THE POWER OF BEING UNDERSTOOD

AUDIT I TAX I CONSULTING

RSM

COSO FRAMEWORK UPDATE
ENTERPRISE RISK MANAGEMENT

STATE OF MAINE

May 24, 2016

RSM

Today’s presenters

Paul Kiley
RSM
Partner - Boston
Risk Advisory Services

Agenda-COSO

Topic	Minutes
COSO background	5
The update process	5
The 17 principles and changes to the 5 components	25
The implementation process and lessons learned	15

COSO BACKGROUND

COSO overview

American Accounting Association | Thought Leaders in Accounting

AICPA American Institute of CPAs®

fei Financial Executives International

ima® The Association of Accountants and Financial Professionals in Business

The Institute of Internal Auditors

- The Committee of Sponsoring Organizations of the Treadway Commission (COSO) is a joint initiative of five sponsoring organizations formed in 1985
- Provides thought leadership through the development of frameworks and guidance on:
  - Internal control
  - Enterprise risk management
  - Fraud
- Designed to improve organizational performance and governance, and to reduce the extent of fraud in organizations
- Released original *Internal Control-Integrated Framework* in 1992 which has become the most widely used control framework used in management's SOX assertion

Select COSO frameworks

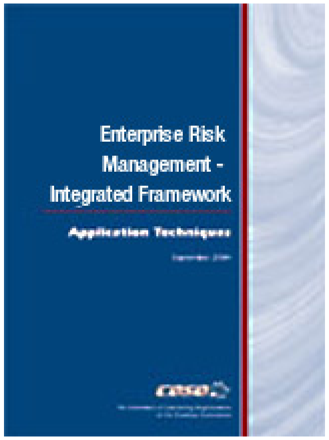
COSO
Internal Control — Integrated Framework
Illustrative Tools for Assessing Effectiveness of a System of Internal Control

Internal Control – Integrated Framework (2013)

COSO
Internal Control over Financial Reporting – Guidance for Smaller Public Companies

ICOFR – Guidance for Smaller Public Companies (2006)

Internal Control – Integrated Framework (1992)



Enterprise Risk Management - Integrated Framework (2004)

THE UPDATE PROCESS

The update process

- Why was the COSO Framework updated?
  - The existing framework was issued in 1992
  - Updated to remain relevant and useful
- This is a “refresh” not a “start over”.
  - Principles based
  - Increased guidance and examples

Overview of what is and is not changing

Update expected to increase ease of use and broaden application

What is *not* changing...

- Core definition of internal control
- Three categories of objectives and five components of internal control
- Each of the five components of internal control are required for effective internal control
- Important role of judgment in designing, implementing and conducting internal control, and in assessing its effectiveness

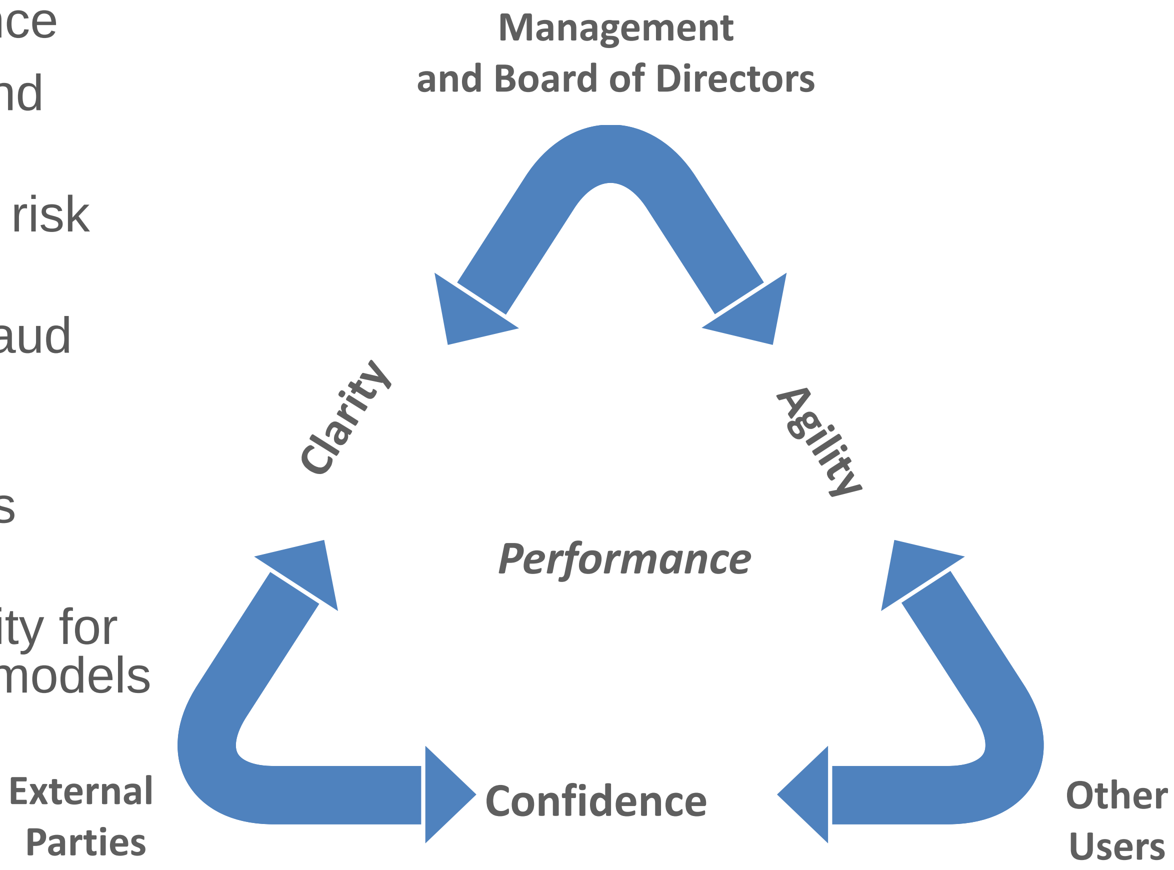
What is changing...

- Changes in business and operating environments considered
- Operations and reporting objectives expanded
- Fundamental concepts underlying five components articulated as principles with points of focus as additional guidance
- Additional approaches and examples relevant to operations, compliance, and non-financial reporting objectives added

Slide Source: COSO IC-IF Outreach Deck_12 29 11 (http://www.ic.coso.org/pages/about-the-project.aspx)

Intended benefits of updated Framework

- Improve governance
- Expand use beyond financial reporting
- Improve quality of risk assessment
- Strengthen anti-fraud efforts
- Adapt controls to changing business needs
- Greater applicability for various business models



Slide Source: COSO IC-IF Outreach Deck_12 29 11
(http://www.ic.coso.org/pages/about-the-project.aspx)

Transition

- Updated Framework was issued May 14, 2013
- COSO continued to make available the original framework during the transition period extending through December 15, 2014, after which time COSO considered it as having been superseded

- Updated Framework supersedes existing Framework and *Internal Control over Financial Reporting – Guidance for Smaller Public Companies*

THE 17 PRINCIPLES AND CHANGES TO THE 5 COMPONENTS

RSM

Effective internal control

- Effective internal control provides reasonable assurance regarding the achievement of objectives and requires that:
  - Each component and each relevant principle is present and functioning
  - The five components are operating together in an integrated manner

Internal control principles

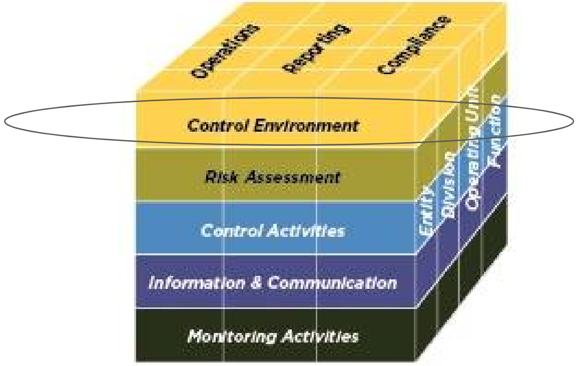
Control Environment	1. Demonstrates commitment to integrity and ethical values 2. Exercises oversight responsibility 3. Establishes structure, authority and responsibility 4. Demonstrates commitment to competence 5. Enforces accountability
Risk Assessment	6. Specifies suitable objectives 7. Identifies and analyzes risk 8. Assesses fraud risk 9. Identifies and analyzes significant change
Control Activities	10. Selects and develops control activities 11. Selects and develops general controls over technology 12. Deploys through policies and procedures
Information & Communication	13. Uses relevant information 14. Communicates internally 15. Communicates externally
Monitoring Activities	16. Conducts ongoing and/or separate evaluations 17. Evaluates and communicates deficiencies

Slide Source: COSO IC-IF Outreach Deck_12 29 11
(http://www.ic.coso.org/pages/about-the-project.aspx)

Control environment

Control environment

The set of standards, processes, and structures that provide the basis for carrying out internal control across the organization.



Newly defined principles

1. The organization demonstrates a commitment to integrity and ethical values.
2. The board of directors demonstrates independence of management and exercises oversight of the development and performance of internal control.
3. Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
4. The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
5. The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

Control environment – changes

- Five principles outline what is commonly called the “tone at the top”
- Expanded discussion and consideration of governance roles and notion of risk oversight
- Includes considerations for internal control in complex business environments
    - Outsourced service providers
    - Business partners
    - External partners

Example principle and related points of focus

Control Environment

1. Demonstrates commitment to integrity and ethical values

Points of Focus:

- Sets the tone at the top
- Establishes standards of conduct
- Evaluates adherence to standards of conduct
- Addresses deviations in a timely manner

- Points of focus are typically important characteristics of principles that can be used to facilitate designing, implementing, and conducting internal control
- There is no requirement to separately assess whether points of focus are in place
- Points of focus may not be suitable or relevant, and others may be identified
- Points of focus may facilitate designing, implementing, and conducting internal control

Example of controls embedded in other internal control components

Component

Control Environment

Principle

1. Demonstrates commitment to integrity and ethical values.

Controls embedded in other components may effect this principle

Human Resources review employees' confirmations to assess whether standards of conduct are understood and adhered to by staff across the entity

Control Environment

Management obtains and reviews data and information underlying potential deviations captured in whistleblower hot-line to assess quality of information

Information & Communication

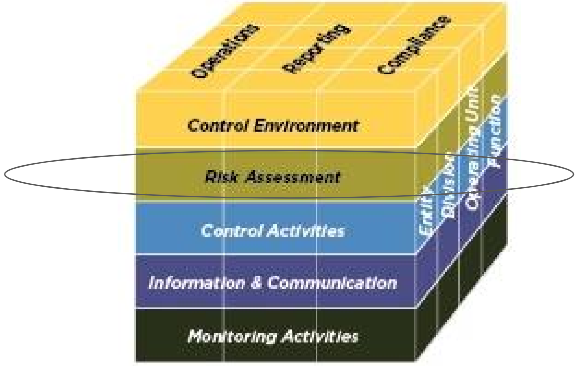
Internal Audit separately evaluates Control Environment, considering employee behaviors and whistleblower hotline results and reports thereon

Monitoring Activities

Risk assessment

Risk assessment

A dynamic and iterative process for identifying and assessing risk to the achievement of objectives.



Newly defined principles

6. The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
7. The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.
8. The organization considers the potential for fraud in assessing risks to the achievement of objectives.
9. The organization identifies and assesses changes that could significantly impact the system of internal control.

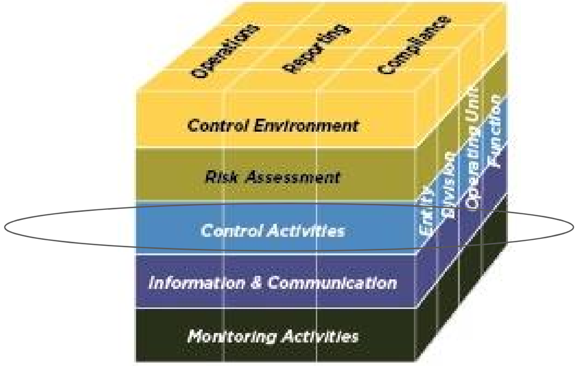
Risk assessment – changes

- Principle specifically focused on consideration of fraud
- Clarifying risk assessment includes
  - Risk identification
  - Risk analysis
  - Risk response
- Expands discussion on management’s need to understand changes in internal and external factors

Control activities

Control activities

The actions established through policies and procedures that help ensure that management's directives to mitigate risks to the achievement of objectives are carried out.



Newly defined principles

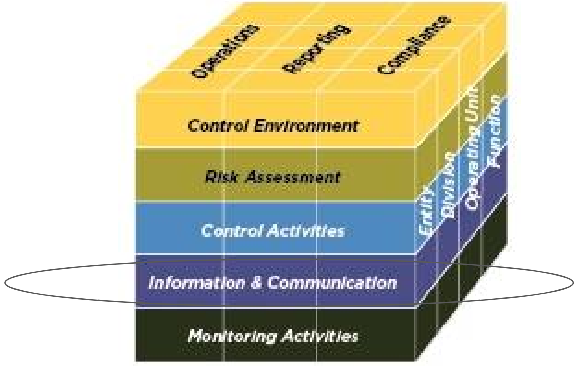
10. The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
11. The organization selects and develops general control activities over technology to support the achievement of objectives.
12. The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.

Control activities – changes

- Broadening discussion of technology
- Expanded discussion of automated control activities and general controls over technology
- Clarifies that control activities are actions established by policies and procedures not the policies and procedures themselves

Information and communication

Information and communication



Communication is the continual, iterative process of providing, sharing, and obtaining necessary information. Internal communication is the means by which information is disseminated throughout the organization. External communication enables inbound communication and provides external information.

Newly defined principles

13. The organization obtains or generates and uses relevant, quality information to support the functioning of other components of internal control.
14. The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
15. The organization communicates with external parties regarding matters affecting the functioning of internal control.

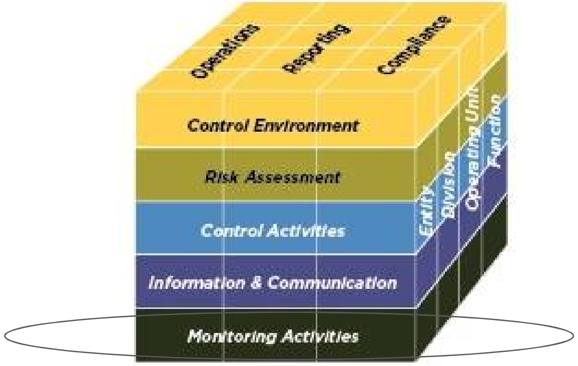
Information and communication – changes

- Emphasizes importance of quality of information
- Expands on reliability and protection of information
- Reflects impacts of technology on speed, means, and quality of flow of information
- Emphasizes importance of communication outside the entity (such as third-party service providers)

Monitoring activities

Monitoring activities

Ongoing evaluations, separate evaluations, or some combination of the two used to ascertain whether each of the five components of internal control are present and functioning.



Newly defined principles

16. The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
17. The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

Monitoring activities - changes

- Clarifies that monitoring activities apply to all components of the Framework, not only control activities
- Includes two main categories of monitoring activities
  - Ongoing evaluations
  - Separate evaluations
- Expands discussion of technology and external service providers

Scalability

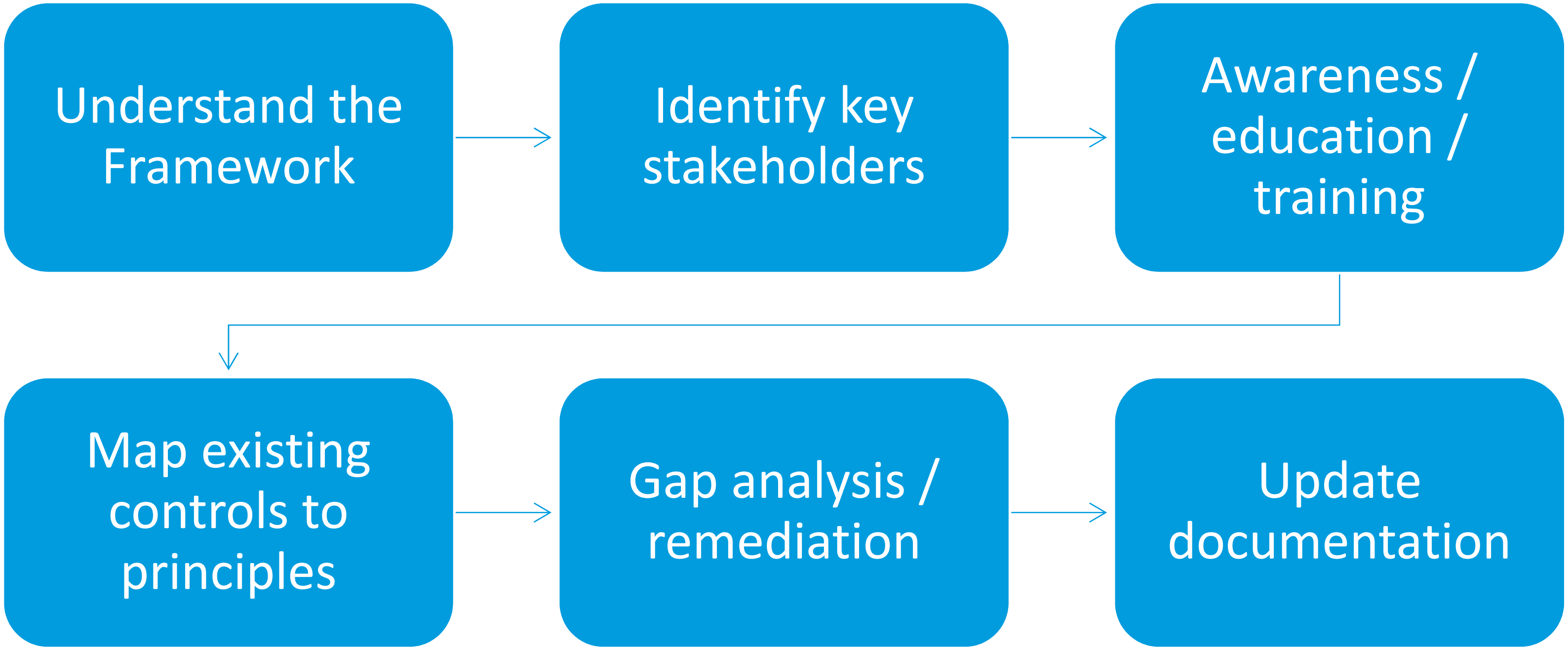
- Appendix C of the Framework provides considerations for smaller entities and governments
- Key consideration factors are provided for:
  - Segregation of duties
  - Management override
  - Board of directors
  - Information technology
  - Monitoring activities

THE IMPLEMENTATION PROCESS

Impact of adopting the updated Framework

- Initial level of effort will vary by organization depending on their existing level of documentation, stakeholder involvement and locations
- Provides flexibility in applying the Framework to multiple, overlapping objectives across the entity
  - Easier to see what is covered and what is missing
  - May reduce likelihood of considering controls that are irrelevant
  - May reduce the number of discrete risks assessed and mitigated
- Potential for initial deficiencies if the system of internal control does not address each of the principles
- Heightened focus on entity-wide controls provides a platform for addressing increased entity-level scrutiny from authoritative bodies (e.g. SEC, PCAOB, AICPA)

Steps for implementing 2013 Framework



Understand the Framework

Identify key stakeholders

Awareness / education / training

Map existing controls to principles

Gap analysis / remediation

Update documentation

Timing considerations

- Updated Framework will supersede original Framework on December 15, 2014
- Earlier implementation encourage
- During the transition external reporting should disclose which version of the Framework was used

Observations/Lessons Learned

- Most common gaps (from Commercial sector) included:
  - Informal Risk Assessment activities
  - No specific Fraud Risk Assessment
  - Insufficient oversight of third-party service providers

- “Compendium” on ICFR was under-utilized

Resources

- RSM Whitepaper, *An Overview of COSO's 2013 Internal Control-Integrated Framework*
  http://RSM.com/Insights/2013-COSO-Framework-Update-webcast-and-whitepaper
- COSO Resources
  - *Internal Control-Integrated Framework*
    - Executive summary
    - Framework and Appendices
    - Illustrative tools for assessing effectiveness of a system of internal control
  - *Internal Control over External Financial Reporting, a Compendium of Approaches and Examples*
    www.coso.org

ENTERPSISE RISK MANAGEMENT

Learning objectives

- ❖ Enterprise Risk Management (ERM) Definitions and Drivers
- ❖ Traditional Risk Management vs. ERM
- ❖ ERM Frameworks (COSO)
- ❖ ERM Practical Implementation Considerations and Key Risks
- ❖ Lessons Learned

Why ERM Is Important

Underlying principles:

- Every entity, whether for-profit or not, exists to realize value for its stakeholders.
- Value is created, preserved, or eroded by management decisions in all activities, from setting strategy to operating the enterprise day-to-day.

RSM

What is “Business Risk”??

The threat that an event or action/inaction will adversely affect an organization’s ability to ***achieve its business and strategic objectives***

– OR –

- Something **bad** will happen
- Something **good** won’t happen

ERM definitions

ERM is a management discipline that focuses on managing risk from a holistic point of view. It’s popularity grew significantly after the numerous failures resulting from the financial crisis.

Official definitions:

Institute of Internal Auditors

“…a structured, consistent and continuous process across the whole organization for identifying, assessing, deciding on responses to and reporting on opportunities and threats that affect the achievement of its objectives.”

COSO ERM Integrate Framework (2004)

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

ISO 31000 (2009)

“A systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, monitoring and reviewing risk.”

ERM Jump Start

- Many companies are interested in developing an ERM program, but have trouble defining what this means in their organization.
  - Various factors affect the way ERM is executed at companies, including their ***size, management culture, prior/current risk assessment activities, mandate and buy-in from executives and the Board***, etc.

- ERM has been described as a **“journey” rather than a “destination”.**
- The key is to begin that journey, without trying to get it perfect on the first iteration
- Remember the 3 definitions, there is not really a “right” or “wrong” way to do ERM.

Traditional risk management vs. ERM

Traditional Risk Management

- Tactical, compliance focused
- Silo-based processes
- Business line or risk type view
- Looks at risks individually
- Business decisions not closely linked to risks
- Driven by Risk Management and Internal Audit
- Supported by rules

Enterprise Risk Management

- Strategic, performance focused
- Consistent risk management approach across the enterprise
- Holistic view of key risks
- Considers risk interactions
- Business decisions based on a clear understanding of risks
- Driven by the board and owned by the business
- Supported by a “risk culture”

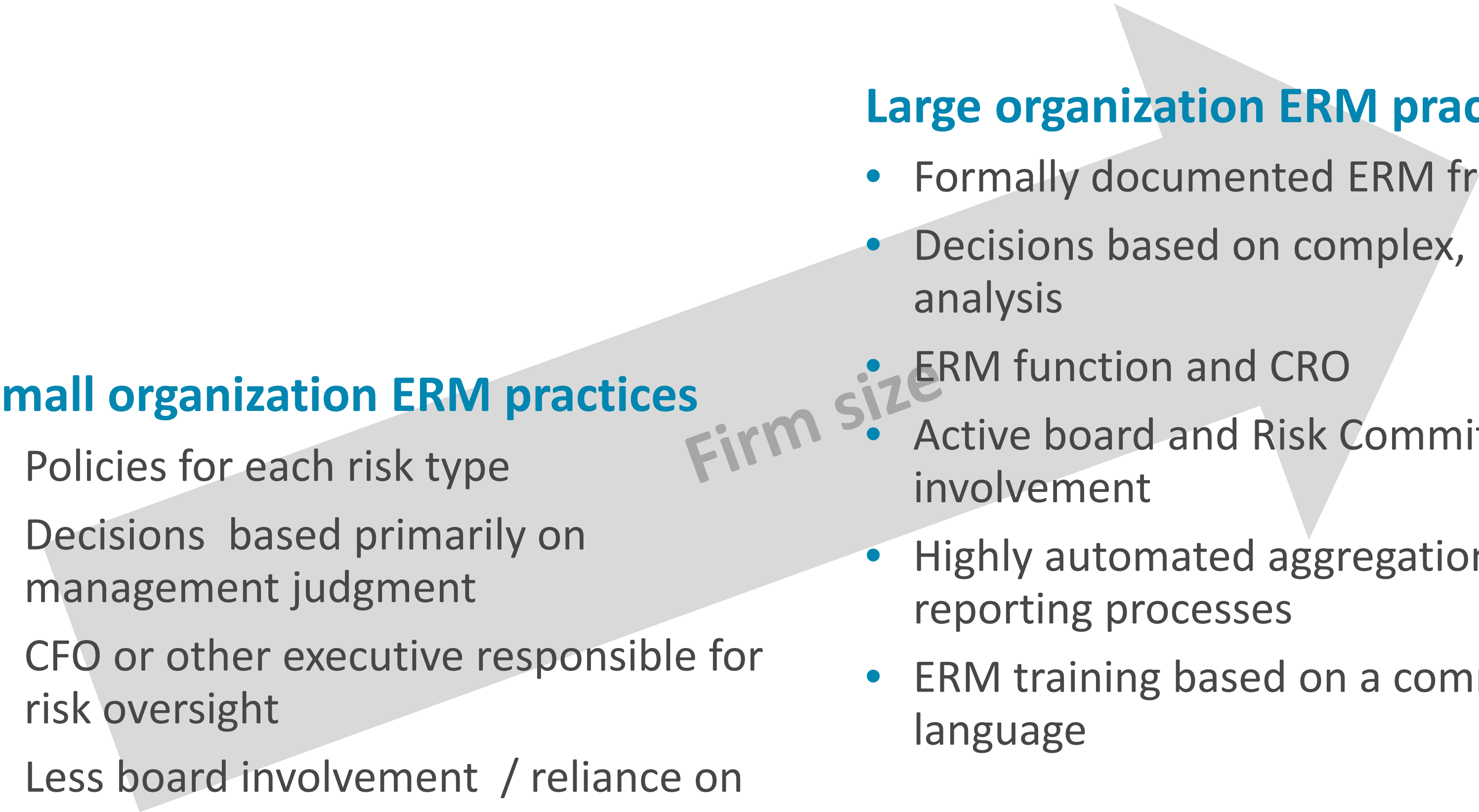
ERM Value

“A rattlesnake may bite us every now and again, but we knew it was there and how much it might hurt…”

Rick Buy, Executive Vice President and Chief Risk Officer…

Enron, 2000

Range of ERM Practices



Small organization ERM practices

- Policies for each risk type
- Decisions based primarily on management judgment
- CFO or other executive responsible for risk oversight
- Less board involvement / reliance on Audit Committee
- Manual aggregation processes
- Tactical risk management training

Large organization ERM practices

- Formally documented ERM framework
- Decisions based on complex, data-driven analysis
- ERM function and CRO
- Active board and Risk Committee involvement
- Highly automated aggregation and reporting processes
- ERM training based on a common risk language

Frameworks

In order to implement ERM, it makes sense to use a model or *framework*

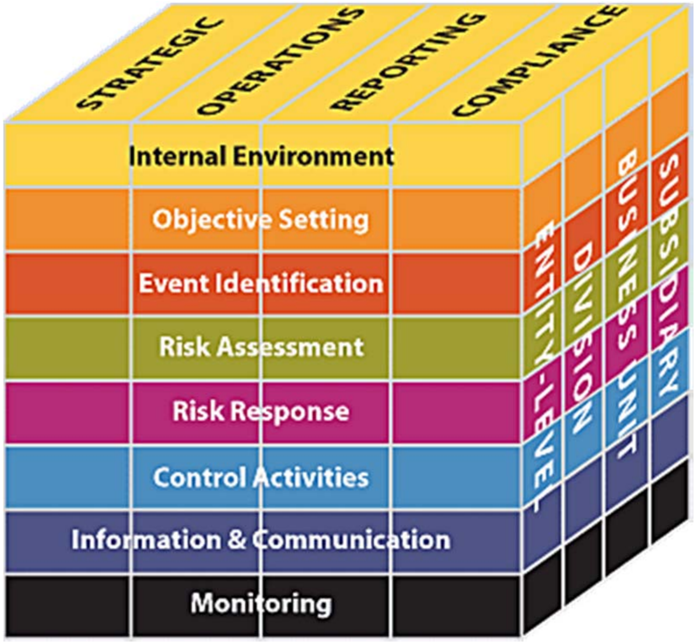
ERM frameworks define essential components, suggest a common language, and provide clear direction and guidance for enterprise risk management.

The most widely used frameworks are COSO and ISO-31000

The ERM Framework

- Entity objectives can be viewed in the
- context of four categories:

  - Strategic
  - Operations
  - Reporting
  - Compliance



RSM

Components of Enterprise Risk Management

Enterprise risk management consists of eight interrelated components. These 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 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.

.

Components of Enterprise Risk Management

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.

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.

.

Components of Enterprise Risk Management (continued)

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

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.

A Practical Approach to Implementing ERM

Start with the basics:

- Understand what you already have
- Using a framework, determine where you want to go
  - “Why” are we doing this?
  - “What” do we want to get out of it—upside vs. downside risk
  - How will your organization’s culture react to ERM adoption?
  - “Who” in your organization (or outside)will be involved at each phase – what are the skill sets necessary
- Determine your time horizon – while there are near term benefits that can be achieved, most ERM frameworks take 18 months or longer before they take root

NEXT, we’ll cover the basic building blocks of a holistic ERM program:

Implementing an ERM program

Strategic and Business Objectives

- ❖ What the organization is trying to accomplish
- ❖ Strategic imperatives and underlying business assumptions
- ❖ “Headwinds” and “tailwinds” associated with these imperatives
- ❖ Critical external and internal drivers affecting imperatives
- ❖ How the organization measures the performance of these imperatives

Risk Governance

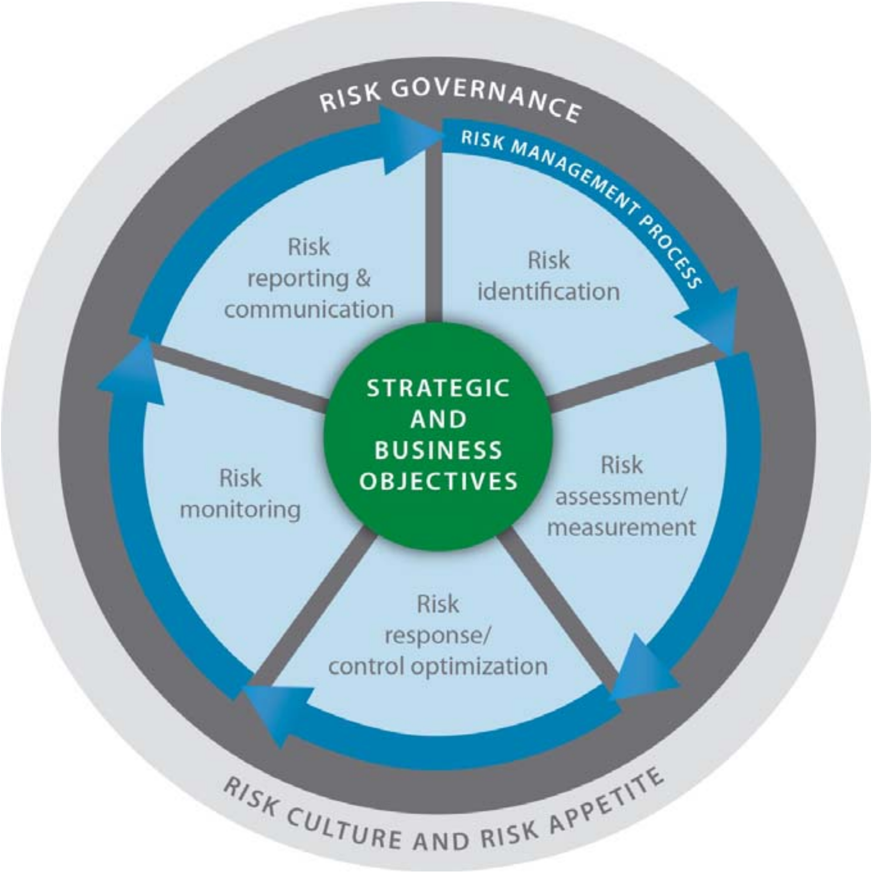
- ❖ Board oversight
- ❖ Risk Committees (including Board and executive ERM committees)
- ❖ Policy governance
- ❖ Clear roles and responsibilities for identifying, assessing and managing risks
- ❖ Continuous alignment with corporate strategy and objectives

Risk Culture and Risk Appetite

- ❖ Risk management training and communication
- ❖ Clear roles and responsibilities for identifying, assessing and managing risks
- ❖ Tone-at-the-top that is supportive of risk management
- ❖ Code of conduct/ethics
- ❖ Risk factors included in incentive plans and performance evaluations

Risk Management Processes

- ❖ Risk identification
- ❖ Risk assessment/measurement
- ❖ Risk response/control
- ❖ Risk monitoring
- ❖ Risk reporting and communication
- ❖ Ongoing program optimization
- ❖ Technology enablement


RISK GOVERNANCE
RISK MANAGEMENT PROCESS
Risk identification
Risk assessment/ measurement
Risk response/ control optimization
Risk monitoring
Risk reporting & communication
STRATEGIC AND BUSINESS OBJECTIVES
RISK CULTURE AND RISK APPETITE

ERM Framework – High Level

An ERM Framework should include:

- Risk governance
- Risk appetite setting
- Enterprise-wide risk management processes
    - Identification of risks
    - Assessment / measurement of risks
    - Monitoring of risks and actions to address risks
    - Management of risk through controls/risk responses
    - Reporting of risks and the status of action plans
- Integration with business decision-making
- Establishment of a strong risk culture

Risk Appetite

- An effective ERM program relies on the establishment and communication of the company’s risk appetite
  - Helps employees to understand the specific risks that the company is willing and not willing to take.
  - Provides a means for ensuring that actual risk-taking is consistent with the company’s risk-taking capacity.

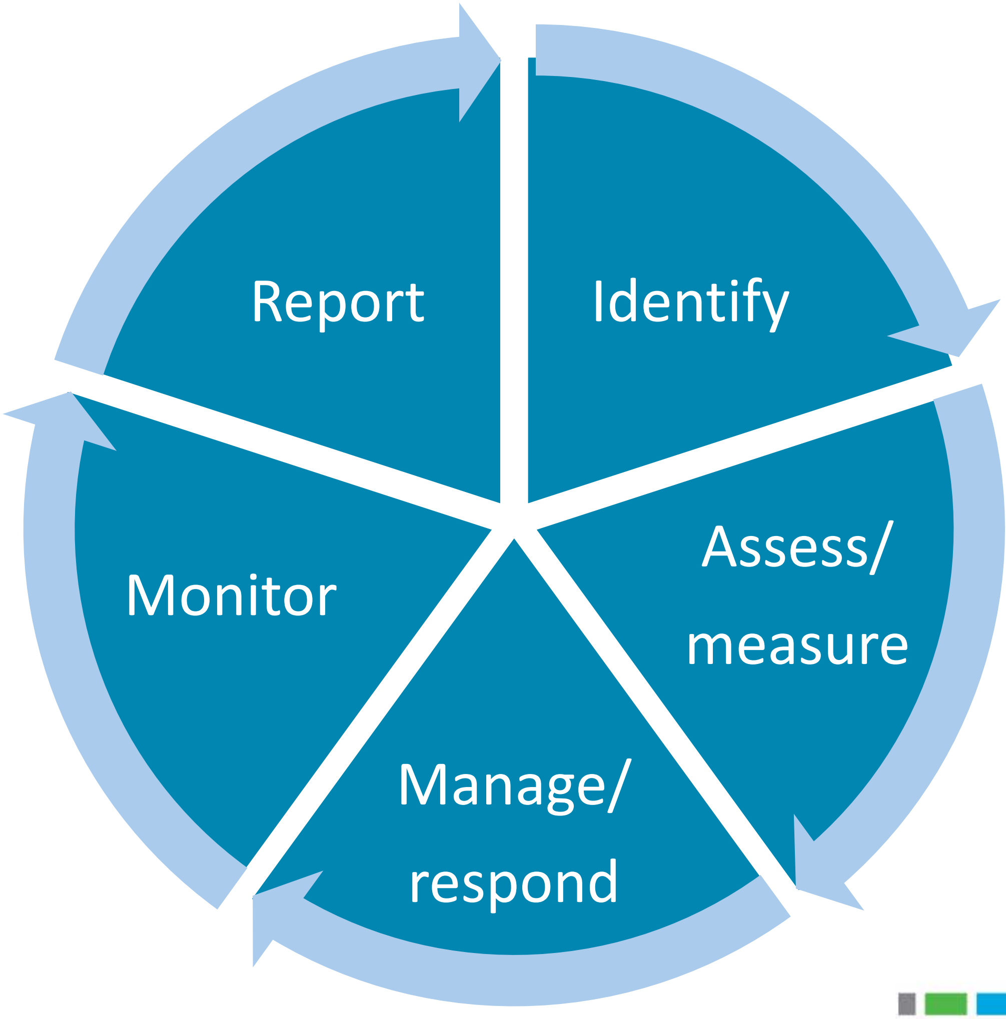
Risk Appetite

- There are many ways to define risk appetite:
  - Statements, such as “a zero tolerance for compliance risk” or “target debt rating of AAA”
  - Specific services and outcomes that are outside of the company’s risk tolerance
  - Metrics that define risk thresholds, such as financial measures (e.g., ROE target) or limits (e.g., % of total risk exposure)

Are you able to articulate your company’s appetite or tolerance for risk?

Risk Management Processes

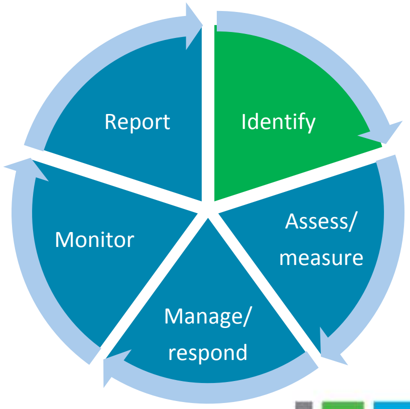
- Risk management processes are grouped in different ways but generally include the following:
- Ideally, each of these processes should be ongoing rather than, for example, annual.



Risk Identification

- Risk identification processes should begin with appropriate planning:
  - Mapping of the company’s business lines and processes
  - Determination of the risk types to be included in the process (e.g., operational, legal, reputational)
  - Identification of resources responsible for the process in each area

- Risks can be identified through various methods, such as *interviews, surveys and/or facilitated workshops*
  - Different levels of the organization may have different perspectives on risks
  - Include emerging risks
  - Be wary of risks that are really the absence of controls



Risk Identification Process

- Determine participants

- Educate them with a “pre-read”

- Live interviews are better than surveys

- Assemble the results of the surveys/interviews into Risk Statements

Example: Identification of Strategic Risks

- Strategic risks are risks that are material to a company’s ability to execute its strategy and achieve its business objectives.
- Sources of strategic risk to consider:

<u>External</u>

- – Financial Markets
- – Talent Markets
- – Brand
- – Partnering
- – Political Environment
- – Regulators
- – Suppliers

<u>Internal</u>

- – Planning
- – Execution
- – Employee engagement
- – Access to capital
- – Infrastructure
- – Readiness

COSO Risk Model

External Factors

Economic	*Natural Environment*	*Political*	*Social*	*Technological*
• Capital availability • Credit issuance, default • Concentration • Liquidity • Financial markets • Unemployment • Competition • Mergers/acquisitions	• Emissions and waste • Energy • Natural disaster • Sustainable development	• Governmental changes • Legislation • Public policy • Regulation	• Demographics • Consumer behavior • Corporate citizenship • Privacy • Terrorism	• Interruptions • Electronic commerce • External data • Emerging technology

Internal Factors

Infrastructure	*Personnel*	*Process*	*Technology*
• Availability of assets • Capability of assets • Access to capital • Complexity	• Employee capability • Fraudulent activity • Health and safety	• Capacity • Design • Execution • Suppliers/ dependencies • Mergers/acquisitions	• Data integrity • Data and system availability • System selection • Development • Deployment • Maintenance

ERM Framework

Phase 2 – Risk Assessment and Measurement

- Rank and prioritize the identified risks according to:
  - **Impact** – the financial, operational, strategy and compliance implications
  - **Likelihood**
  - **Other Criteria-** Control Effectiveness, Velocity
- Coordinate a facilitated session with the ERM core team (or executives) to evaluate the prioritization results and discuss:
  - Agreement with the risk prioritization
  - Questions or concerns relative to the risk prioritization
  - High and moderate risks to evaluate impact and likelihood factors for clarification and understanding of overall risk exposure
  - Risks with significant deviation in results / spread in prioritization results to gain insight on reasons for variation

Facilitated Sessions

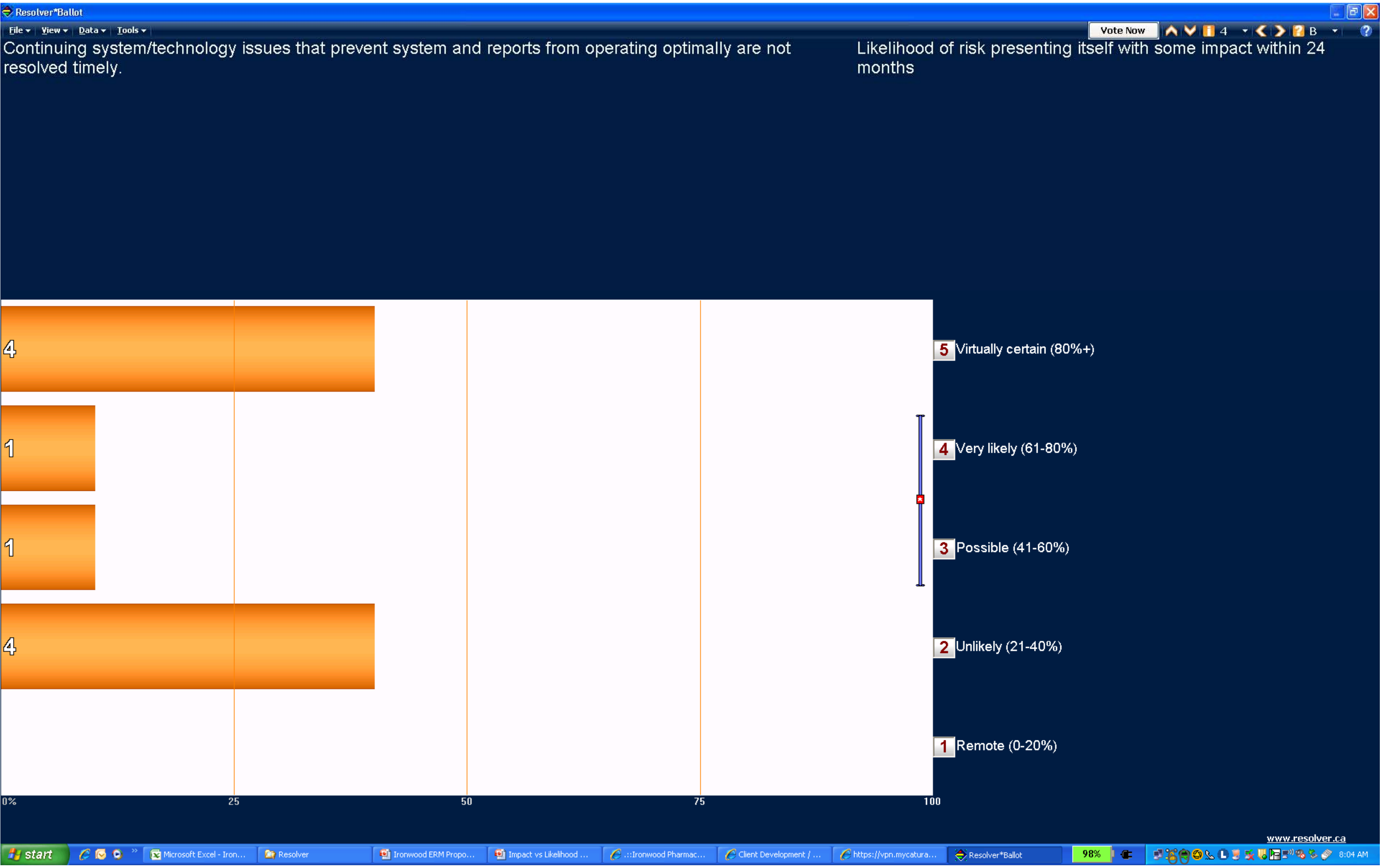
- Facilitated sessions are one of the most important tools in the ERM arsenal

- Get senior executives offsite for AT LEAST ½ a day

- They wont want to do it, but later they will say it added the most value of the whole effort

RSM

Tools- BPS Resolver Voting Software



Continuing system/technology issues that prevent system and reports from operating optimally are not resolved timely.

Likelihood of risk presenting itself with some impact within 24 months

5 Virtually certain (80%+)

4 Very likely (61-80%)

3 Possible (41-60%)

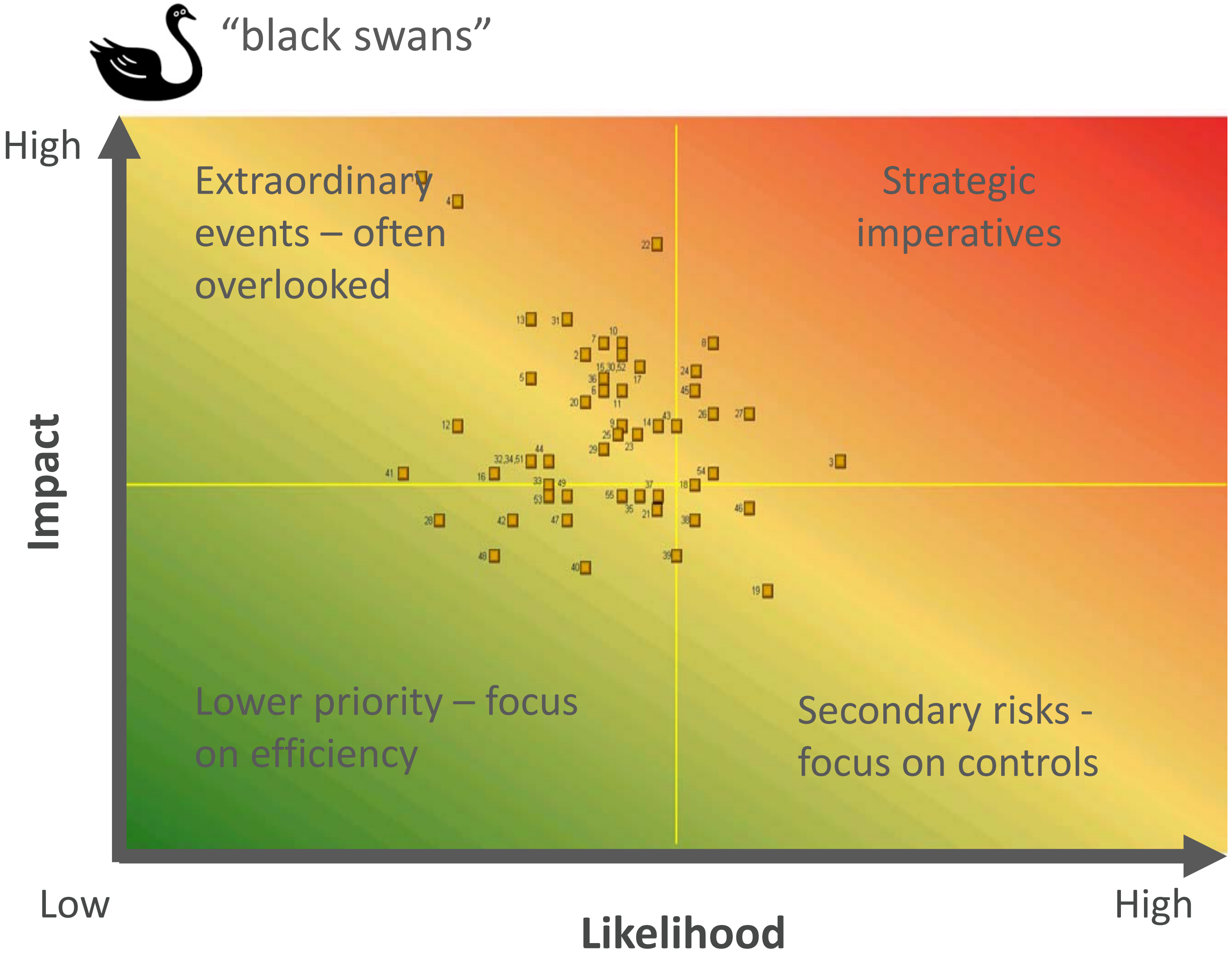
2 Unlikely (21-40%)

1 Remote (0-20%)

this risk occurs?
(Select the worst one for your vote…)

Impact Rating Scale			
Score	Financial (damages, fines, loss of business, etc.)	Reputational	Operational
5	Devastating financial impact (may cause overall organizational failure)	Could result in **a sustained negative impact** to reputation and / or national / global media coverage (front page of prominent media).	Non achievement of management objectives that could have a **catastrophic** operational impact or significant loss of goal achievement.
4	Material financial impact	Could result in **a severe negative impact** to reputation and / or national media coverage.	Non achievement of key objectives that could result in **severe** operational damage or loss of goal achievement.
3	Significant financial impact	Could result in **a moderate negative impact** to reputation and /or regional media coverage.	Significant threat to one or more business objectives that could result in **moderate operational damage** or loss of goal achievement.
2	Relatively small financial and/or strategic impact	Could result in **a limited negative** impact on reputation and/or local media coverage.	Could result in a limited, but **manageable**, operational or goal impact.
1	Neither financial nor strategic impact requiring management time and resources	No likely impact on reputation.	Not likely to result in any operational impact or loss of goal achievement.

Sample Risk Assessment Voting Output



“black swans”

Extraordinary events – often overlooked

Strategic imperatives

Lower priority – focus on efficiency

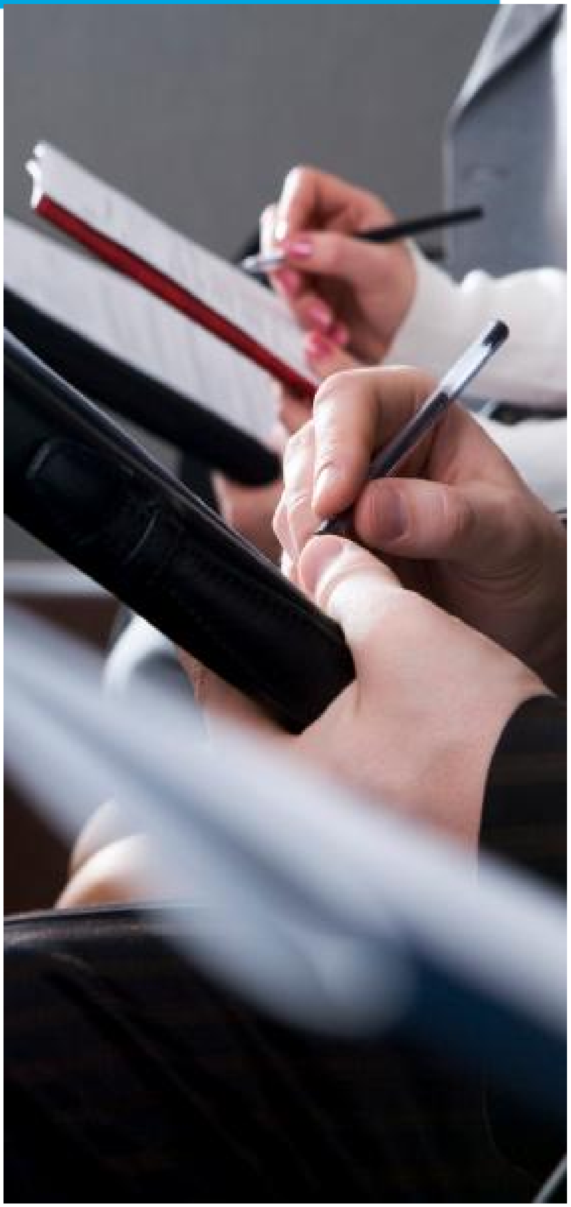
Secondary risks - focus on controls

ERM Framework

Phase 3 – Risk Response/Control

Phase III will allow you to identify and assess how each key risk is mitigated and identify existing control gaps. In this phase we will:

- Identify risk treatment for high and moderate risks
- Coordinate a discussion with the ERM core team to evaluate risk treatments and discuss:
  - Agreement with mitigation analysis
  - Identified risk gaps
  - Evaluate design and known effectiveness of mitigating strategies
  - Risk management strategy
    1. Avoid
    2. Retain
    3. Reduce
    4. Transfer
  - Gap remediation strategy



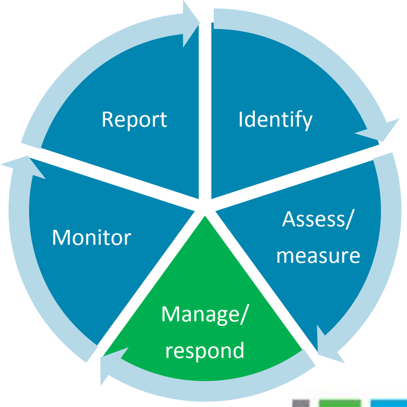
Risk Management / Responses

- Risk responses should be based on assessment of loss frequency and impact
  - Management actions should be specific to reducing likelihood or impact, depending on which one was assessed as high

The most common risk responses include:

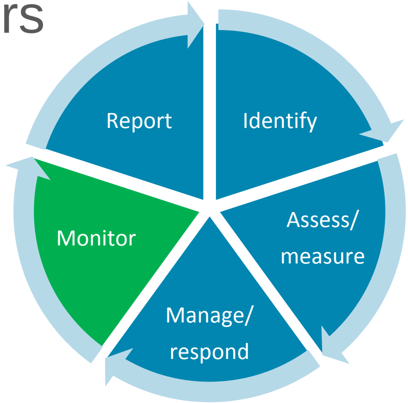
- Avoid (get out)
- Accept/retain (monitor)
- Reduce (institute controls)
- Transfer or share (partner with someone)

- Action plans with assigned owners should be developed and monitored by a risk committee



Risk Monitoring

- Risk monitoring should follow from risk assessments
  - Higher risks should be monitored more frequently and in more depth
- Key risk indicators (KRIs) are critical to early identification of risks and, as a result, fewer surprises
  - KRIs should be forward-looking
  - Key Performance Indicators (KPIs), are primarily backward-looking



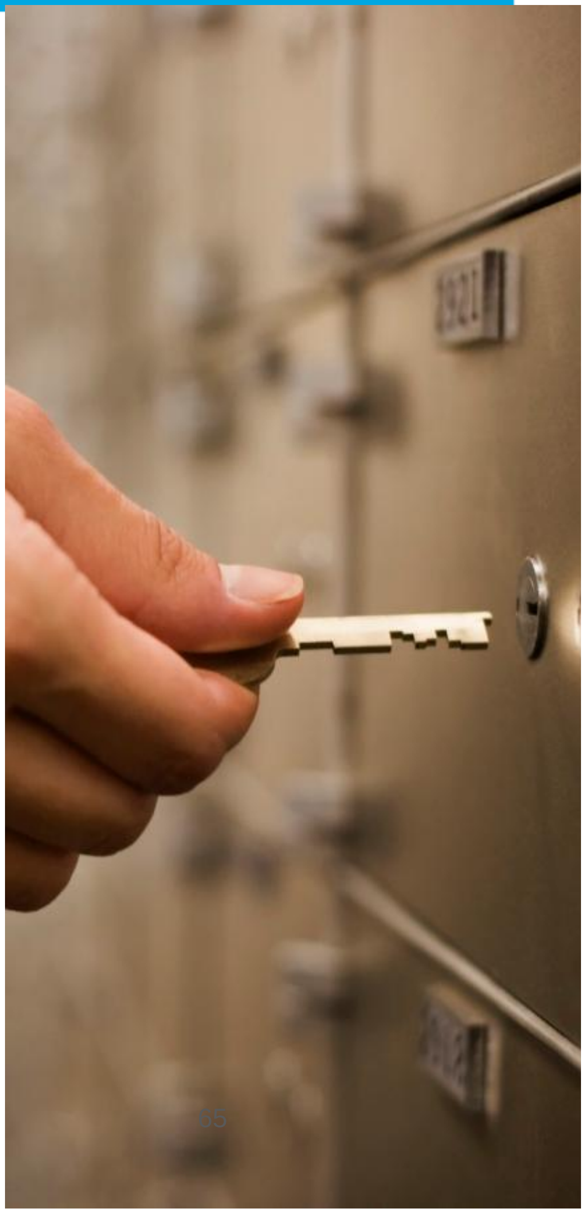
Report

Identify

Assess/ measure

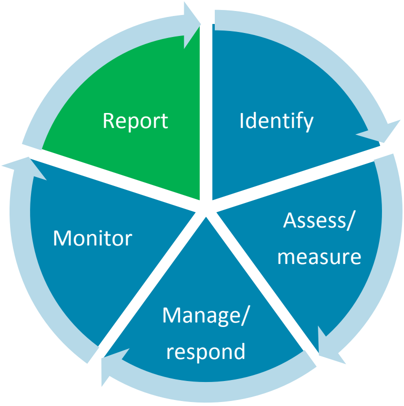
Manage/ respond

Monitor



Risk Reporting

- Reporting should also follow from risk assessments, with higher risks reported in more depth
- Emphasis of risk reporting should be on highlighting *key risks* and recommendations for and status of *management action*
- Volumes of detail should be avoided, particularly for board reporting
- Reports should include early indicators and emerging risks
- Best practices include the development of ERM dashboards that provide a holistic view of risk and thoughtful analysis



Management Oversight & Periodic Review

- Accountability for risks
- Ownership
- Updates
  - Changes in business objectives
  - Changes in systems
  - Changes in processes

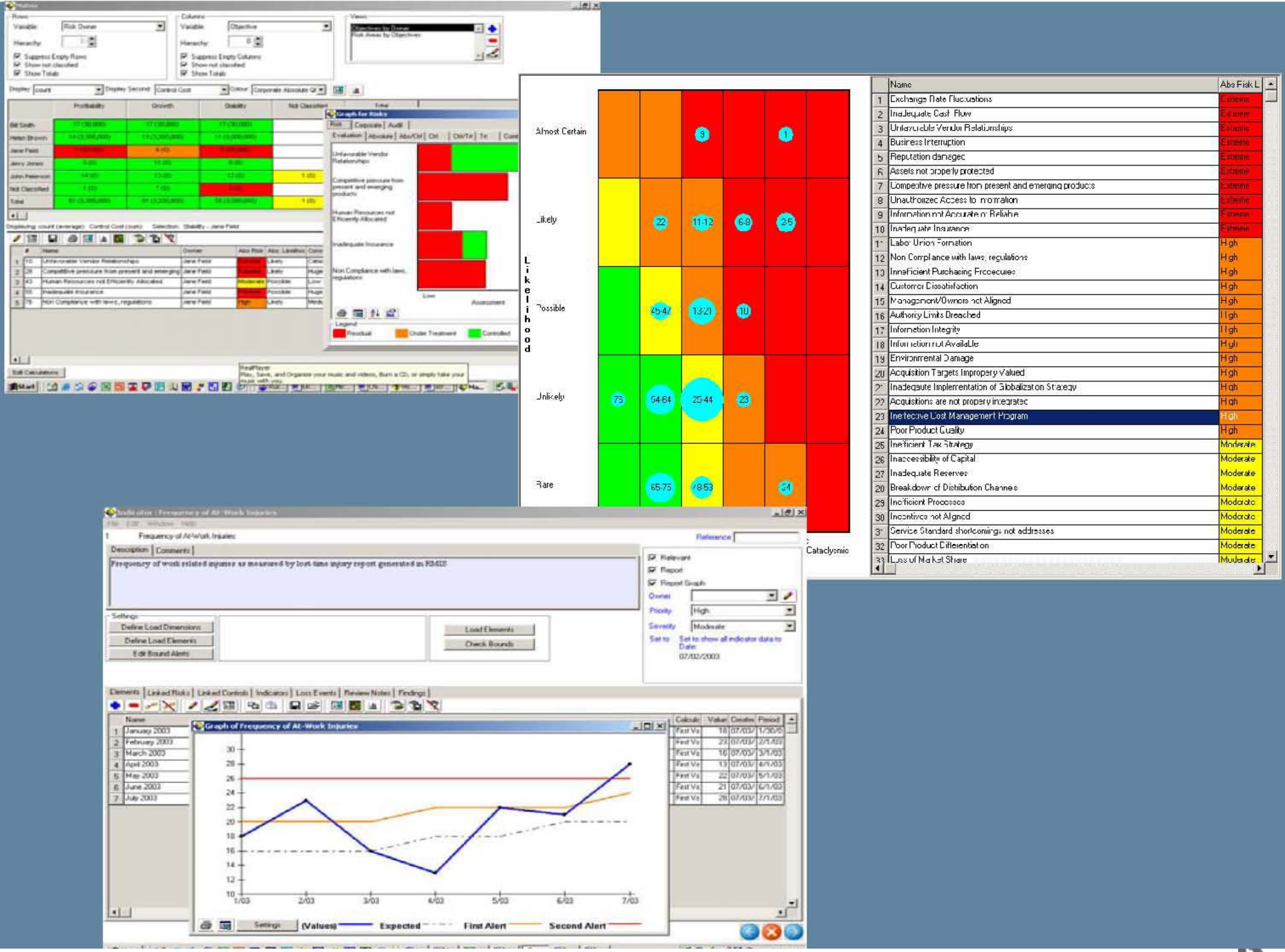
201X Top 20 Risks With Action Plans

2012 Rank	Cat	Risk Description	Owner(s)	Current Mitigation	Action Plans
1	M	**Risk that [partner] has no redundancy in manufacturing and a failure occurs in Mfg. facility**	**VP Supply**	-Both corporate operations and the foreign site have re-organized -Routine visits and complete review of mitigation of our and FDA's comments and recommendations completed -Mock launch done and revisited to help ensure readiness -Full agreement on 100% on-site redundancy and launch and the need for full independent back-up asap post launch -Governance of operations delineated / codified in Quality Agreement -Successful collaborative relationship between operational teams	- back-up site online ASAP post approval -2nd Site approved via NDA filing (6-month review) -Realization of backup site capacity increase ASAP -Continued best-practice sharing leadership through network
2	C	**The risk of a significant marketing, selling or promotional compliance issue driven by us.**	**Gen. Counsel**	-Current compliance program incorporates industry, regulatory and legal best practices -Promotional review committee in place and highly effective -Commercial management already trained on policies and procedures -Comprehensive compliance technology solution in development -Compliance, legal and commercial management highly experienced in identifying and investigating compliance issues	-Implement and roll out comprehensive training program, including eLearning component -Implement robust auditing and monitoring procedures Train sales managers to actively monitor field related activity and identify compliance issues prior to their escalation -Take swift and serious action when compliance violations are identified -Ensure no retaliation for reported violations

Integrating ERM into decision-making

- To be effective and sustainable, risk management must be integrated into day-to-day business line activities and corporate decisions
  - Risk Managers must be involved at the onset of strategy setting processes
  - Risks associated with new programs and services should be considered and communicated to the board/stakeholders
  - Analysis of emerging risks and stress tests should influence business decisions
  - Risk information should be shared across the organization to avoid the same event recurring

Examples of Tools



☑ Suppress Empty Rows
☑ Show not classified
☑ Show Totals

☑ Suppress Empty Columns
☑ Show not classified
☑ Show Totals

	Profitability	Growth	Stability	Not Classified	Total
Bill Smith	17 (30,000)	17 (30,000)	17 (30,000)		
Helen Brown	14 (3,300,000)	13 (3,300,000)	11 (3,000,000)		
Jane Field	[illegible]	9 (0)	[illegible]		
Jerry Jones	9 (0)	11 (0)	9 (0)		
John Peterson	14 (0)	13 (0)	12 (0)	1 (0)	
Not Classified	1 (0)	1 (0)	[illegible]		
Total	[illegible]	[illegible]	[illegible]	1 (0)	

Displaying: count (average) Control Cost (sum) Selection: Stability - Jane Field

	#	Name	Owner	Abs Risk	Abs. Likelihood	Cons
1	10	Unfavorable Vendor Relationships	Jane Field	Extreme	Likely	Catas
2	26	Competitive pressure from present and emerging	Jane Field	Extreme	Likely	Huge
3	43	Human Resources not Efficiently Allocated	Jane Field	Moderate	Possible	Low
4	55	Inadequate Insurance	Jane Field	Extreme	Possible	Huge
5	79	Non Compliance with laws, regulations	Jane Field	High	Likely	Medi

RealPlayer
Play, Save, and Organize your music and videos, Burn a CD, or simply take your music with you.

	Name	Abs Risk L
1	Exchange Rate Fluctuations	Extreme
2	Inadequate Cash Flow	Extreme
3	Unfavorable Vendor Relationships	Extreme
4	Business Interruption	Extreme
5	Reputation damaged	Extreme
6	Assets not properly protected	Extreme
7	Competitive pressure from present and emerging products	Extreme
8	Unauthorized Access to information	Extreme
9	Information not Accurate or Reliable	Extreme
10	Inadequate Insurance	Extreme
11	Labor Union Formation	High
12	Non Compliance with laws, regulations	High
13	Innefficient Purchasing Procedures	High
14	Customer Dissatisfaction	High
15	Management/Owners not Aligned	High
16	Authority Limits Breached	High
17	Information Integrity	High
18	Information not Available	High
19	Environmental Damage	High
20	Acquisition Targets Impropery Valued	High
21	Inadeqaute Implementation of Globalization Strategy	High
22	Acquisitions are not propery integrated	High
23	Ineffective Cost Management Program	High
24	Poor Product Quality	High
25	Inefficient Tax Strategy	Moderate
26	Inaccessibility of Capital	Moderate
27	Inadequate Reserves	Moderate
28	Breakdown of Distribution Channels	Moderate
29	Inefficient Processes	Moderate
30	Incentives not Aligned	Moderate
31	Service Standard shortcomings not addresses	Moderate
32	Poor Product Differentiation	Moderate
33	Loss of Market Share	Moderate

Indicator : Frequency of At-Work Injuries

File Edit Window Help

1 Frequency of At-Work Injuries

Reference

Description | Comments

Frequency of work related injuries as measured by lost-time injury report generated in RMIS

☑ Relevant
☑ Report
☑ Report Graph

Owner:
Priority: High
Severity: Moderate
Set to: Set to show all indicator data to Date
07/02/2003

Settings
Define Load Dimensions
Define Load Elements
Edit Bound Alerts

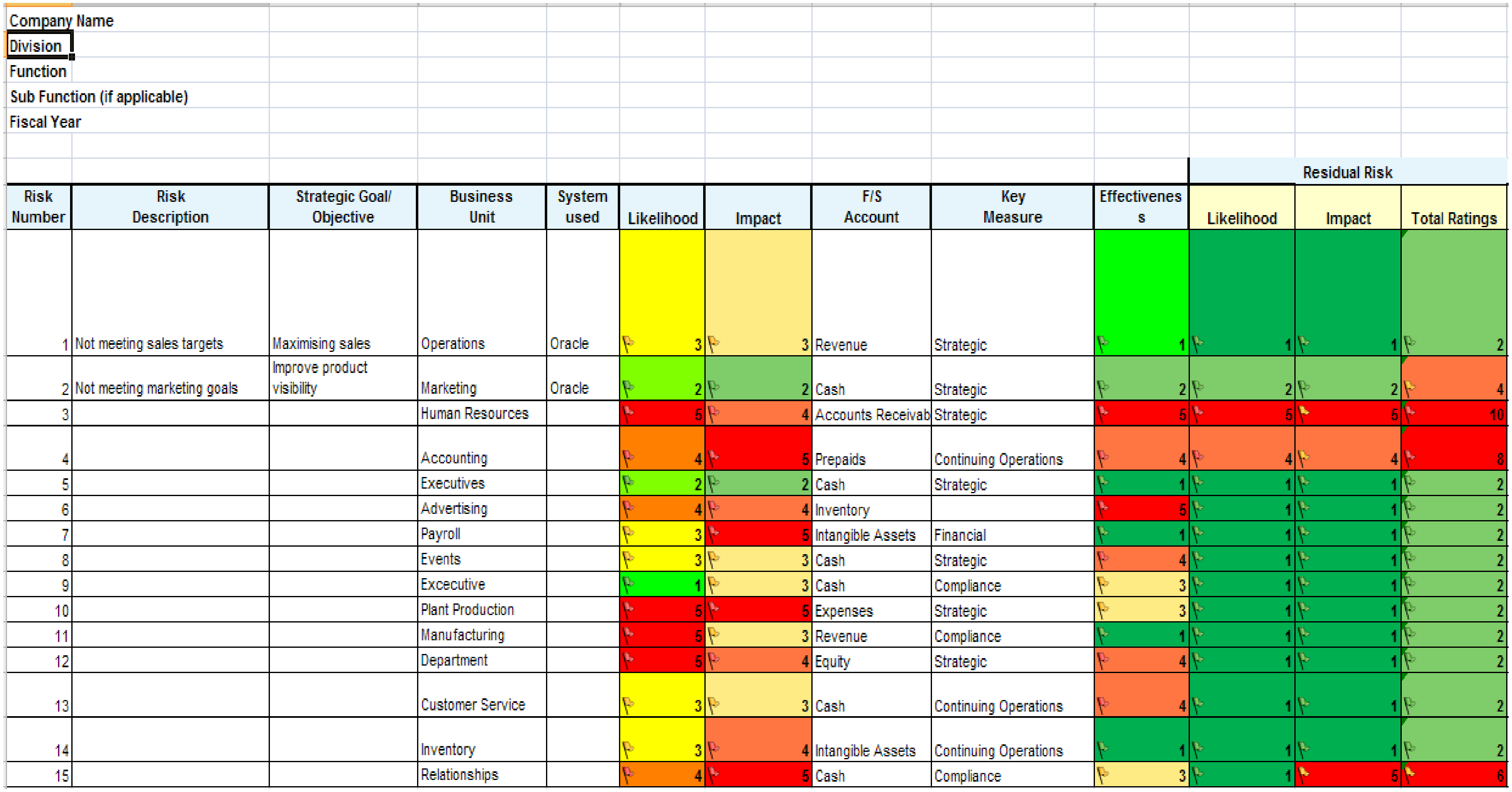
Load Elements
Check Bounds

Elements | Linked Risks | Linked Controls | Indicators | Loss Events | Review Notes | Findings

	Name
1	January 2003
2	February 2003
3	March 2003
4	April 2003
5	May 2003
6	June 2003
7	July 2003

Calculc	Value	Create	Period
Fest Va	18	07/03/	1/30/0
Fest Va	23	07/03/	2/1/03
Fest Va	16	07/03/	3/1/03
Fest Va	13	07/03/	4/1/03
Fest Va	22	07/03/	5/1/03
Fest Va	21	07/03/	6/1/03
Fest Va	28	07/03/	7/1/03

Sample Risk Inventory



Company Name

Division

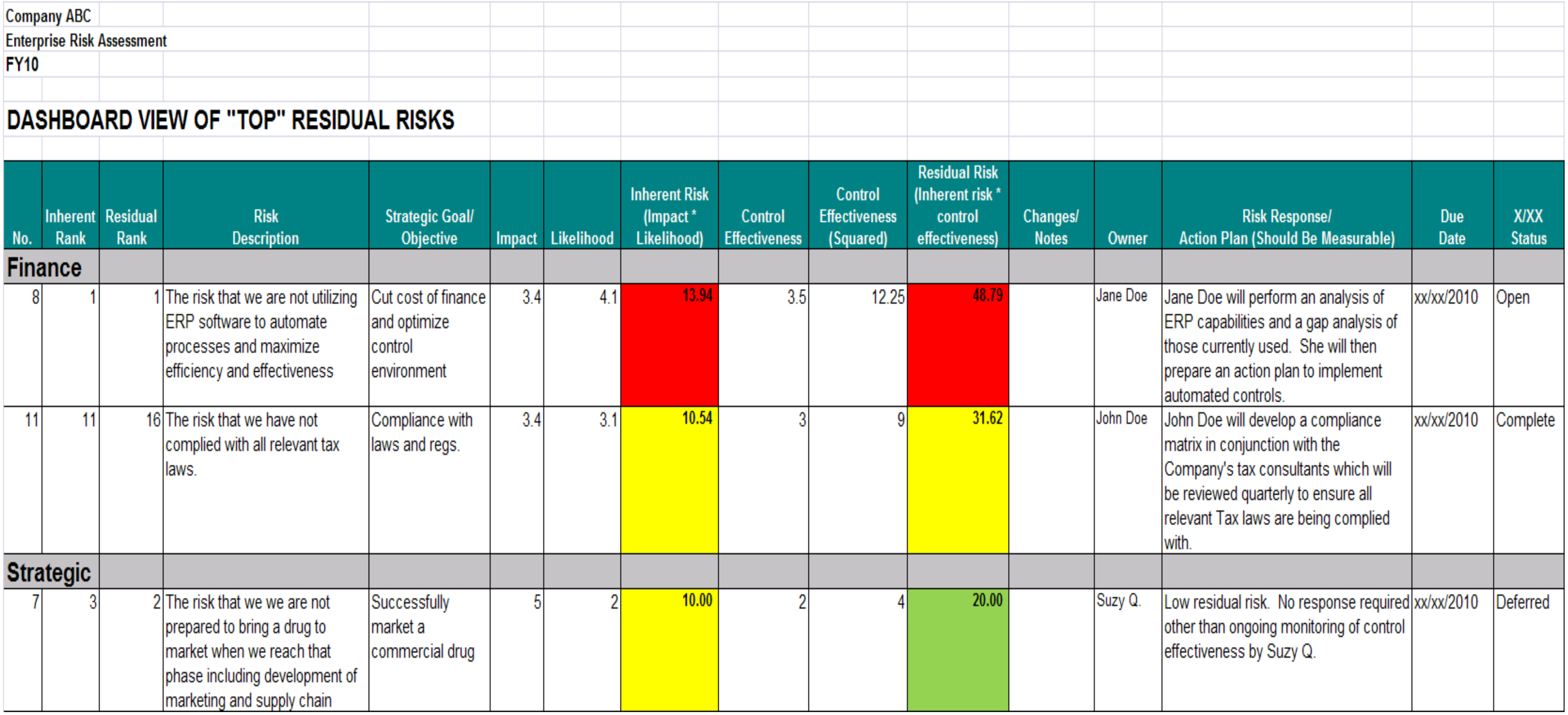
Function

Sub Function (if applicable)

Fiscal Year

										Residual Risk		
Risk Number	Risk Description	Strategic Goal/ Objective	Business Unit	System used	Likelihood	Impact	F/S Account	Key Measure	Effectivenes s	Likelihood	Impact	Total Ratings
1	Not meeting sales targets	Maximising sales	Operations	Oracle	3	3	Revenue	Strategic	1	1	1	2
2	Not meeting marketing goals	Improve product visibility	Marketing	Oracle	2	2	Cash	Strategic	2	2	2	4
3			Human Resources		5	4	Accounts Receivab	Strategic	5	5	5	10
4			Accounting		4	5	Prepaids	Continuing Operations	4	4	4	8
5			Executives		2	2	Cash	Strategic	1	1	1	2
6			Advertising		4	4	Inventory		5	1	1	2
7			Payroll		3	5	Intangible Assets	Financial	1	1	1	2
8			Events		3	3	Cash	Strategic	4	1	1	2
9			Excecutive		1	3	Cash	Compliance	3	1	1	2
10			Plant Production		5	5	Expenses	Strategic	3	1	1	2
11			Manufacturing		5	3	Revenue	Compliance	1	1	1	2
12			Department		5	4	Equity	Strategic	4	1	1	2
13			Customer Service		3	3	Cash	Continuing Operations	4	1	1	2
14			Inventory		3	4	Intangible Assets	Continuing Operations	1	1	1	2
15			Relationships		4	5	Cash	Compliance	3	1	5	6

Sample Dashboard Report



Company ABC
Enterprise Risk Assessment
FY10

DASHBOARD VIEW OF "TOP" RESIDUAL RISKS

No.	Inherent Rank	Residual Rank	Risk Description	Strategic Goal/ Objective	Impact	Likelihood	Inherent Risk (Impact * Likelihood)	Control Effectiveness	Control Effectiveness (Squared)	Residual Risk (Inherent risk * control effectiveness)	Changes/ Notes	Owner	Risk Response/ Action Plan (Should Be Measurable)	Due Date	X/XX Status
Finance															
8	1	1	The risk that we are not utilizing ERP software to automate processes and maximize efficiency and effectiveness	Cut cost of finance and optimize control environment	3.4	4.1	13.94	3.5	12.25	48.79		Jane Doe	Jane Doe will perform an analysis of ERP capabilities and a gap analysis of those currently used. She will then prepare an action plan to implement automated controls.	xx/xx/2010	Open
11	11	16	The risk that we have not complied with all relevant tax laws.	Compliance with laws and regs.	3.4	3.1	10.54	3	9	31.62		John Doe	John Doe will develop a compliance matrix in conjunction with the Company's tax consultants which will be reviewed quarterly to ensure all relevant Tax laws are being complied with.	xx/xx/2010	Complete
Strategic															
7	3	2	The risk that we we are not prepared to bring a drug to market when we reach that phase including development of marketing and supply chain	Successfully market a commercial drug	5	2	10.00	2	4	20.00		Suzy Q.	Low residual risk. No response required other than ongoing monitoring of control effectiveness by Suzy Q.	xx/xx/2010	Deferred

Lessons learned

- Tone at the Top
- Crawl – Walk – Run
- Build on Tools / Processes in Place
- Simplicity at the Outset
- Culture – Culture – Culture

Questions?

Please feel free to contact:

Paul Kiley
RSM
Partner-Boston
Risk Advisory Services
617.241.1287
paul.kiley@rsmus.com

Brendan Day
RSM
Manager-Boston
Risk Advisory Services
617.241.1475
Brendan.day@rsmus.com

QUESTIONS AND ANSWERS?

Paul Kiley, Partner

Summary of Experience
Paul is a partner in RSM's risk advisory practice. He has over 25 years of accounting and internal control experience. He is responsible for leading SOX, internal audit, Service Organization Control (SOC) and Enterprise Risk Management engagements. Paul also serves as the leader of RSM's Northeast Region SOC services. Paul has extensive experience in various industries, including technology, professional services, biotech, manufacturing, consumer products, retail, and property and casualty insurance.

Prior to joining RSM, Paul was a vice president at Caturano and Company. He was also previously an internal audit/SOX director for a publicly traded company and was a senior manager in the business process risk consulting group at Arthur Andersen.

Professional Affiliations
Paul a member of the Massachusetts Society of Certified Public Accountants, American Institute of Certified Public Accountants, Institute of Internal Auditor's (IIA) member, IIA Boston Chapter past-president, Developed and delivered seminars to several chapters of the IIA, and a Board member and Chair of Finance Committee at Cardinal Cushing Center

Education
Bachelor of Business Administration, accounting, University of Massachusetts Amherst

RSM US LLP

80 City Square
Boston, MA 02129
617 912 9000

+1 800 274 3978
www.rsmus.com

This document contains general information, may be based on authorities that are subject to change, and is not a substitute for professional advice or services. This document does not constitute audit, tax, consulting, business, financial, investment, legal or other professional advice, and you should consult a qualified professional advisor before taking any action based on the information herein. RSM US LLP, its affiliates and related entities are not responsible for any loss resulting from or relating to reliance on this document by any person.

RSM US LLP is a limited liability partnership and the U.S. member firm of RSM International, a global network of independent audit, tax and consulting firms. The member firms of RSM International collaborate to provide services to global clients, but are separate and distinct legal entities that cannot obligate each other. Each member firm is responsible only for its own acts and omissions, and not those of any other party. Visit rsmus.com/aboutus for more information regarding RSM US LLP and RSM International.

RSM