Enterprise Risk Management: Developing, Implementing, and Sustaining an Effective ERM Program

an independent member of BAKER TILLY INTERNATIONAL

BAKER TILLY VIRCHOW KRAUSE, LLP

Candor. Insight. Results.

Presentation Overview

BAKER TILLY
VIRCHOW KRAUSE, LLP

Candor. Insight. Results.

> Session Objectives
> Enterprise Risk Management (ERM) Background and Theory
> Initiation and Planning
> Enterprise Risk Assessment
> Risk Response
> Sustaining ERM
> Closing Thoughts

Session Objectives

BAKER TILLY
VIRCHOW KRAUSE, LLP

Candor. Insight. Results.

> Gain an understanding of enterprise risk management theory
> Understand the risk assessment process and practical applications
> Become familiar with a process for identifying, prioritizing and addressing risks
> Learn approaches for sustaining ERM

Enterprise Risk Management: Background and Theory

Risk Management Failures in History

BAKER TILLY
VIRCHOW KRAUSE, LLP

Candor. Insight. Results.

1637: The Tulip Bulb Craze
1720: The South Sea Bubble
1989: The S&L Crisis
1995: The Barings Derivatives Scandal
2001: Enron
2002: WorldCom
2008: Housing Collapse
2010: Gulf Oil Spill
2012: JP Morgan, Knight Capital

WORLDCOM

savings & loans

Defining Risk and Enterprise Risk Management

BAKER TILLY
VIRCHOW KRAUSE, LLP

Candor. Insight. Results.

Risk is the potential for loss of value or the sub-optimization of gain – it may be caused by an event, or series of events, that can adversely affect the achievement of objectives which are generally to:

> Protect the value of its existing assets

> Create new or future value

Enterprise Risk Management (ERM) is a continuous process that identifies, mitigates, and monitors potential future events that create uncertainty, in a manner that reduces potential loss and increases potential gain.

"Risk is fundamentally a deviation from intended results."

The Purpose of ERM

BAKER TILLY
VIRCHOW KRAUSE, LLP

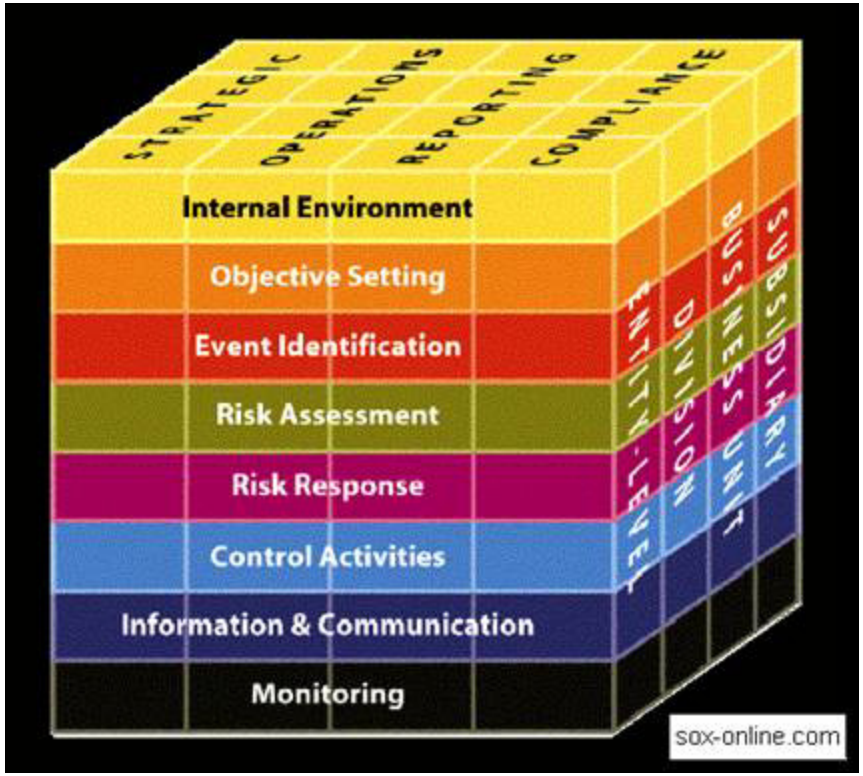
Candor. Insight. Results.

ERM can be used as a management tool, incorporating the general control structure to form the basis for assessing and managing organizational risks.

Risk management should:

> Assist organizations in identifying and managing risks within their risk appetite.

> Be aligned with organizational objectives in order to assist in meeting strategic goals.

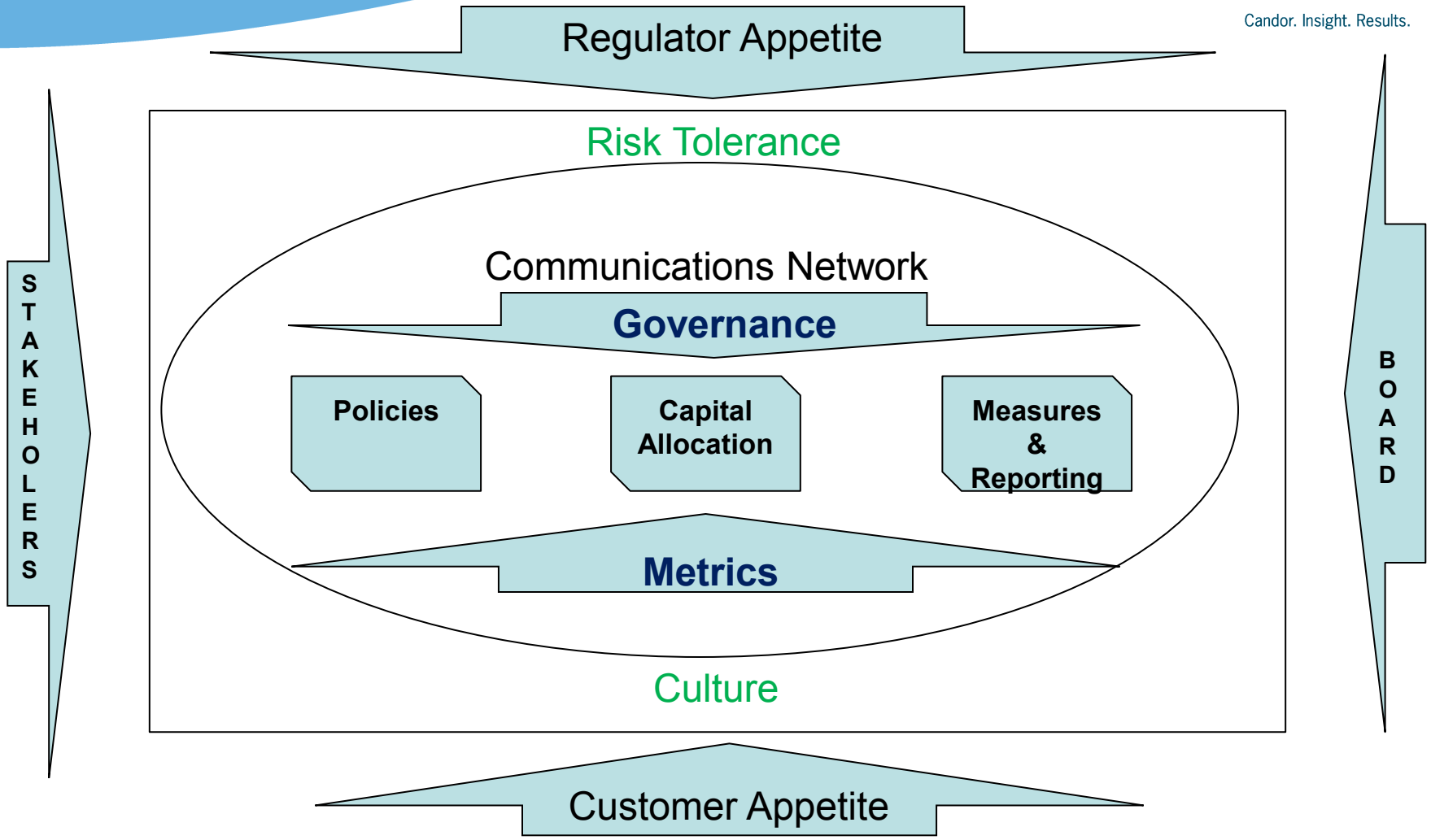


Source: COSO, *Enterprise Risk Management – An Integrated Framework*

ERM Framework

BAKER TILLY
VIRCHOW KRAUSE, LLP

Candor. Insight. Results.



Typical Functions that Use Enterprise Risk Management

BAKER TILLY
VIRCHOW KRAUSE, LLP

Candor. Insight. Results.

- **Strategic planning** - identifies external threats and competitive opportunities, along with strategic initiatives to address them
- **Marketing** - understands the target customer to ensure product/service alignment with customer requirements
- **Compliance & Ethics** - monitors compliance with code of conduct and directs fraud investigations
- **Accounting / Financial compliance** - directs the Sarbanes-Oxley Section 302 and 404 assessment, which identifies financial reporting risks
- **Law Department** - manages litigation and analyzes emerging legal trends that may impact the organization
- **Insurance** - ensures the proper insurance coverage for the organization
- **Operational Quality Assurance** – verifies operational output is within tolerances
- **Operations management** - ensures the business runs day-to-day and that related barriers are surfaced for resolution
- **Credit** - ensures any credit provided to customers is appropriate to their ability to pay
- **Customer service** - ensures customer complaints are handled promptly and root causes are reported to operations for resolution
- **Internal audit** - evaluates the effectiveness of each of the above risk functions and recommends improvements
- **Treasury** - ensures cash is sufficient to meet business needs, while managing risk related to commodity pricing or foreign exchange

The Evolution of ERM

BAKER TILLY
VIRCHOW KRAUSE, LLP

Candor. Insight. Results.

A robust ERM program reflects a new way of thinking about Risk Management, replacing past concepts with new ways of approaching risk:

Past		Present
Insurable and financial risks = Hazard Risk Management	→	**Operational, strategic, financial and insurable risks =** Enterprise Risk Management
Focus on preservation of tangible assets	→	**Recognition of the value of** tangible and intangible assets
Each department/function manages its risks independently silo approach	→	**Coordinated at highest level within the organization** holistic approach
Risk Management is a separate function within the organization	→	**RM is everyone's daily concern** embedded in the operations
Focused on avoidance of negative events risks are threats	→	**Considering all business uncertainties** risks are threats and opportunities business risk management

Why ERM: The Value Proposition

BAKER TILLY
VIRCHOW KRAUSE, LLP

Candor. Insight. Results.

There are several reasons why an organization should consider implementing an ERM program:

> Enhanced corporate governance
> Improved process efficiency
> Optimized resource allocation
> Compliance with Federal laws and regulations
> Increased transparency
> Reduced volatility
> Consistent approach to risk management

ERM Engagement Overview

BAKER TILLY
VIRCHOW KRAUSE, LLP

Candor. Insight. Results.

ERM engagements should contain the following activities:

> **Initiation and Planning**:
  - Develop and communicate the ERM program and ERM Charter.
  - Conduct training sessions with key stakeholders to introduce them to ERM methodologies.

> **Enterprise Risk Assessment**:
  - Identify and prioritize the universe of risk areas and organizational entities to comprise the scope of the enterprise risk management program.

> **Risk Response**:
  - Develop mitigation strategies for the highest priority risks.
  - If resources are limited, management should focus greater attention on those risks deemed to have high severity, low risk tolerance, and high entity governance exposure.

> **Sustaining ERM**:
  - Develop ongoing monitoring policies and procedure to detect and address changes in risk severity and mitigation effectiveness.

Initiation and Planning

Initiation and Planning

BAKER TILLY
VIRCHOW KRAUSE, LLP

Candor. Insight. Results.

The initiation and planning phase of an ERM engagement should include the following steps:

> Structuring ERM Governance

> Communication and Training

Initiation and Planning: ERM Charter

BAKER TILLY
VIRCHOW KRAUSE, LLP

Candor. Insight. Results.

Developing a risk committee or governance structure and an ERM charter early in the process is critical:

> Determine the purpose and structure of the Risk Committee

> Articulate the key ERM program objectives

> Establish an appropriate composition of members and include a variety of expertise and skill sets

> Assign clear authority, roles and responsibilities

> Provide for independent oversight and ongoing monitoring of the committee

> Align Risk Committee with other related risk based groups – design charters that complement, not compete, with one another

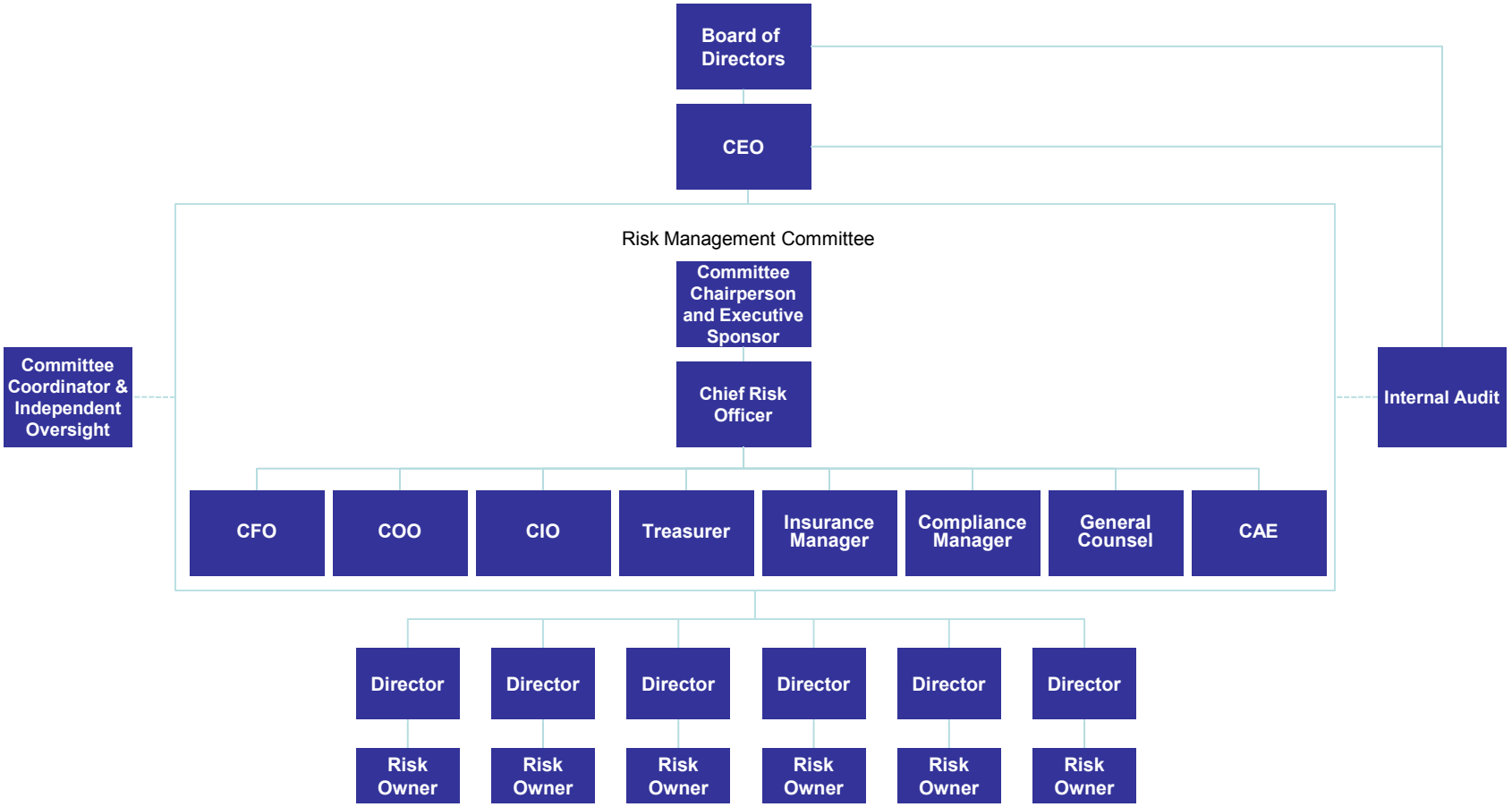
> Link to performance management

Initiation and Planning: Governance Structure

BAKER TILLY
VIRCHOW KRAUSE, LLP

Candor. Insight. Results.

Sample Risk Governance Structure:



Initiation and Planning: Roles and Responsibilities

BAKER TILLY
VIRCHOW KRAUSE, LLP

Candor. Insight. Results.

Board of Directors Responsibilities:

> Overall responsibility for an organization's risk management and control processes
> Strategy setting, formulating high-level business objectives, and resource allocation
> Monitoring management's risk appetite, given the business objectives
> Inquiry into the most significant risks and the appropriateness of management's action plan

CEO Responsibilities:

> Sets the tone at the top to maintain a positive and open environment for all risk management activities
> Shapes the principals and values of the risk management program
> Maintains oversight and provides leadership to the Risk Committee
> Apprises themselves with enterprise risk by meeting periodically with key functional managers to review their responsibilities

Initiation and Planning: Roles and Responsibilities (cont.)

BAKER TILLY
VIRCHOW KRAUSE, LLP

Candor. Insight. Results.

Risk Committee Responsibilities:

> Policy and standard setting
> Accountability setting
> Risk management
> Reporting
> Management discussion and analysis support

Risk Sponsor Responsibilities

> Ensure timely completion and reporting of risk remediation activities to the Risk Committee
> Continuously monitor and report status on risk
> Communicate any locally developed risk management best practices to the Risk Committee
> Perform periodic self-assessment of the key controls and validation procedures

Initiation and Planning: Roles and Responsibilities (cont.)

BAKER TILLY
VIRCHOW KRAUSE, LLP

Candor. Insight. Results.

Risk Owner Responsibilities:

> Ensure day-to-day performance of controls to address risk levels

> Report any identified deviations or changes to the risk level to the Risk Sponsor

Internal Audit Responsibilities

> Verify the operating effectiveness of new mitigation activities and perform ongoing testing as part of the audit plan

> Examine, evaluate, report, and recommend improvements on the adequacy and effectiveness of management's ERM process

> Assist the organization in identifying, evaluating, and implementing risk management methodologies and controls to address risk

> Utilize the ERM process for planning audit activities

> Ensure that the ERM program addresses that:

- Risks are identified and prioritized
- Management and the board have determined the level of risk acceptable to the organization
- Risk mitigation activities are designed to manage risk at levels acceptable to management and the board
- Ongoing monitoring occurs, and the board and management are updated on status

Initiation and Planning: Communication and Training

BAKER TILLY
VIRCHOW KRAUSE, LLP

Candor. Insight. Results.

The importance and value of Risk Management will need to be communicated from the highest levels of the organization

> Explain “why” ERM is being implemented along with “what” needs to be done
> Channels of communication should be built to flow up and down the organization
> All levels of the organization should be clearly aware of expectations both before and after implementation
> Initial successes should be pursued and publicized to the wider organization
> Multiple teams need to proactively and consistently collaborate to successfully implement ERM

Enterprise Risk Assessment

Enterprise Risk Assessment – Scope

BAKER TILLY
VIRCHOW KRAUSE, LLP

Candor. Insight. Results.

To be effective, the scope of the ERM framework needs to be clearly defined.

> Define the internal, external and risk parameters to consider in managing risk

> Establish expectations around the development of an organization's risk culture

> Ensure that critical ERM objectives are tied to performance objectives

> Prioritize ERM objectives so they are in line with the organization's mission and major initiatives, given current resource constraints and availability

> Identify and establish risk budgets and funding for necessary mitigation activities

Enterprise Risk Assessment – Risk Identification

BAKER TILLY
VIRCHOW KRAUSE, LLP

Candor. Insight. Results.

Accurate and comprehensive risk identification as part of an ERM program is critical to developing effective controls and mitigating risk in the long term.

> Inventory an organization's universe of risk

> Determine the best method, or combination of methods, for effectively identifying risk:
  - Facilitated workshops
  - Interviews or surveys
  - Department wide surveys
  - External review

> Schedule periodic sessions to reevaluate the risk universe and identify emerging exposures

> Leverage risk assessments performed previously

Enterprise Risk Assessment – Risk Universe of Business Threats

BAKER TILLY
VIRCHOW KRAUSE, LLP

Candor. Insight. Results.

External Environment

- Competitor
- Legal & Regulatory
- Catastrophic Loss
- Power and Fuel Costs
- Customer Expectations
- Regional Market Issues
- Natural Disasters
- Terrorism

Business Strategies & Policies

- Strategy & Innovation
- Capital Allocation
- Business / Service Portfolio
- Organization Structure
- Organization Policies

Business Process Execution

- Operations – Planning
- Operations – Process/Technology Design
- Operations – Process/Technology Execution & Continuity
- Resource Capacity & Allocation
- Vendor/Partner Reliance
- Interdependency
- Customer Satisfaction
- Regulatory Compliance
- Knowledge/Intellectual Capital
- Change Integration

People

- Leadership
- Skills/Competency
- Change Readiness
- Communication
- Performance Incentives
- Accountability
- Fraud & Abuse

Analysis & Reporting

- Performance Management
- Budgeting/Financial Planning
- Accounting Information
- External Reporting & Disclosure
- Pricing/Margin
- Market Intelligence
- Contract Commitment

Technology & Data

- Technology Infrastructure/Architecture
- Data Relevance & Integrity
- Data Processing Integrity
- Technology Reliability & Recovery
- IT Security

Enterprise Risk Assessment – Risk Analysis and Evaluation

BAKER TILLY
VIRCHOW KRAUSE, LLP

Candor. Insight. Results.

An organization's ERM program will be more effective if it leverages industry standard frameworks for risk management.

> Using the information obtained for each risk, analyze and evaluate each key risk identified within the risk universe
  - Determine the likelihood of the risk occurring.
  - Assess the potential impact if the risk were to occur.

> Determine which perspectives to utilize in analyzing specific risks:
  - Organizational goals
  - Organizational strategy
  - Organizational tolerance
  - Operational Impact
  - Likelihood of Occurrence
  - Mitigation Effectiveness
  - Persistence
  - Velocity
  - Complexity
  - Risk Tolerance

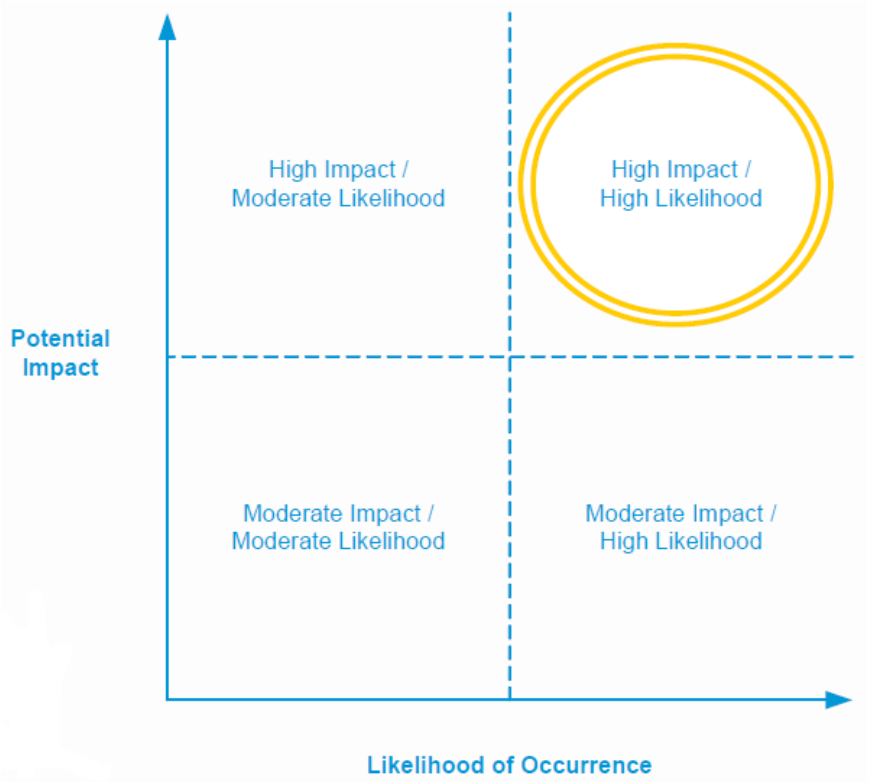
Enterprise Risk Assessment – Risk Map

BAKER TILLY
VIRCHOW KRAUSE, LLP

Candor. Insight. Results.

A clear way to show risk prioritization is through a visual depiction such as a risk map.

> A risk map represents the likelihood of occurrence and the potential impact of the identified risks.
> Risks with higher likelihood and impact will receive the highest priority when developing a plan to manage risks.
> Develop appropriate risk metrics and measurements.

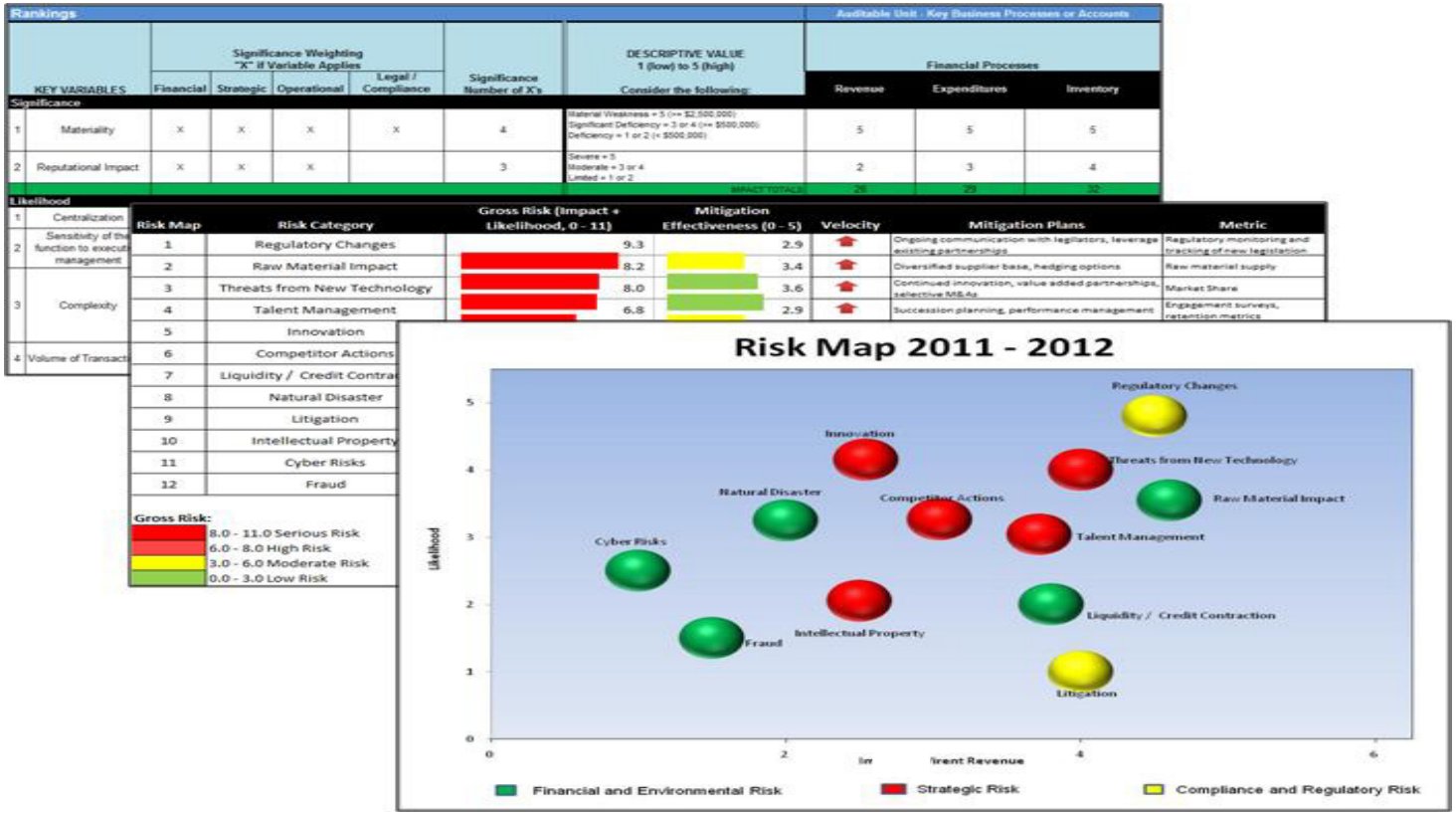


Enterprise Risk Assessment Templates

BAKER TILLY
VIRCHOW KRAUSE, LLP

Candor. Insight. Results.

> Tools to effectively assess risk



Enterprise Risk Assessment – Additional Considerations

BAKER TILLY
VIRCHOW KRAUSE, LLP

Candor. Insight. Results.

> Always assess risks in the context specific to the organization.
  - No two organizations have precisely the same strategies and goals.
  - Therefore, no two organizations should prioritize risks in the same way.
> One best practice is to discuss the prioritization of risks with a group of stakeholders.
> An organization needs to reach a consensus on:
  - Which risks are most important.
  - Where to dedicate time and resources to make positive change.

Risk Response

Risk Response

BAKER TILLY
VIRCHOW KRAUSE, LLP

Candor. Insight. Results.

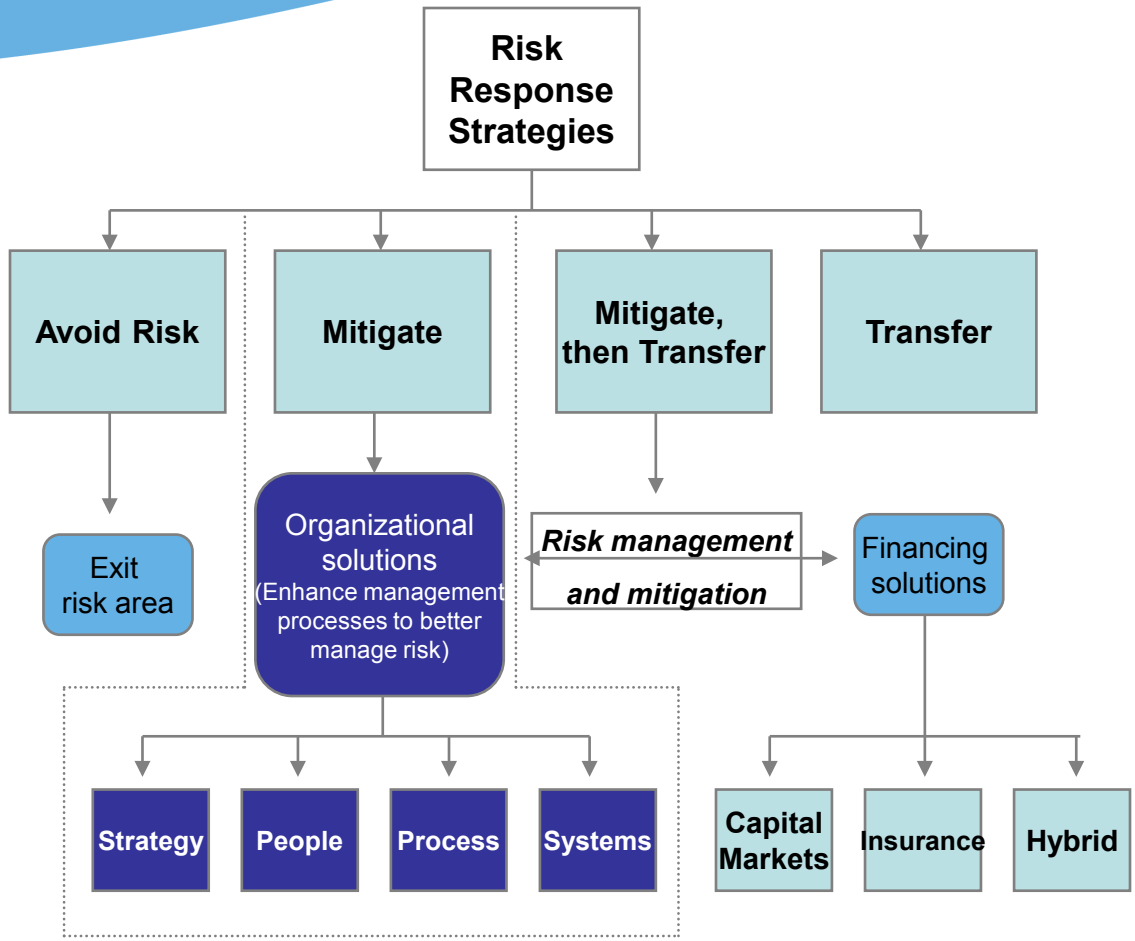
As part of its ERM program, an organization should seek to both mitigate as well as exploit the advantages of risk as it analyzes its treatment of risk. Once risks are organized and prioritized an organization may chooses to do one or many of the following:

> Avoid the risk
> Seek an opportunity and exploit the risk
> Remove the source of risk
> Change the likelihood
> Change the consequences
> Share the risk with another party
> Retain the risk

Risk Response

BAKER TILLY
VIRCHOW KRAUSE, LLP

Candor. Insight. Results.



Source: The Economist Intelligence Unit, Enterprise Risk Management - Implementing New Solutions

Risk Response – Developing a Risk Mitigation Plan

BAKER TILLY
VIRCHOW KRAUSE, LLP

Candor. Insight. Results.

An organization may also develop a plan for addressing the highest priority risk areas and should consider the following:

> Bring together key stakeholders to:

- Discuss current actions being taken to mitigate each identified risk
- Discuss which risk areas may need additional focus
- Discuss potential steps to address those areas

> Determine and agree on an action plan including:

- Specific tasks to perform
- Individuals responsible for each task
- Timeline for the action plan
- Measurement and assessment of changes

Risk Response – Developing a Risk Mitigation Plan (cont.)

BAKER TILLY
VIRCHOW KRAUSE, LLP

Candor. Insight. Results.

When developing a risk mitigation plan organizations should also convene on a regular basis

> Assemble a representative group of individuals who have responsibility for a specific risk
> Discuss progress and issues
> Share best practices

Collaborate with others when necessary

> Individual may not be sufficiently able to address the issue
> May require additional input from outside parties
> Engage the internal audit department or external consultants to supplement the available skills and capacity

Risk Response – Developing a Risk Mitigation Plan: Reporting

BAKER TILLY
VIRCHOW KRAUSE, LLP

Candor. Insight. Results.

Organizations should report progress, successes and obstacles to management and/or the board of trustees

> Should be on a regular basis

> Increase understanding of the challenges

> Make cases for additional resources, as necessary

Sustaining ERM

Sustaining ERM

BAKER TILLY
VIRCHOW KRAUSE, LLP

Candor. Insight. Results.

- Consistent monitoring and review is necessary to ensure key controls and mitigation efforts remain appropriate and are implemented
- Although each individual is responsible for managing the risk in his or her area, there should be a recurrent independent review
- Outstanding gaps or observations should be appropriately communicated
- Leverage technology to monitor risks and assign mitigation activities (workflow)

Sustaining ERM

BAKER TILLY
VIRCHOW KRAUSE, LLP

Candor. Insight. Results.

Sustaining an effective ERM environment may be accomplished via a combination of a push/pull approach, mainly through two programs:

> ***Push:*** Risk Monitoring Program whereby every associate is made responsible to disclose, within their level of oversight, the occurrence of a critical control point indicating a potential out-of-control condition or any risk events potentially effecting the enterprise

> ***Pull:*** Risk Owner Assessment Program whereby the risk owners are periodically polled to assess their business risks for changes and management effectiveness

Sustaining ERM – Evaluation of the ERM Program

BAKER TILLY
VIRCHOW KRAUSE, LLP

Candor. Insight. Results.

- Ultimately the responsibility for risk management lies with the management and the board.
- Risk management should be periodically evaluated as to its adequacy to protect enterprise assets, reputation, and ongoing operations.
- Reporting to the Audit Committee, the internal audit function should possess the objectivity and good judgment to examine, evaluate, report, and recommend improvements on the adequacy and effectiveness of management's ERM program.

Closing thoughts

Additional Considerations – Common Challenges

BAKER TILLY
VIRCHOW KRAUSE, LLP

Candor. Insight. Results.

There are several common challenges that organizations face when considering or implementing ERM including:

> Lack of visible, active support from Board or CEO-level authority
> Implementing without a framework or plan
> Overselling the value
> Too early integration with no tangible value
> Supplying TOO MUCH information to digest
> Over-facilitating on part of the project team
> Implementing as a project or part time endeavor
> Relying too much on ERM as the end all for risk management at the expense of other business tools

Additional Considerations – Getting Started

BAKER TILLY
VIRCHOW KRAUSE, LLP
Candor. Insight. Results.

In order to overcome barriers and obstacles to success:

> Set initial achievable targets
- Program organization and infrastructure
- Objectives and goals
- Initial strategy

> Training and communication
- ERM core team
- Executives, process owners and other relevant stakeholders

> Keep it simple – start with risk assessment
- Entity wide
- Specific process

> Evaluate results and refine strategy

Additional Considerations – Success Factors

BAKER TILLY
VIRCHOW KRAUSE, LLP

Candor. Insight. Results.

- Strong and visible support from management
- Dedicated team of cross-functional staff to operationalize ERM and integrate into business practices
- Align ERM to the Key strategic and financial objectives of the organization and to the business processes
- Recognize that ERM is a process and takes time to evolve
- Provide adequate training and supporting tools
- Leverage well-accepted processes within the organization and introduce ERM as a value add, rather than a new, stand-alone program
- Look for new, innovative ideas from employees and external sources
- Proceed incrementally and leverage success – start with an entity-wide risk assessment and assess next steps based upon the successes of this initial effort

BAKER TILLY
VIRCHOW KRAUSE, LLP

Candor. Insight. Results.

Questions & Comments

www.bakertilly.com

an independent member of
BAKER TILLY
INTERNATIONAL