE <ul style="list-style-type: none"> • Rank by highest value to mitigate down to risk appetite threshold • Assign executive risk owners • Identify most important and controllable improvements • Identify response alternatives • Develop hierarchy of cost of mitigation
\$5MM			REDEPLOY? CUMULATIVE IMPACT?

IMPACT (Gross Risk)

Adapted from the IIA's SIAS Number 9, "Risk Assessment"

- Financial
 - **Asset size, liquidity, or transaction volume.**
 - Cost of prior risk experience (direct hits and near misses)*
- Stakeholders
 - **Impact on customers, suppliers**
- Reputation*
- Legal/Regulatory*
 - **Impact on government regulations**
- Environment, Health and Safety*
- Speed of Onset*

*Deloitte Impact Criteria

Vulnerability (Net Risk)

1. Control Effectiveness (People, Process and Systems)
 - Ethical climate/pressure on management to meet objectives
 - Competence, adequacy, and integrity of personnel
 - Adequacy and effectiveness of the system of internal control
 - Management judgments and accounting estimates
 - Degree of computerized information systems
2. Speed of Response - Detection, Response, Recovery
3. Complexity
 - Complexity or volatility of activities / Geographical dispersion
4. Response to Prior Risk Experience
 - Acceptance of audit findings and corrective action taken
 - Date and results of previous audits
5. Rate of Change (expansion or contraction)
 - Organizational, operational, technological, or economic.
6. External Conditions
 - Competitive conditions / Financial and economic conditions.

Most Vulnerabilities Are Known in Advance

“Before 9/11 the Federal Emergency Management Agency listed the three most catastrophic disasters facing America: a terrorist attack on New York, a major earthquake in San Francisco and a hurricane strike on New Orleans....”

New York Times, Sept. 9, 2005

“95% of all computer vulnerabilities are known in advance.”

Computer Emergency Response Team
Carnegie Mellon

Implications for Internal Audit

1. Audit individual risks, entities, processes and systems in descending order of mitigated value and criticality
2. Audit controls for those risks with highest impact / low vulnerability
3. Differentiate between inherent and residual risk
4. Prioritize based on vulnerabilities not probabilities
5. Give appropriate guidance as to where and what to audit
6. Address what should be done with risks that are outside of the audit scope
7. Address potential interactions among specific risks, entities processes and systems
8. Understand and address scenarios

Implications for Internal Audit

M = High Impact / High Vulnerability

- Provide assistance in design of controls where impact and vulnerability are high
- Track progress on remediation plans

A = High Impact / Low Vulnerability

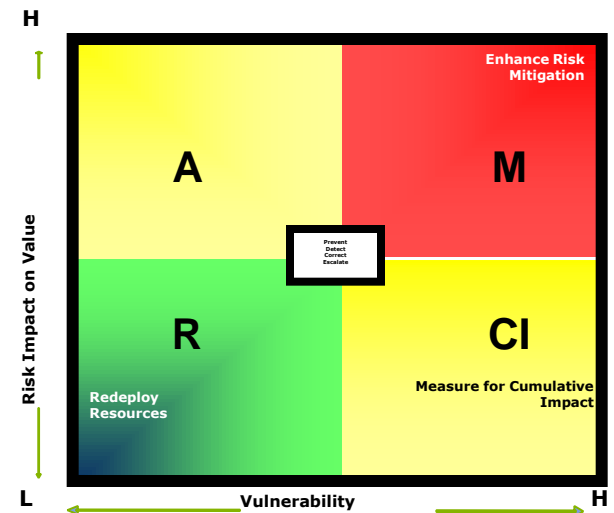
- Obtain assurance confidence in preparedness is justified

R = Low Impact / Low Vulnerability

- Obtain assurance on effectiveness
- Identify ways to improve efficiency

CI = Low Impact / High Vulnerability

- Assess cumulative impacts and frequency



Risk Intelligent Internal Auditor Should:

- Identify risks to value and control
- Assess scenarios and chains of events
- Assess gross and net risk
- Provide assurance on mitigated value
- Factor in speed of onset and response
- Recognize many regulators still use impact and likelihood criteria
 - Resistance can be expected
 - If needed, look at likelihood of residual risk
- Harmonize, synchronize and rationalize risk assessment criteria and processes with other risk assessors where it makes sense
 - Reduce burden on business
 - Improve effectiveness and efficiency

Invitation to Participate in an ERM Benchmark Survey

- Survey launched in April 2005. Over 80 companies have submitted responses, spanning all major industries.
- Recently updated and “evergreen”
- Will provide interim reports to all survey participants.
- Framework for a series of Regional ERM Roundtables.
- In order to participate in the survey and receive copies of reports, please follow the survey link:
<https://www.surveymonkey.com/s.asp?u=617131944186>
- Completion of the survey should take less than 30 minutes.

All individual responses will be kept confidential. Please submit only 1 survey response per company.

Questions?

Key Contacts

Rick Funston

Principal, National Practice Leader

Governance and Risk Oversight

rifunston@deloitte.com

office: +1-313-396-3014

Eric Hespenheide

Managing Partner, Global Internal Audit Services

ehespenheide@deloitte.com

Office: +1-313-396-3163

Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, its member firms, and their respective subsidiaries and affiliates. As a Swiss Verein (association), neither Deloitte Touche Tohmatsu nor any of its member firms has any liability for each other's acts or omissions. Each of the member firms is a separate and independent legal entity operating under the names "Deloitte", "Deloitte & Touche", "Deloitte Touche Tohmatsu", or other related names. Services are provided by the member firms or their subsidiaries or affiliates and not by the Deloitte Touche Tohmatsu Verein.