

Enterprise Risk Management

The
Cadence
Group



March 24, 2011



Introduction

Presenter: Gordy Jacobsen

- President and co-founder of The Cadence Group
- Specializes in Enterprise and IT Risk Management and Internal Audit
- Prior to Cadence, worked for PricewaterhouseCoopers in the Salt Lake City (Utah), San Jose (California) and Wellington (New Zealand) offices in their System and Process Assurance practice.
- MACC and BS, Accounting from Brigham Young University
- Member of AICPA, UACPA and ISACA



Agenda

1. Background on The Cadence Group – 5 min
2. Definition of Enterprise Risk Management (ERM) – 10 min
3. Driving Factors for ERM – 15 min
4. Common ERM Frameworks – 10 min
5. Organizational Structure of a Risk Function – 15 min
6. Roles and Responsibilities – 10 min
7. Risk Assessments – 20 min
8. ERM in Practice – 25 min
9. Questions & Answers

Background on The Cadence Group

The
Cadence
Group





Cadence Values

The Cadence Group is a Utah-based compliance and advisory firm. We pride ourselves on providing high-quality, interactive customer service to our clients. We achieve this high level of service through our value proposition, which includes the following attributes:

- *Experience* – Providing high-level expertise through seasoned professionals. With experienced personnel, our projects are completed proficiently while reducing the time and costs overhead associated with on-the-job training, coaching, reviewing and revising the work of less-experienced staff.
- *Flexibility* – Enabling clients to determine how to best use our services. We can either perform all the related tasks necessary to complete each phase of an engagement, we can coach and review work performed or provide clients with a combination of each. We continuously work with our clients to understand the engagement requirements, timing restrictions and desired deliverables to ensure a successful outcome.
- *Efficiency* – Ensuring engagements are effectively managed and skillfully executed. Our clearly defined objectives, relevant experience and cost-sensitive organizational structure allows our clients to receive requested services in a timely and cost-effective manner.



Cadence Services

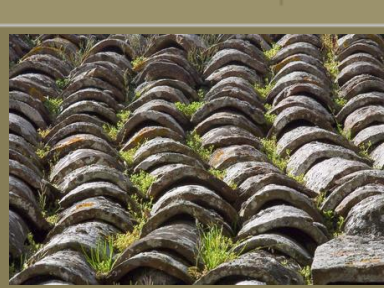
The Cadence Group provides enterprise risk management services. We specifically focus on business processes, financial reporting and compliance services in the areas of finance, accounting and information technology. Our services include:

- *Enterprise and IT Risk Management*
- *Financial Reporting and Technical Accounting*
- *Internal Audit Services*
- *Sarbanes-Oxley 404 Readiness Services*
- *Service Organization Control Reporting (formerly SAS 70 Audits)*
- *PCI Compliance Services*
- *HIPAA Compliance Services*

Definition of Enterprise Risk Management

The
Cadence
Group





Perceived Definition

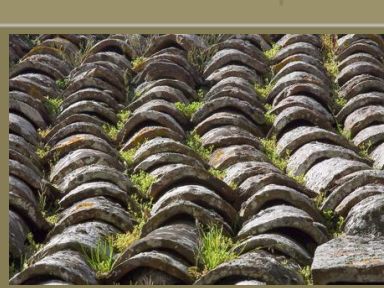
So what is Enterprise Risk Management...

“avoiding screw ups”

“staying off the front page”

“regulatory compliance”

“business prevention”



COSO Definition

Enterprise Risk Management is...

A process:

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

Source: COSO, Enterprise Risk Management – Integrated Framework

Driving Factors for ERM

The
Cadence
Group





Risk Management = Trust

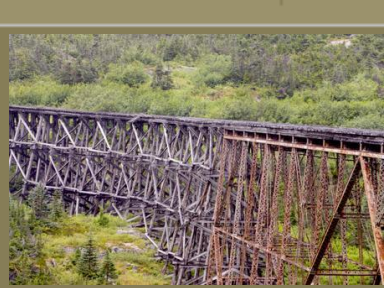
“Thoughtfully assessing and addressing enterprise risk and placing a high value on corporate transparency can protect the one thing we cannot afford to lose: trust.”

– Dale E. Jones, Vice Chairman, Heidrick & Struggles



Why ERM?

- Board expectations are increasing with respect to risk oversight
- Stakeholders are pressuring management to identify and explain risks
- Credit agencies (S&P) are factoring ERM analysis into rating process
- Insurance rates are decreasing for companies with established ERM
- Customers are requiring suppliers to have effective ERM
- Management is wanting to reduce risk for business decisions
- Industry groups are formalizing ERM frameworks and standards
- Regulations mandating or justifying ERM are increasing
 - Dodd-Frank Act
 - SEC Rule No. 33-9089
 - Managing Regulatory Requirements



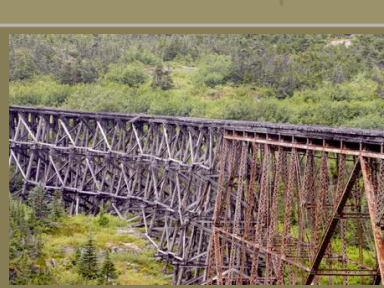
Dodd-Frank Act

Section 165 of the Dodd-Frank Act requires most large, publicly traded, financial service companies to establish a Risk Committee with the following characteristics:

- Be supervised by the Board of Governors of the Federal Reserve
- Be responsible for enterprise-wide risk management oversight and practices
- Be required to include at least one risk management expert having experience in identifying, assessing, and managing risk exposures of large, complex firms

To meet these requirements, companies should consider:

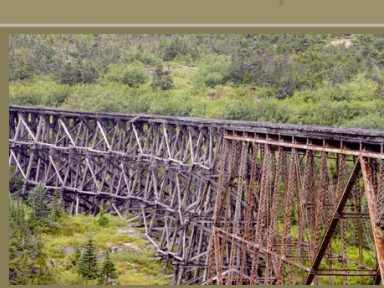
1. Creating a central reporting platform
2. Establishing a common taxonomy and library for policies, processes, risks, controls and regulatory requirements
3. Integrating multiple areas of risk to provide aggregated analysis and full reporting of all risks across the enterprise



SEC Rule No. 33-9089

New disclosure requirements are in place to enhance the information provided in annual reports, and proxy and information statements to better enable shareholders to evaluate the leadership of public companies.

- *Risk*: Requires disclosure about the board's role in risk oversight and disclosure about a company's compensation policies and practices as they relate to risk management.
- *Governance and Director Qualifications*: Requires expanded disclosure of the background and qualifications of directors and director nominees and new disclosure about a company's board leadership structure and accelerating the reporting of information regarding voting results.
- *Compensation*: Revises the reporting of stock and option awards and requires disclosure of potential conflicts of interest of compensation consultants in certain circumstances.



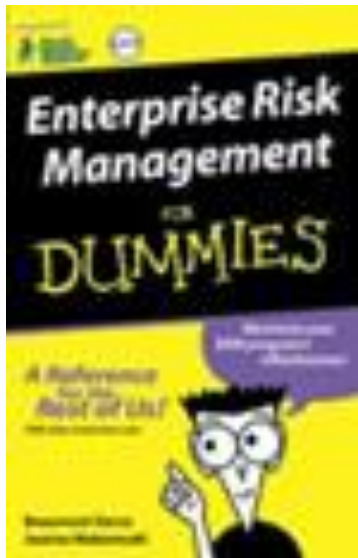
SEC Rule No. 33-9089 (Item 407)

Specific to the board's role in risk oversight, disclosure should:

- Outline the board leadership structure and the reason why this leadership structure is the most appropriate for the company.
- Define how the board oversees risk management activities and monitors risk, including how risk management reports to the board (i.e. directly to the board, through a committee or through a specific board member).
- Detail the following content:
 - Policies related to risk identification and prioritization processes
 - Risk appetite, tolerances and relationship to company strategy
 - Management of risk and reward decisions



Regulatory Compliance



Sarbanes-Oxley Act

PCI

Basel II

Gramm-Leach Bliley

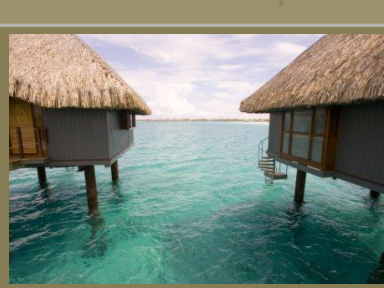
HIPAA / HITECH

Others?

Common ERM Frameworks

The
Cadence
Group

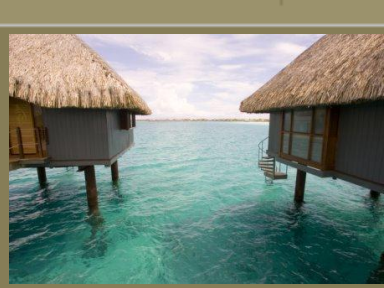




Positive Side of Risk

“One thing that makes it possible to be an optimist is if you have a contingency plan for when all hell breaks loose.”

– Randy Pausch, *The Last Lecture*

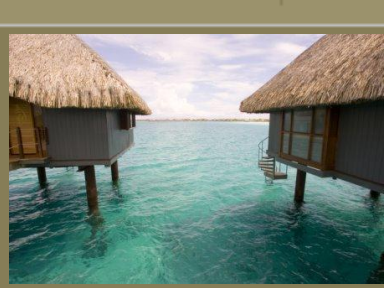


ISO 31000

The ISO in its current form was created in 2009 from the AUS / NZ 4360 standard (which was developed in 1999). The ISO 31000 family of documentation currently includes:

- ISO 31000: Principles and Guidelines on Implementation
- IEC 31010: Risk Management – Risk Assessment Techniques
- ISO/IEC 73: Risk Management – Vocabulary

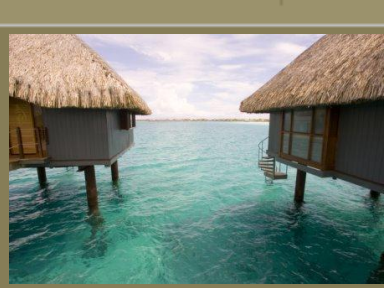
Risk is defined as an *exposure to the consequences* of uncertainty, or potential deviations from what is planned or expected.



ISO 31000 (cont.)

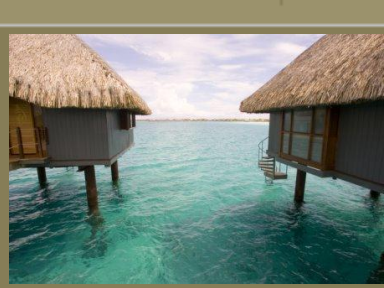
The ISO 31000 risk management process involves:

1. *Communicate and Consult* – Communicate and consult with internal and external stakeholders as appropriate at each stage of the risk management process and concerning the process as a whole.
2. *Establish the Context* – Establish the external, internal and risk management context in which the rest of the process will take place. Criteria against which risk will be evaluated should be established and the structure of the analysis defined.
3. *Identify Risks* – Identify where, when, why and how events could prevent, degrade, delay or enhance the achievement of the objectives.
4. *Analyze Risks* – Identify and evaluate existing controls. Determine consequences and likelihood and hence the level of risk. This analysis should consider the range of potential consequences and how these could occur.



ISO 31000 (*cont.*)

5. *Evaluate Risks* – Compare estimated levels of risk against the pre-established criteria and consider the balance between potential benefits and adverse outcomes. This enables decisions to be made about the extent and nature of treatments required and about priorities.
6. *Treat Risks* – Develop and implement specific cost-effective strategies and action plans for increasing potential benefits and reducing potential costs.
7. *Monitor and Review* – It is necessary to monitor the effectiveness of all steps of the risk management process. This is important for continuous improvement. Risks and the effectiveness of treatment measures need to be monitored to ensure changing circumstances do not alter priorities.

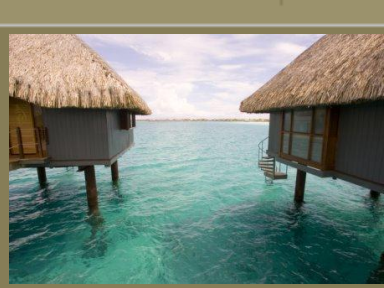


CAS Framework

In 2003, the Casualty Actuarial Society (CAS) defined ERM as the discipline by which an organization in any industry assesses, controls, exploits, finances, and monitors risks from all sources for the purpose of increasing the organization's short and long-term value to its stakeholders. The CAS conceptualized ERM as proceeding across the two dimensions of ***risk type*** and ***risk management processes***.

The risk types and examples include:

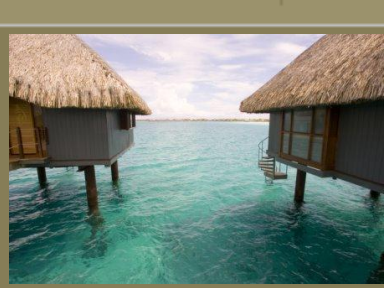
- *Hazard Risk* (liability torts, property damage, natural catastrophe)
- *Financial Risk* (pricing risk, asset risk, currency risk, liquidity risk)
- *Operational Risk* (customer satisfaction, product failure, integrity, reputational risk)
- *Strategic Risk* (competition, social trend and capital availability)



CAS Framework (*cont.*)

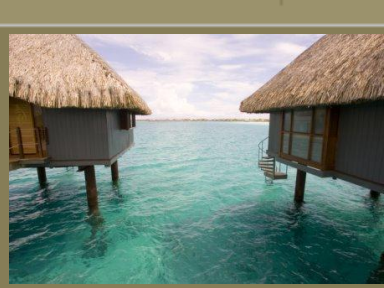
The CAS risk management process involves:

- *Establishing Context*: This includes an understanding of the current conditions in which the organization operates on an internal, external and risk management context.
- *Identifying Risks*: This includes the documentation of the material threats to the organization's achievement of its objectives and the representation of areas to the organization may exploit for competitive advantage.
- *Analyzing/Quantifying Risks*: This includes the calibration and, if possible, creation of probability distributions of outcomes for each material risk.

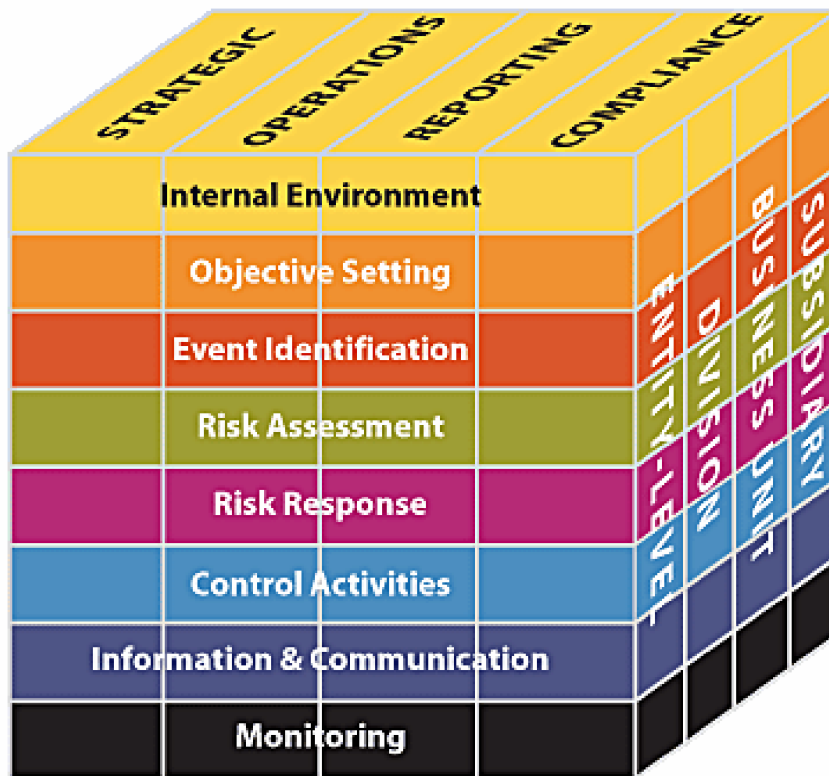


CAS Framework (*cont.*)

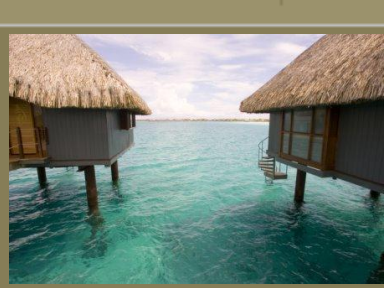
- *Integrating Risks*: This includes the aggregation of all risk distributions, reflecting correlations and portfolio effects, and the formulation of the results in terms of impact on the organization's key performance metrics.
- *Assessing/Prioritizing Risks*: This includes the determination of the contribution of each risk to the aggregate risk profile, and appropriate prioritization.
- *Treating/Exploiting Risks*: This includes the development of strategies for controlling and exploiting the various risks.
- *Monitoring and Reviewing*: This includes the continual measurement and monitoring of the risk environment and the performance of the risk management strategies.



COSO Framework



Published in 2004, the COSO *Enterprise Risk Management – Integrated Framework* expanded upon a previous publication: *Internal Control – Integrated Framework*, which was widely used for public companies complying with the Sarbanes-Oxley Act. The ERM framework expands on internal control, providing a more robust and extensive focus on the broader subject of enterprise risk management.

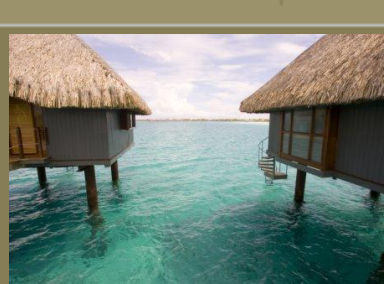


COSO Framework (*cont.*)

The COSO framework organizes an organization's objectives into the following four categories:

- *Strategy* – high-level goals, aligned with and supporting the organization's mission
- *Operations* – effective and efficient use of an organization's resources
- *Reporting* – reliability of operational and financial reporting
- *Compliance* – compliance with applicable laws and regulations

While these categories are distinct, a business objective can fall into more than one category. They are meant to be customized to meet the organization and specific objectives of the organization.



COSO Framework (*cont.*)

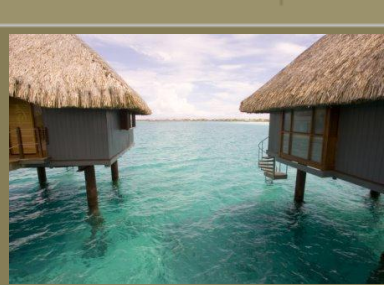
The COSO framework includes eight interrelated components:

- *Internal Environment* – The internal environment encompasses the tone of an organization, and sets the basis for how risk is viewed and addressed by an entity'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 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. Opportunities are channeled back to management's strategy or objective-setting processes.



COSO Framework (*cont.*)

- *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 effective.
- *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 made as necessary. Monitoring is accomplished through ongoing management activities, separate evaluations, or both.



Framework Comparison

ISO	CAS	COSO
Communicate and Consult	Establishing context	Internal Environment
Establish the Context	Identifying risks	Objective Setting
Identify risks	Analyzing /Quantifying Risks	Event Identification
Analyze risks	Integrating Risks	Risk Assessment
Evaluate risks	Assessing/Prioritizing Risks	Risk Response
Treat risks	Treating/Exploiting Risks	Control Activities
Monitor and review	Monitoring and Reviewing	Information and Communication
		Monitoring

= processes associated with the risk assessment

Organizational Structure of a Risk Function

The
Cadence
Group





Controlling Risks

“Risk is like fire: If controlled it will help you; if uncontrolled it will rise up and destroy you.”

– Theodore Roosevelt



Top Risk Management Failures

1. Poor governance and “tone at the top”
2. Reckless risk taking
3. Inability to implement enterprise risk management
4. Non existent, ineffective or inefficient risk assessment
5. Falling prey to a “herd mentality”
6. Misunderstanding the “if you can’t measure it, you can’t manage it” mindset
7. Accepting a lack of transparency in high-risk areas
8. Not integrating risk management with strategy-setting and performance management
9. Ignoring the dysfunctionalities and “blind spots” of the organization’s culture
10. Not involving the board in a timely manner.

* Source: Protiviti’s *The Bulletin* (Volume 3, Issue 6)



Risk Management = Business Prevention?

Executive sponsorship of the risk function is essential to its success. Typically, the executive sponsor is either the Chief Risk Officer (if designated) or the Chief Financial Officer with the ultimate responsibility with the Chief Executive Officer.

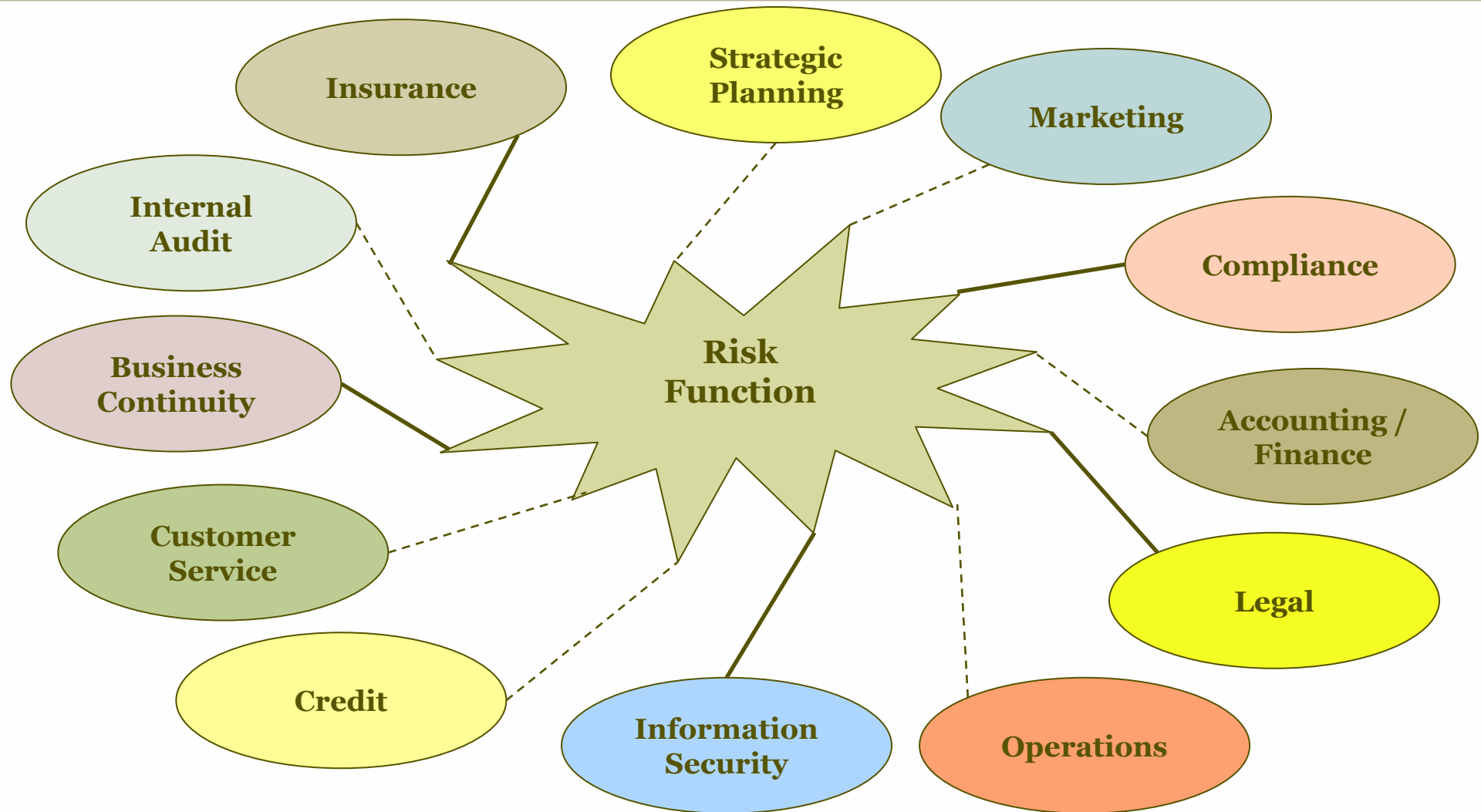
Without executive sponsorship, the risk management function will not likely be able to successfully complete the following:

- Create a risk management culture
- Incorporate risk into strategic discussions
- Perform a risk assessment
- Assign risks to risk owners
- Obtain meaningful data to report

Without executive sponsorship, risk management becomes business prevention.



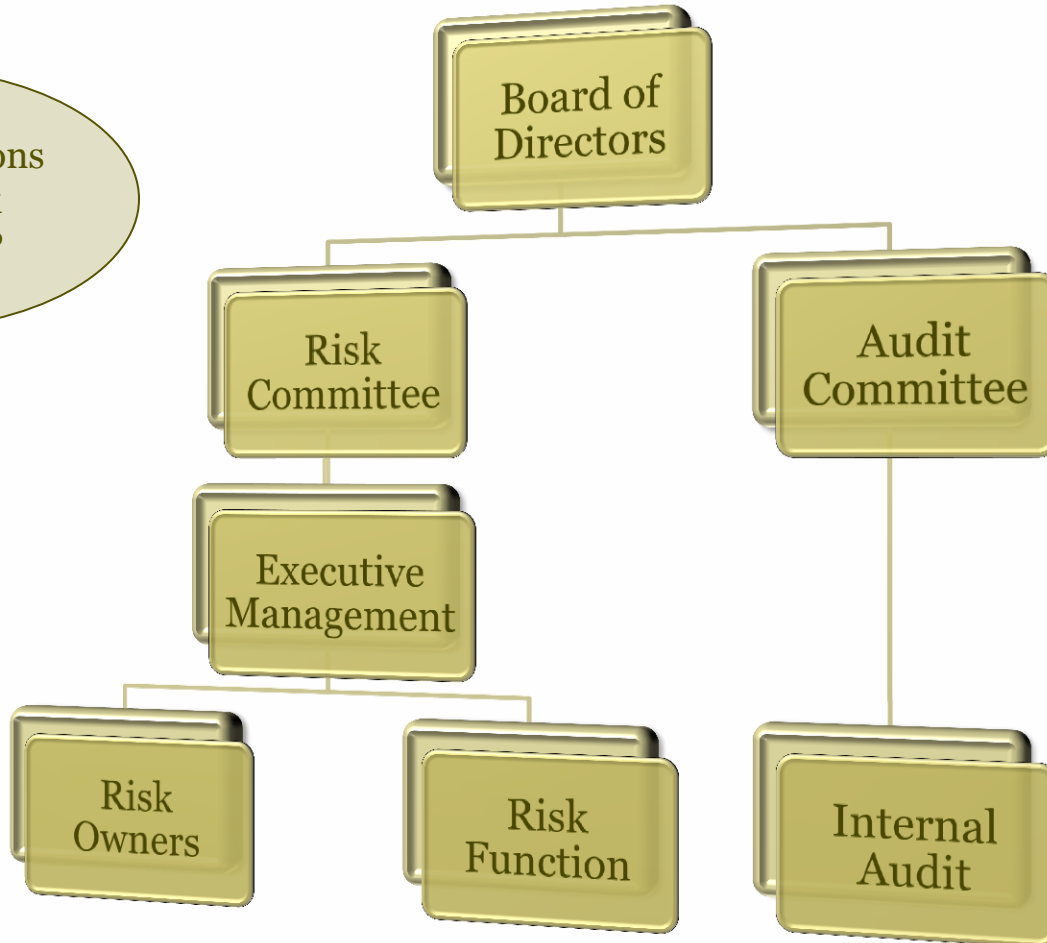
Incorporating the Business





Risk Committee?

Are organizations creating risk committees?



Roles and Responsibilities

The
Cadence
Group





Understanding Roles

“Duty is the most sublime word in our language. Do your duty in all things. You cannot do more. You should never wish to do less.”

– Robert E. Lee



Risk Owners: Line Management and Employees

Risk management is the responsibility of the employees and is typically assigned to specific risk owners. Risk owners include managers and key employees who have the responsibility of executing the approach outlined in the agreed risk response.

Specifically, risk owners:

- Have the responsibility for identifying the risks
- Monitor and manage risks according to ERM policies and procedures



Executive Management

Senior leadership has the responsibility to perform the following:

- Support an active risk management organization
- Ensure a formal ERM framework exists and that it supports the organization
- Develop principles, policies and procedures to support the framework
- Monitor the critical risks in an active manner
- Maintain proper balance exists between risk and strategy
- Report critical risk information to the board



Board of Directors

The Board of Directors must be a critical participant in the process. Frameworks and regulations designate the board to have the primary ownership for ensuring appropriate governance and overseeing enterprise risk management.

To create an effective risk management function, boards must establish formal processes to perform the following:

- Receive and react to critical risk information
- Approve the enterprise risk assessment
- Reconcile the defined risk appetite and tolerances with the strategic direction
- Oversee the structure and adherence to ERM framework



Risk Management

The Risk Management function supports enterprise risk management through the following:

- Promote risk management culture through training and awareness
- Review the framework, policies and procedures associated with risk management
- Provide support to risk owners to help ensure that risks are properly managed across the organization
- Support executive management in reporting risk management activities



Internal Audit

Internal Audit has the role of monitoring the risk management function to assess the effectiveness of the function. Internal audit should not own day-to-day risk management and assessment activities.

Specifically, Internal Audit should:

- Help facilitate risk assessment processes
- Provide oversight and assurance regarding the organization's effectiveness in identifying and appropriately controlling risks
- Consult with the risk management function regarding the effectiveness of the ERM program

Risk Assessments

The
Cadence
Group





Risk Centralization

“Having a single view of risk is critical to making consistent and informed decisions. When risk management is siloed, without one person or team owning the process, no one has visibility to aggregate exposures and accountability for the decisions.”

– John Farrell, KPMG Enterprise Risk Management Partner



Determining Risk Appetite

Risk appetite – the level of uncertainty the organization is prepared to accept in order to achieve strategic objectives. It should:

- Reflect the strategy and objectives of the organization
- Outline willingness and capacity to accept risk, including tolerance for loss or negative events
- Include qualitative and quantitative characteristics
- Account for organization's skills, resources and technology
- Consider the need for various profiles in regions, business units and product lines
- Have board approval



Performing a Risk Assessment

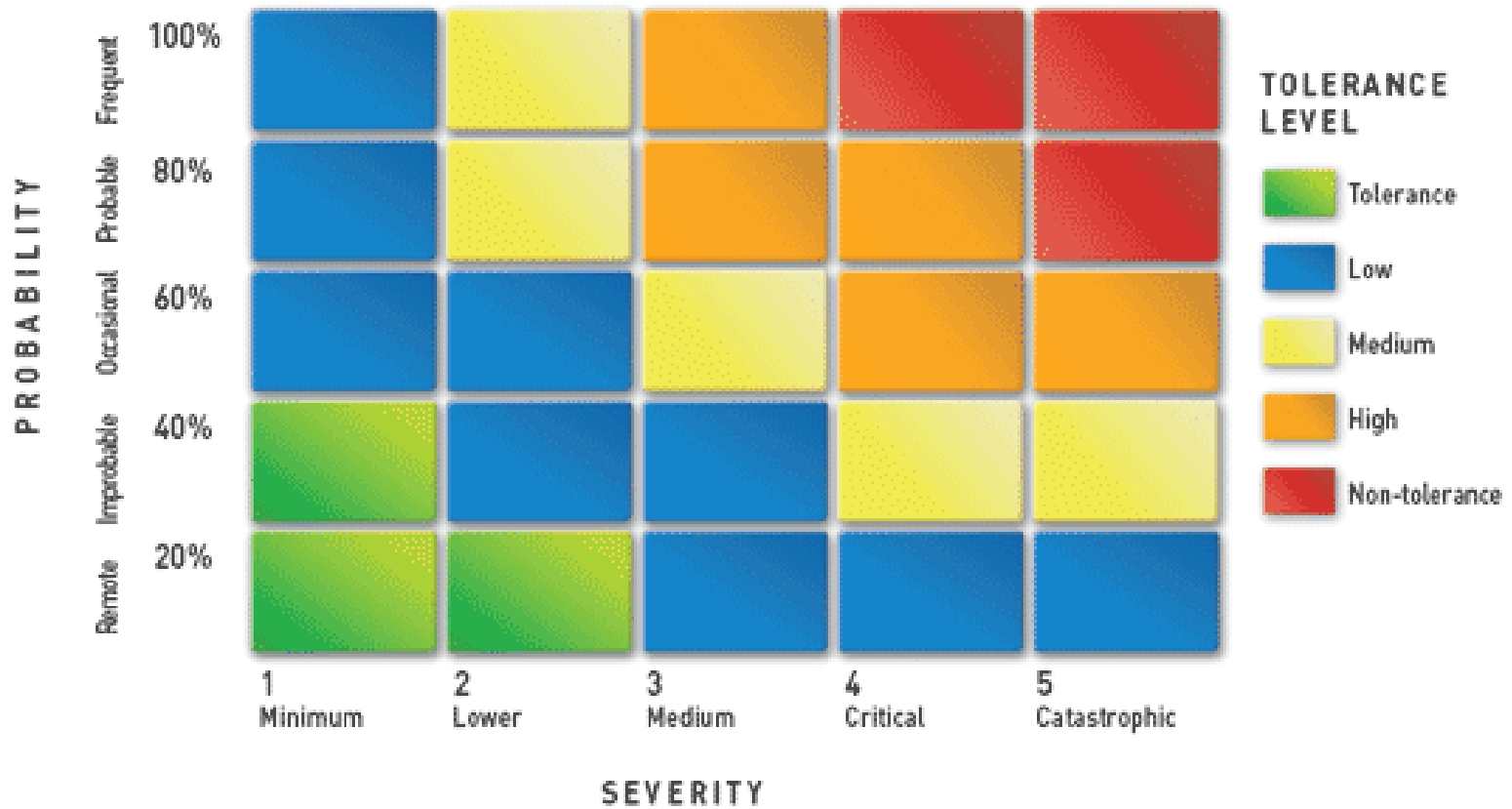
Risk owners (or perspective risk owners) should identify risks and categorize them as it pertains to the following:

- *Impact, Severity or Magnitude:* Consequences the risk may have on the organization's strategic objective. Typically, this attribute is measured in both quantitative (cost) and qualitative terms.
- *Probability or Likelihood:* Chance the risk may occur. This attribute is measured in the probability (percentage) that the risk will occur.

In addition to the above categories, organizations are also measuring the *velocity* of the risk or the speed at which risk travels through an organization. Velocity is generally measured by defining the time to impact.

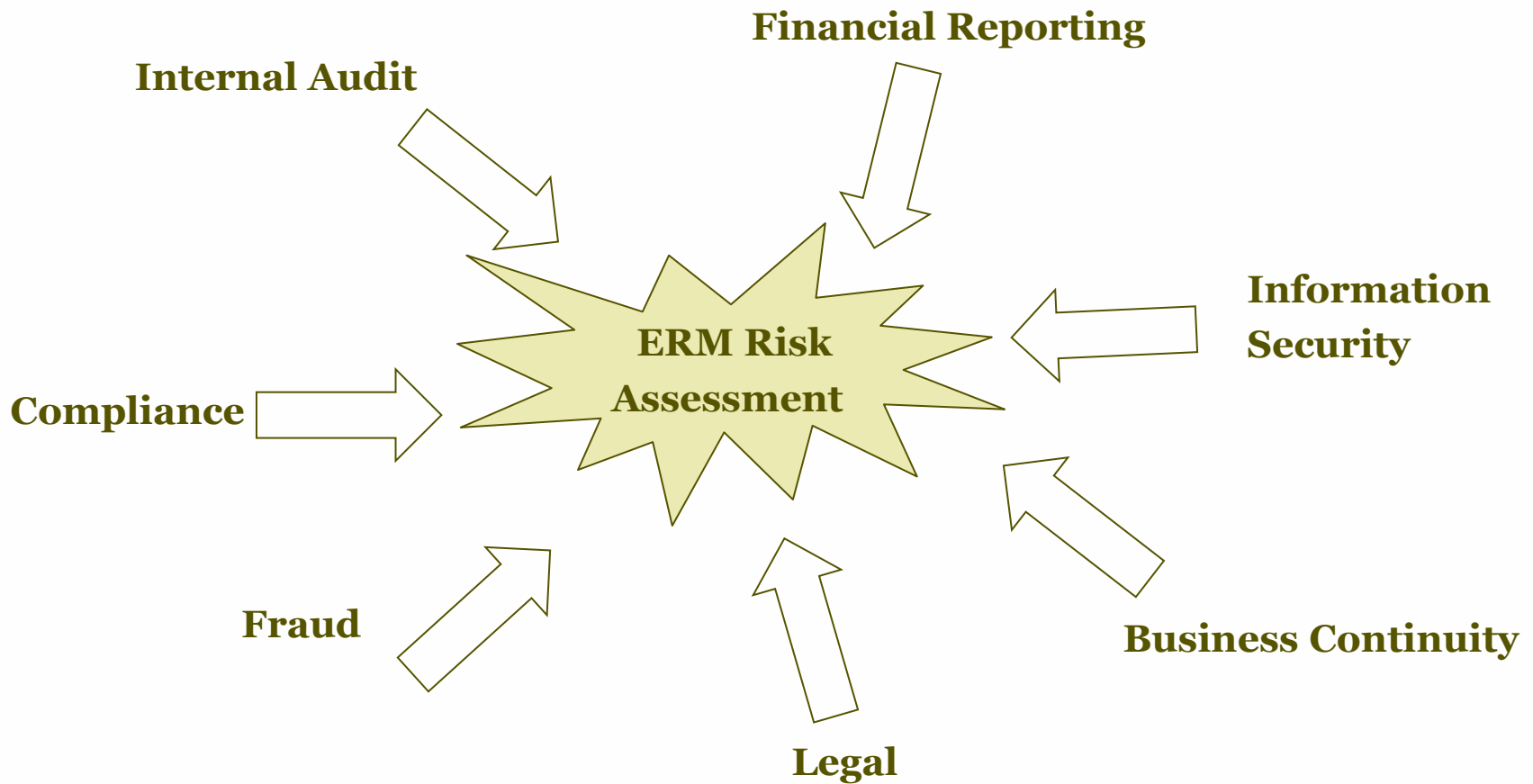


Illustrative Heat Map



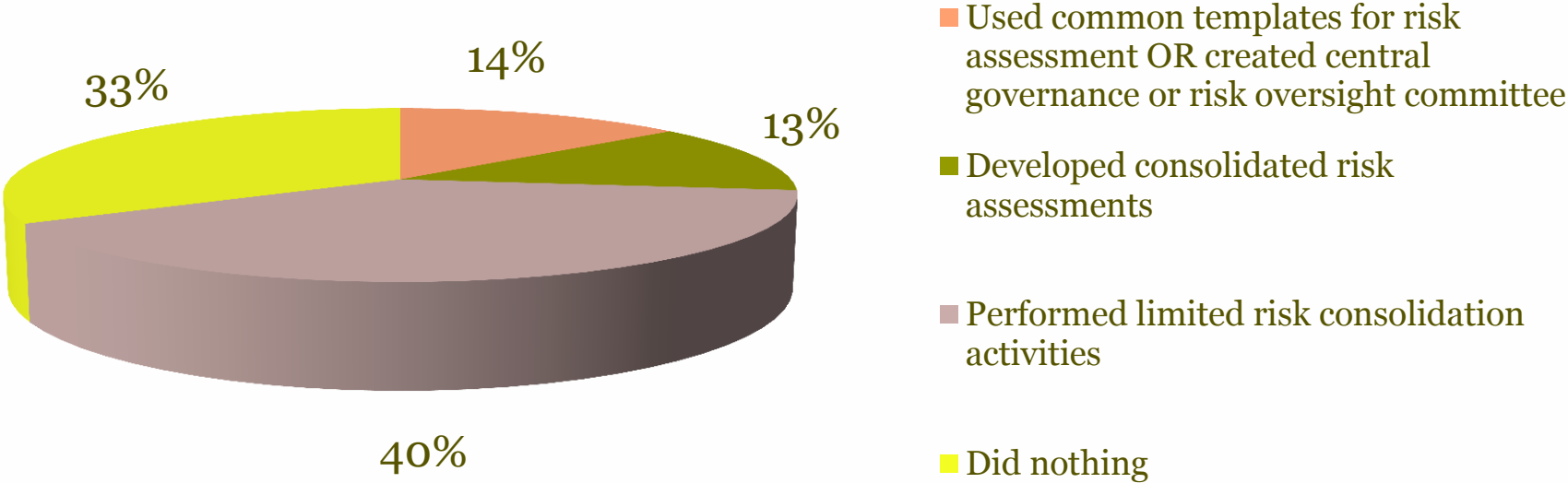


Aligning Risk Assessments



Risk Assessment Redundancy

Company Risk Consolidation Activities



Source: KPMG 2009 Survey of Internal Auditors and Boards



Emerging Risks = Risk Radar

In addition to known risks, management should seek to assess emerging risks. To identify these risks, management should regularly perform a scan of characteristics and changes in the environment to identify events that may have impacted the shareholder value in the past or may impact it in the future. Risks may result from economic, social, political, technological, and natural environmental events.

The risk assessment process is generally performed through scenario analysis. Through these scenarios, the emerging risks, their associated drivers, management can assess the likelihood and impact as well as a risk response.

Case Study: Wal-Mart during Hurricane Katrina

Source: PricewaterhouseCoopers, Extending Enterprise Risk Management (ERM) to address emerging risks

ERM in Practice

The
Cadence
Group





What are we managing?

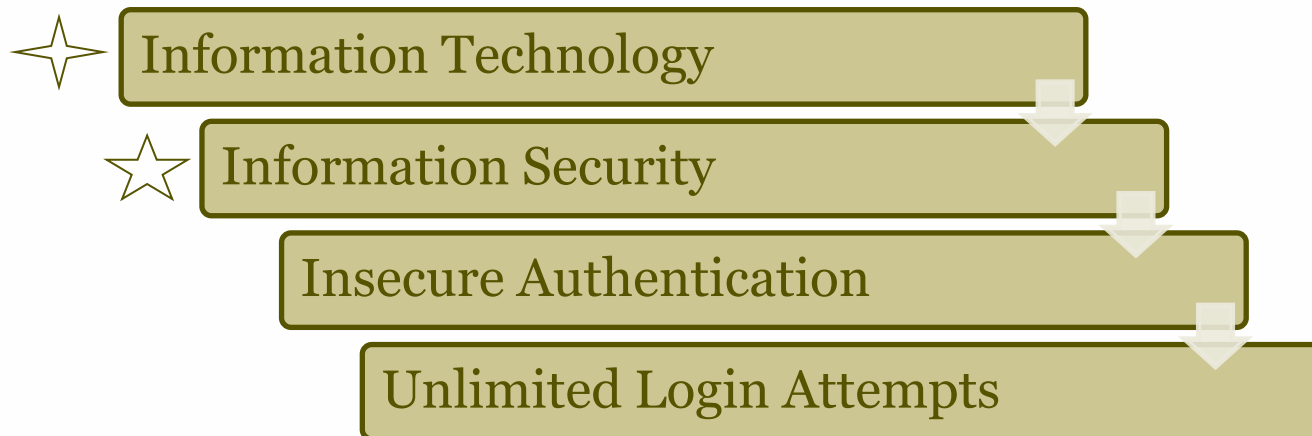
“It takes 20 years to build a reputation and 5 minutes to ruin it and if you understand this you will do things differently.”

– Warren Buffett



Risk Assignment

Upon completion of the risk assessment, risk ownership should be formalized. The practice of assigning ownership is difficult and requires careful planning to ensure it is assigned to the appropriate people at the appropriate risk level. Refer to the following example of a risk hierarchy:



✦ Assign CIO (Executive Sponsor)

★ Assign Security Manager (Risk Owner)



Risk Response

For each identified risk, the risk owner should develop one of the following risk responses:

- *Avoid*: avoiding or exiting the activities giving rise to risk
- *Reduce or Mitigate*: taking action (implementing controls) to reduce the likelihood or impact related to the risk... includes outsourcing.
- *Share or Insure*: transferring or sharing a portion of the risk in an effort to reduce it
- *Accept*: taking no action due to the cost/benefit

Case Study: Energy Solutions



Jimmer the Risk?

High magnitude, high likelihood...





Risk Monitoring

The adopted framework should outline the frequency with which a risk owner re-assesses the risk (including severity and probability). If velocity is tracked, this may factor into the frequency of the review.

In addition, for instances where the risk was reduced or mitigated, testing should be performed to confirm that the processes or controls put in place are effectively in mitigating the identified risk. The framework should incorporate a risk-based approach to testing. For high risk areas or areas requiring independence, Internal Audit may provide this testing.



Risk Reporting

Reporting should be considered at several levels:

- **Risk Owner:** Reporting at the risk owner level includes detailed information about the control and may be in an ORC (objective, risk and control) matrix. The risk owner also requires the capability to update risk information.
- **Executive Management:** Reporting at this level may be in the form of a executive-specific dashboard, summarizing the risks the executive sponsors. Executives with enterprise responsibilities (e.g. CRO) may have a dashboard that includes all risks.
- **Board of Directors / Risk Committee:** In addition to the ERM strategy and framework, board members should receive a high-level overview of the risks facing the organization, specifically highlighting the risks in excess of prescribed tolerance levels.



ERM Systems

The risk assessment process is data intensive. In addition to the nature or description of the risk, management may want to consider capturing these and other key attributes of risk management:

- Risk Description
- Mapping to Strategic Objectives
- Mapping to Compliance Initiative (if applicable)
- Risk Level (assuming use of a risk hierarchy)
- Impact, Severity or Magnitude
- Probability or Likelihood
- Risk Response
- Risk Monitoring Approach and Results
- Risk Ownership
- Impacted Regions, Business Units and Product Lines



ERM Shortcomings

The three largest obstacles in creating an effective enterprise risk management program are:

1. **Risk Culture** – The inability to have ‘buy in’ from all of the stakeholders, especially senior management and the board will inevitably lead to failure.
2. **Risk Management Processes** – If the framework isn’t consistently understood and applied throughout the organization, the ability to effectively communicate and manage risks diminishes.
3. **Technology** – The ability to communicate and process large volumes of data is necessary to effectively track the multiple risk management processes, including risk identification, ownership, assessment, management and monitoring.



Risk Management Maturity

ERM Element	Basic (Compliant)	Mature (Process)	Advanced (Strategic)
Risk Governance	A central risk management policy to supporting external requirements	A risk management structure with clear accountabilities to support risk management objectives	Risk management accountability integrated with performance management
Risk Assessment	Annual risk assessment with limited analysis and interpretation	Frequent risk assessments in line with normal management reporting including analysis	Risk and control activities embedded in business processes
Risk Quantification and Aggregation	Quantification of selected risks	Quantification of operational risk, advance quantification of selected risks	Entity wide aggregation across all risk areas
Risk Monitoring and Reporting	Business risk reporting designed to support external reporting requirements	Extensive reporting to the board (or committee) on current risk levels and future risk issues	Alignment of risk reporting provides a comprehensive single view of risk
Risk and Control Optimization	Fewer surprises through the management of key risks	Greater stakeholder confidence and improved risk mitigation strategies	Risk-adjusted strategy performance evaluation and capital allocation



Successful ERMs

1. Risks are centrally located and commonly understood.
2. Risks are incorporated into strategy and address needs of all applicable stakeholders.
3. Risk management roles and responsibilities are clearly defined from the board to risk owners.
4. Processes to identify, management and report risks are consistent.
5. Risk management competency improves across the organization.
6. Organization becomes forward-looking and preventative in its approval to risk management.

Questions?

The
Cadence
Group



Phone 801 337 3917 • Fax 866 326 6612
www.thecadencegroup.com