Creating Value for Management Through ERM

Steve Zawoyski
Partner
PwC

Governance, Risk & Compliance – G33

ISACA®
Trust in, and value from, information systems
San Francisco Chapter

Agenda

- ERM Defined
- Approach to ERM
- Practical ERM Elements
- Linking risk & Performance
- Leading Practices
- Conclusions

ENTERPRISE RISK MANAGEMENT DEFINED

How you define ERM depends upon where you stand!

It’s a challenge to define “ERM”:

- It’s a hyper maturing concept
- It’s a “trans-industry” capability
- Risk is an not universally defined term
- Limited capacity to quantify risk (vs qualitative assessment)

Issues Driving Focus on ERM

The business and regulatory environments have become increasingly complex, raising corporate risk profiles

Higher Risk Profiles

- Increasing scope and complexity of business activities
- Increasing risks from technology (e.g., speed of execution, data vulnerability)
- Continuous changes in regulatory requirements
- Challenging and uncertain economic environment

Higher Expectations

- Regulators expect corporate risk infrastructure to be commensurate with scale of business activities
- Investors demand more corporate visibility and accountability for risk management
- Rating agencies (e.g., S&P and Moody's) are evaluating risk management program effectiveness

Higher Consequences

Strategic consequences exist if companies are unable to manage risk, compliance and control requirements effectively

- Depressed market value and share price
- Financial losses and/or damaged reputation
- Regulator action/legal noncompliance resulting in damaged reputation/costs
- Regulatory enforcement actions diminish operations and strategic opportunities

Spectrum of ERM Solutions

- Industry
- Risk
- Level of regulation
- Organization
- Sustainability
- Investment

Defining ERM – theory

ERM is a principles-based approach to manage, not eliminate, risk

ERM is a process:

- Built into routine business practices
- Designed to:
  - ***Identify*** emerging events with the potential to affect the entity,
  - ***Assess*** the potential impact consistently, and
  - ***Manage*** risk within a predetermined risk appetite
- Geared to the achievement of objectives
- Applied across the enterprise to the organization's strategic goals

Leading companies use ERM as a critical tool to facilitate performance management

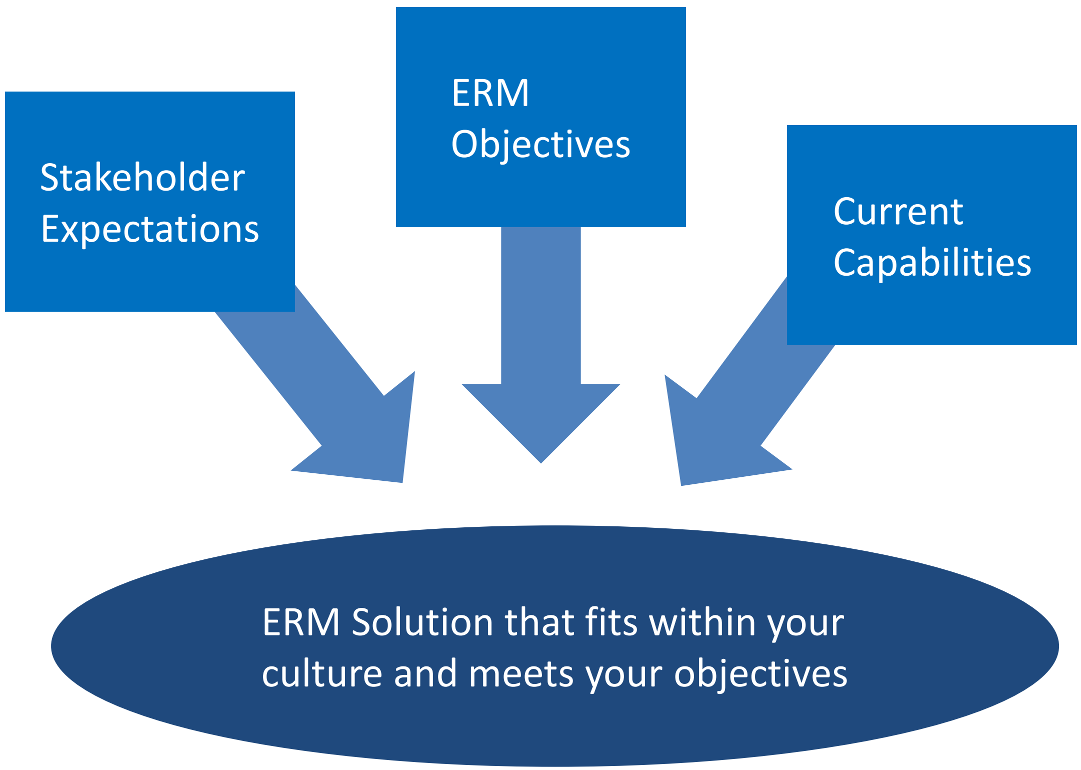
Risk Management Process

Identify	Critical assumptions/variables of the organization
Assess	Relative importance/sensitivity
Evaluate	Options impact at relevant thresholds
Mitigate or Exploit	Execute option based upon actual performance
Monitor	Performance to identify new variables/assumption thresholds

ESTABLISHING AN APPROACH TO ERM

ERM-What are you trying to accomplish?

Develop an understanding of your objectives, stakeholder expectations and current risk management capabilities to develop the right ERM solution.



Key questions to consider when developing your ERM Program. While there is no "right way" to implement ERM, there are right questions to ask!

- **Why**
  - What has prompted you to start discussing ERM now?
- **Objective**
  - What is your organization trying to achieve from an ERM program?
- **Investment**
  - What is the level of effort you're willing to expend in order to meet the expected benefits?
- **Impact**
  - How do you want the effort to be sustained over a long period of time?
- **Current State**
  - What are you doing currently, either formally or informally, around risk management?

Key Stakeholders Expectations

Board of Directors/Audit Committee	Executive Leadership and Management	Risk/Audit/Compliance/Sox
Confidence that risks are being properly managed	Well Informed Strategic Decision Making	Increase risk awareness and streamline risk reporting

ERM Objectives

Governance	Operational	Strategic
Enhance Risk Awareness to Senior Management and the Board	Embed Risk Management Activities in the Business	Link Risk Management to Strategic Planning and the Strategic Objectives of the Organization

Current Capabilities

Initial	Repeatable	Defined	Managed	Optimized
Just beginning ERM discussions, risk informally managed	Perform Risk Assessments annually	Risk Framework defined and embedded in some key processes	Risk Management is owned by the business and embedded in day to day activities	Risk Management is used to identify opportunities and exploit them

Understanding Your Key Stakeholder Expectations

Defining the expectations at different levels within the organization. You need to show relevancy for various stakeholder groups and get buy-in across the organization to be successful. ERM is not just about annual risk assessments, but about making strategically informed decisions. **You can use the business to manage risk or use risk to manage the business.**

Key Stakeholders Expectations

Board of Directors/Audit Committee	Executive Leadership and Management	Risk/Audit/Compliance/Sox
Confidence that risks are being properly managed	*Well Informed Strategic Decision Making*	*Increase risk awareness and streamline risk reporting*
• A formal risk governance and reporting structure aligned with strategy and objectives • A consistent view of risk reported from all levels of the organization • Confidence that significant risks are being appropriately managed and monitored • Understand details of risks facing the company including emerging risks • Established risk appetites and tolerances are being monitored and adhered to	• A formal risk governance and reporting structure aligned with strategy and objectives • A consistent view of risk for prioritization and decision-making • Increased communication of risk dependencies across functional groups • Open lines of communication regarding organizational strategy, goals and expectations • Incorporate risk in the strategic decision making process • Embed risk management practices in business processes	• Provide assurance that significant risks are being considered and appropriately managed at all levels • Increase efficiency and effectiveness of risk management practices • Leverage risk assessment to align audit activities with enterprise risks • Proactively increase risk-consciousness across the organization • Systematic approach to capturing, summarizing and reporting risk information

Understanding your ERM objectives

What does your organization hope to get out of their ERM program? How will you define and measure success?

ERM Objectives

Governance

Enhance Risk Awareness to Senior Management and the Board

- Start understanding current Risk Management practices
- Start to identify and define risk appetite and tolerances
- Repeatable process in place to identify, assess, and manage risks across the organization
- Facilitates the consideration of risk activities from various sources such as SoX, IA, and Compliance
- Enables board communication on Risks
- Documented Risk Management Governance Structure
- Define common risk language and assessment criteria across the organization

Operational

Embed Risk Management Activities in the Business

- Risks are managed formally at all levels in the organization
- Risk management is part of routine activities and some decision making
- Risk appetite and tolerances are formally defined and monitored through Key Risk Indicators and/or Key Performance Indicators
- Reduce financial and operational surprises

Process Focus

Focus Shift

Cultural Focus

- Risk Interdependencies are considered
- Formal escalation procedures when risk tolerances are exceeded
- Adopted common risk language throughout the business
- Enable ongoing reporting to Sr. Management and board through established dashboards

Strategic

Link Risk Management to Strategic Planning and the Strategic Objectives of the Organization

- ERM concepts and practices are integrated into the planning processes
- Risks are considered routinely throughout the organization in both process and decision making
- Align strategies with risk tolerances
- Risks are viewed at a portfolio level, not siloed
- Management has in place processes and programs to anticipate and monitor future and emerging risks
- Scenario based/Sensitivity analysis on known top risks
- Performance measurement – BU, Investments & project performance are evaluated on a risk-adjusted basis

Investment

Understanding Your High-Level Current Capabilities

We believe that Company's are managing their risk either formally or informally. Successful ERM programs understand these capabilities and leverage them.

Current Capabilities

Initial	Repeatable	Defined	Managed	Optimized
Just beginning ERM discussions, risk informally managed	*Perform Risk Assessments annually*	*Risk Framework defined and embedded in some key processes*	*Risk Management is owned by the business and embedded in day to day activities*	*Risk Management is used to identify opportunities and exploit them*

Questions to ask at a high-level to understand current risk management capabilities

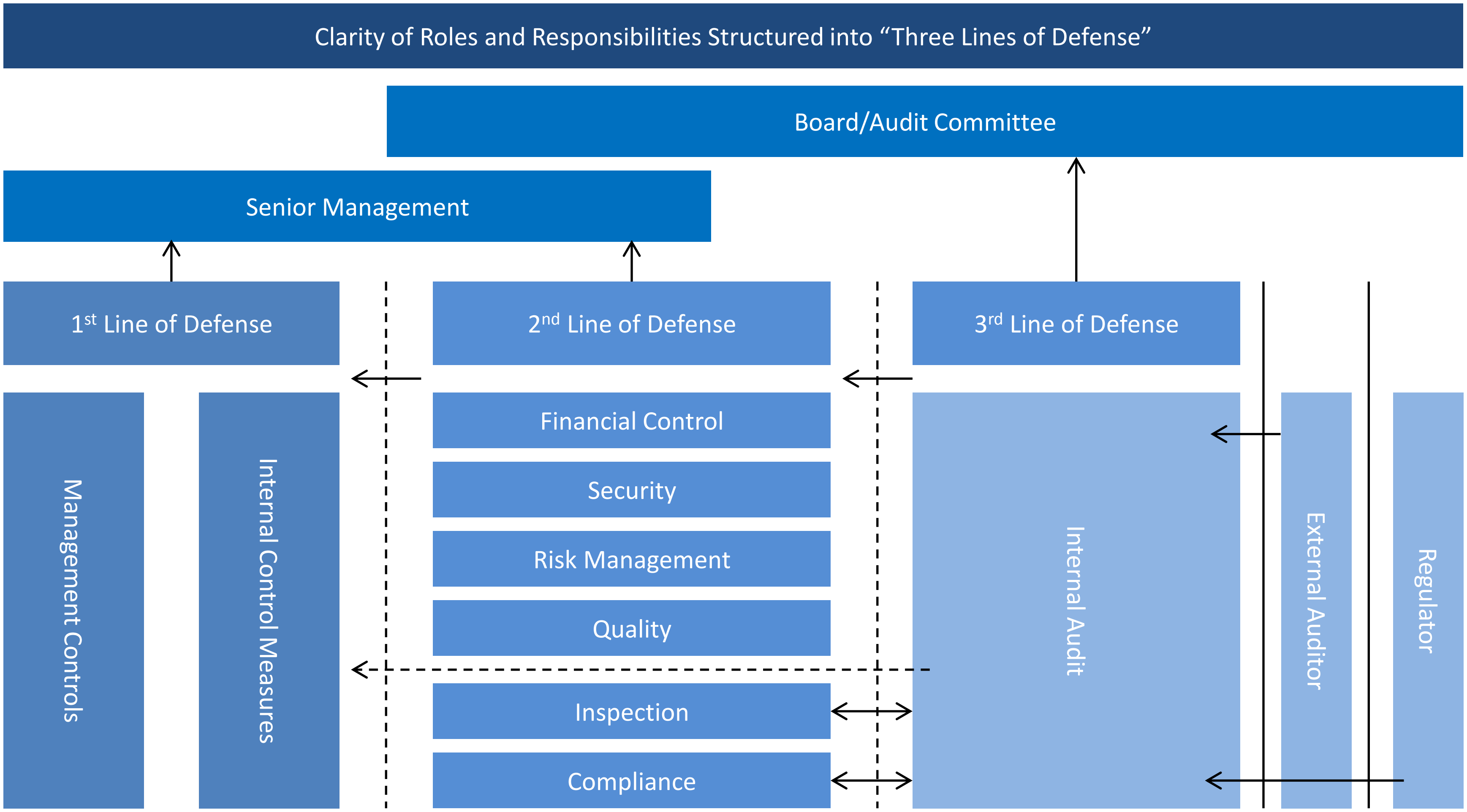
Risk Governance, Roles and Responsibilities	• How has risk management governance and oversight been defined? • Who is involved? What are their roles and responsibilities?
Methods Used to Identify, Assess & Manage Risk	• How are risks identified, categorized, assessed and prioritized? • Is this done enterprise-wise or individual functions, BUs, etc?
Risk Assessment Criteria & Thresholds	• How are risks being assessed? • Have risk appetite and risk thresholds been defined across the company?
Monitoring and Reporting Risks	• How are risks captured, stored, analyzed and reported? • How is risk information monitored and issues escalated?
Integration of Risk Management with other Processes	• How is risk information used in defining the business strategy and objectives? • How is risk information used to support business decision making?
Risk Culture	• What is the company's culture around risk management?

Success Factors

- Establish a clear and realistic objective for ERM in the organization
- Recognize and adapt to the different expectations of the various stakeholder/customer groups
- Leverage already established RM capabilities
- Maintain a high return/effort ratio

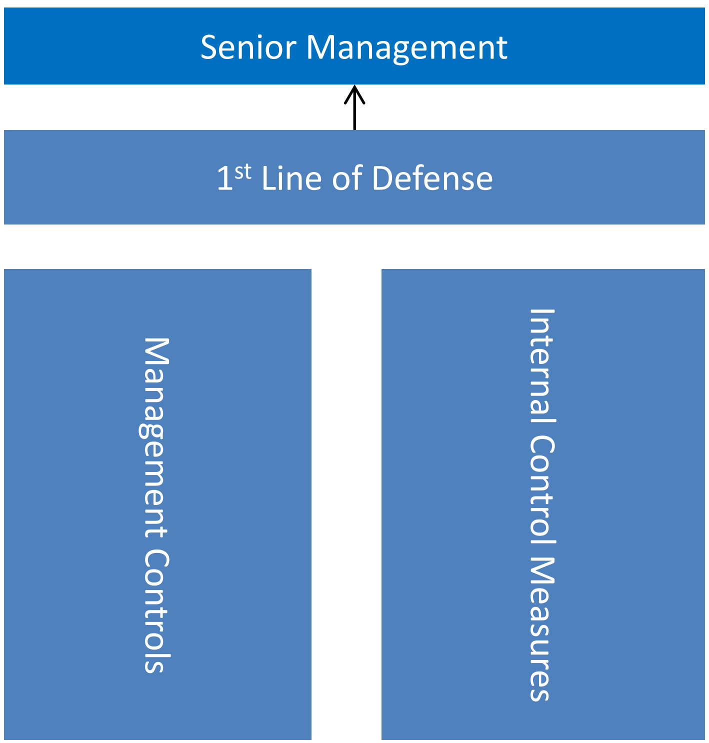
PRACTICAL ELEMENTS

Roles and responsibilities for Risk Management



1st line of defense

Operational management has ownership, responsibility and accountability for assessing, controlling and mitigating risks.



Roles & Responsibilities

- Convert strategy into operational objectives
- Maintain a system of effective internal controls
- Execute risk and control procedures on a day-to-day basis
- Assign procedural and operational responsibilities
- Implement corrective actions to address process and control deficiencies

2nd line of defense

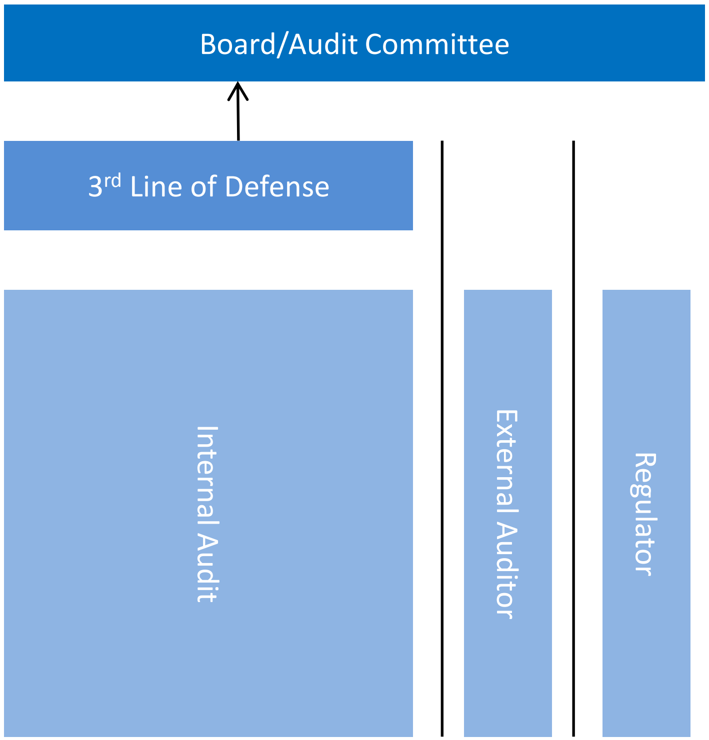
Risk Management and Compliance facilitates and monitors practices by operational management and assists in reporting information up and down the organization.

Roles & Responsibilities

- Provide positive Tone at the Top
- Establish compliance and risk management policies, roles and responsibilities and implementation goals
- Establish the integrated control and risk framework (common language)
- Promote compliance and risk management competence
- Facilitate the development of the risk and control monitoring and reporting process
- Report to senior management and board on progress and recommended actions

3rd line of defense

Internal Audit provides assurance to the board and senior management on the effectiveness of compliance and risk management.

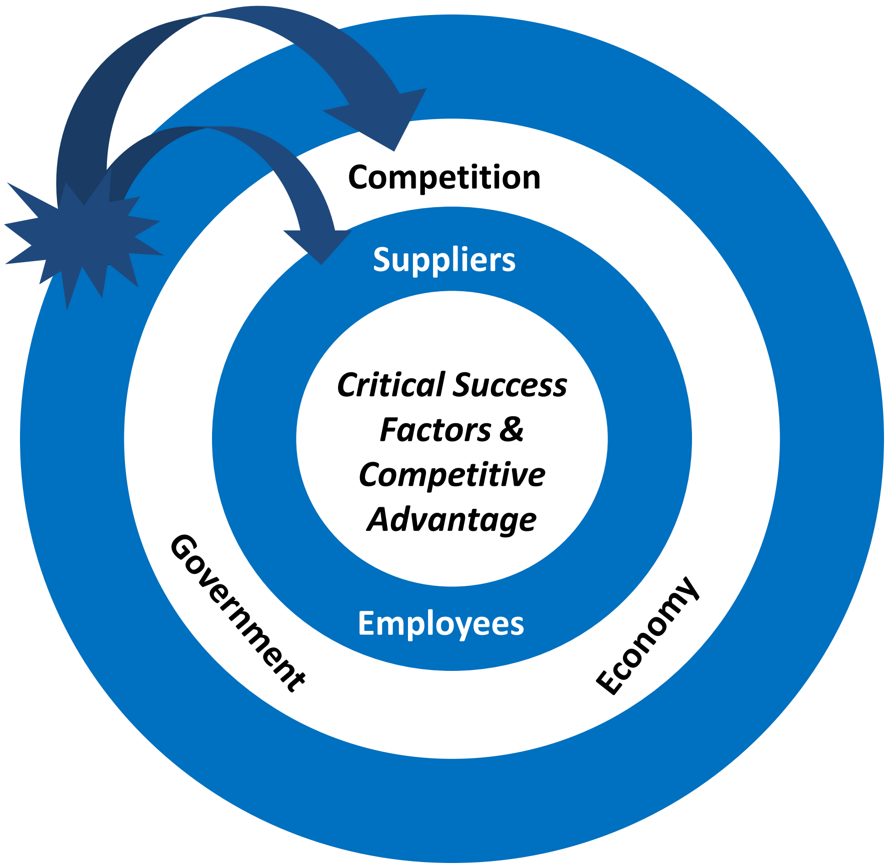


Roles & Responsibilities

- Provide objective assurance to the board and senior management
- Serve as an in-house consultant to the second and first line of defense
- Provide a connection with the external audit and regulatory bodies
- Coordinate of the internal audit plan with the inspection activities performed by the first and second line of defense

Complexity

Business operates in complex and adaptive environments. Its difficult to identify and predict the random events and their impact to the organization. In hindsight, this may seems possible, however, its difficult and time consuming to attempt to predict random and unrelated events.



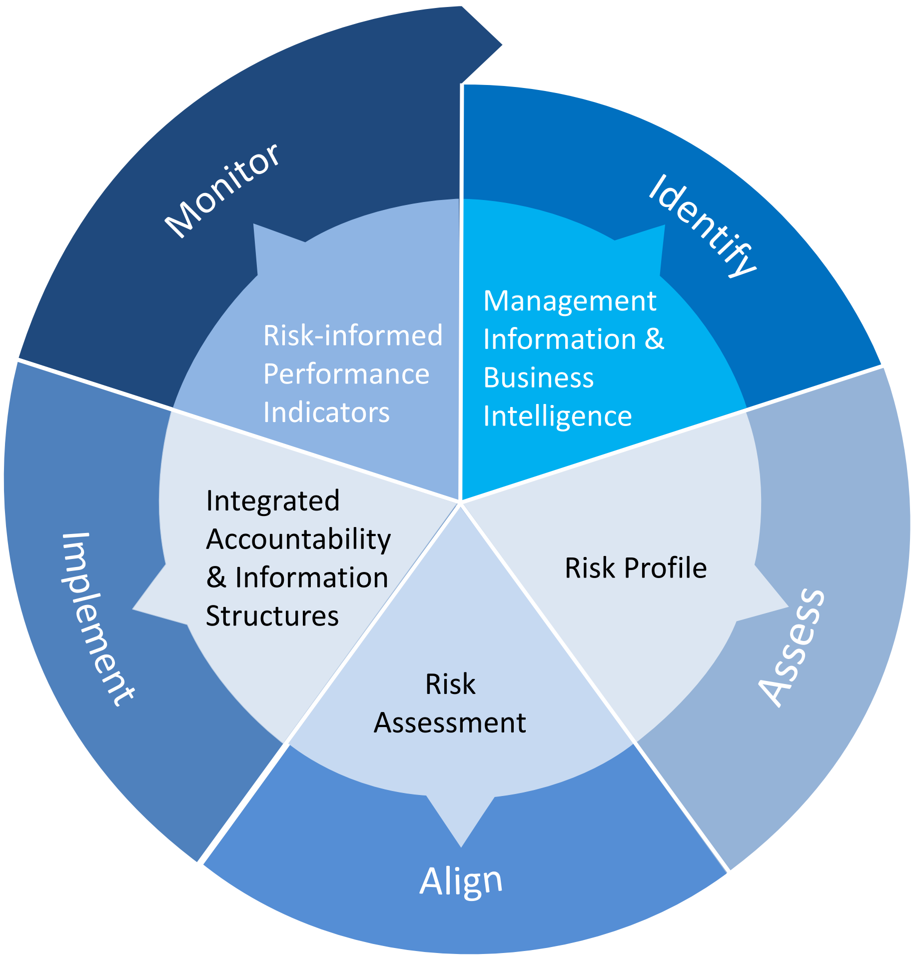
By establishing a narrow set of "variables" or assumptions which are core to the organization's success they can prioritize and effectively monitor the potential impact of changes in the business environment

Risk: Culture. Inherent/Residual, Tolerance, Appetite and Capacity

- **Risk Culture** is the general attitude of the organization with regard to risk taking.
- **Inherent risk** is the risk associated with an activity absent of risk management activities
- Residual risk is the risk associated with an activity after consideration of risk management activities.
- **Risk tolerance** looks at acceptable/unacceptable deviations from what is expected at the individual and aggregate risk level.
- **Risk appetite** is a proactive expression of the level of risk that a business wishes to bear — its “desirability” for risk.
- **Risk capacity** is an assessment of the maximum risk an organization could bear without serious impairment to its business capability. It provides an upper boundary to risk appetite.

LINKING RISK AND PERFORMANCE – A PROPOSED PROCESS

Linking risk and performance: A continuous process



Keys to successful implementation of this process include:

- Leveraging existing information, processes and people from throughout the enterprise
- Viewing risks, measurements and performance capabilities across organizational silos
- Maintaining focus on and linkage to key business objectives *(relevance)*
- Drive toward organizational capability and talents (as opposed to functional capability)

Linking risk and performance: Identify

- Establish a complete understanding of the strategic environment and goals:
  - What are the key business objectives?
  - What is the planning and achievement horizon for those objectives?
  - How are those objectives measured?
  - What systems, processes and people underlie those activities?
  - Is clear accountability established for the achievement of those objectives?
  - Have risks been appropriately identified or considered in the planning cycle?

PRACTICAL CONSIDERATIONS

- Objectives-centric view, but crossing internal silos
- Measurements are key (KPIs)
- Maintain relevance at strategy level
- Understand the core operational/strategy environment

Linking risk and performance: Assess

- Assess the risk profile of the organization:
  - Identify key risks to business objectives, considering the risk management categories: strategic, operational, financial, compliance.
  - Consider both internal and external sources for the identification of risks:
    - Facilitated risk assessment, survey tools, interviews, external publications and studies
  - Leverage subject matter expertise inside and outside the organization
  - Objective in the risk profile is to consider the activities of the organization (value creating activities) and identify the relevant risks.

PRACTICAL CONSIDERATIONS

- Stay focused: too many risks will impair the ability to respond/manage
- Maintain link to the identify stage – it's all about business objectives
- Consider risks that cross organizational silos ("big picture")

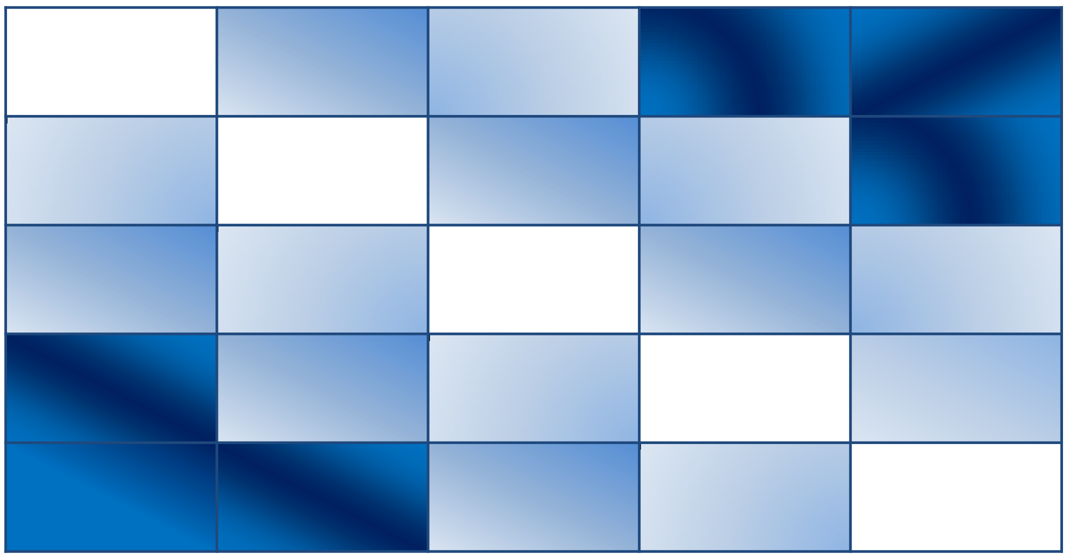
Linking risk and performance: Align

- Most organizations will have many more risks identified than capability to respond
- The key question becomes what risks warrant response given limited resources
- Prioritization of the risk assessment drives the allocation of resources and ensures relevance
  - Linkage is about maintaining the objective view of the risk environment but reconciling that to the overall business objectives
  - Some risks will impact multiple objectives, most objectives stand to be impacted by multiple risks
  - Assessment must be relevant to strategic objectives, or relevance is lost

PRACTICAL CONSIDERATIONS

- Assess stage leaves open the question of risk response
- Assessment alone does not add value – must align with objectives and prioritize
- Maintain relevance at strategy level

Linking risk and performance: Align *(continued)*



Note: Likelihood and impact is one evaluation model – certain risks may warrant more complex or quantitative risk measurement models

PRACTICAL CONSIDERATIONS

- Assess stage leaves open the question of risk response
- Assessment alone does not add value – must align with objectives and prioritize
- Maintain relevance at strategy level

Linking risk and performance: Implement

- Align resources and accountability structure:
  - 51% of senior executives surveyed by PwC said that one person (usually the CFO) is responsible for risk management and performance management
  - 49% reported that oversight resides with a combination of executives
  - A collaborative accountability structure – with the right incentives and oversight – is optimal for managing risk and performance concurrently
- Ask the right questions:
  - What is my company's ability to withstand shock? What could my balance sheet endure?

PRACTICAL CONSIDERATIONS

- For example, finance might manage financial risks, while legal might manage and oversee compliance risks
- While accountability might be a collaborative model, measures should be consistently defined

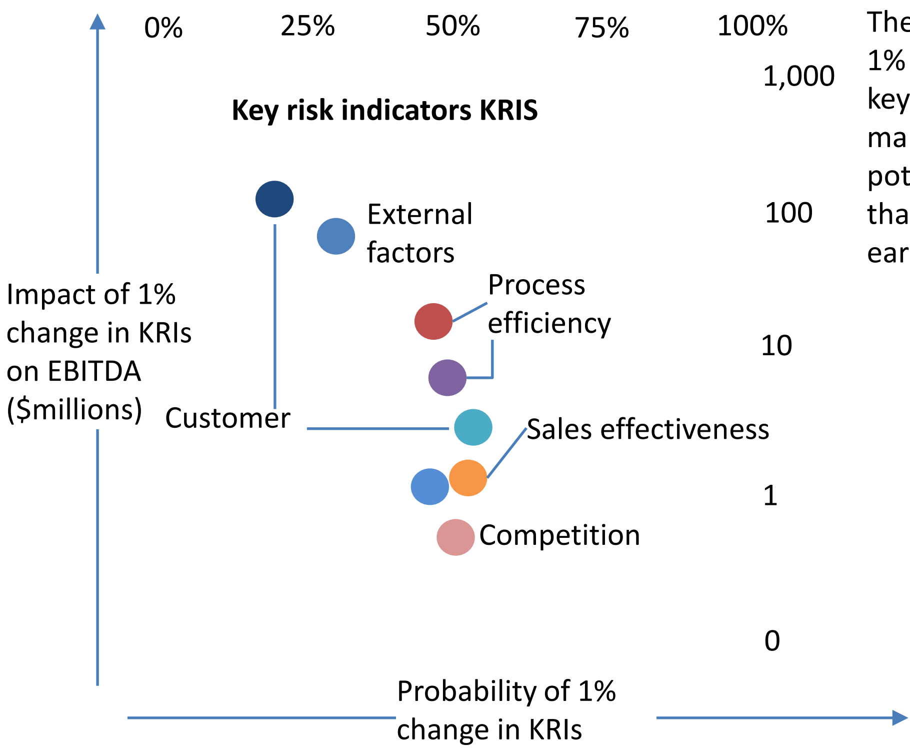
Linking risk and performance: Monitor

- Consistent, actionable measurement that informs decision is the ultimate outcome of this process
  - Defined thresholds – what trigger or results drives response?
    - Scenario planning provides opportunity for organizations to consider impact of risks before triggers are set
    - Financial models can consider the performance implications of incremental changes in the risk measures
  - Many companies already have the necessary risk and performance data but it’s buried in silos across functional units that never sync up

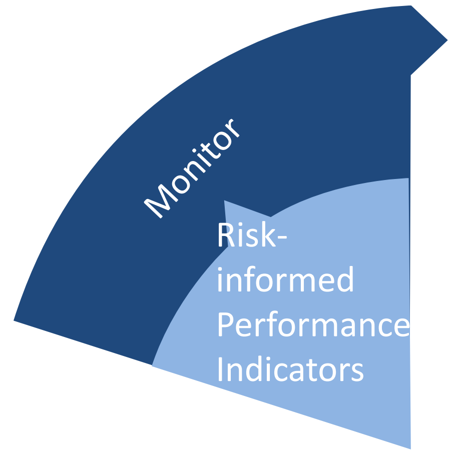
PRACTICAL CONSIDERATIONS

- 80% of executives surveyed by PwC said quality and timeliness of information presented one of the top challenges for improving risk management over the next two to three years

Linking risk and performance: Monitor *(continued)*



The probability of a 1% change in eight key risk indicators is mapped against the potential impact of that change on earnings (EBITDA).



PRACTICAL CONSIDERATIONS

- 80% of executives surveyed by PwC said quality and timeliness of information presented one of the top challenges for improving risk management over the next two to three years

LEADING PRACTICES

Comprehensive ERM Framework

01 Risk Strategy
01 Obligations
03 Risk Appetite
04 Risk Profile
05 Stakeholder Management

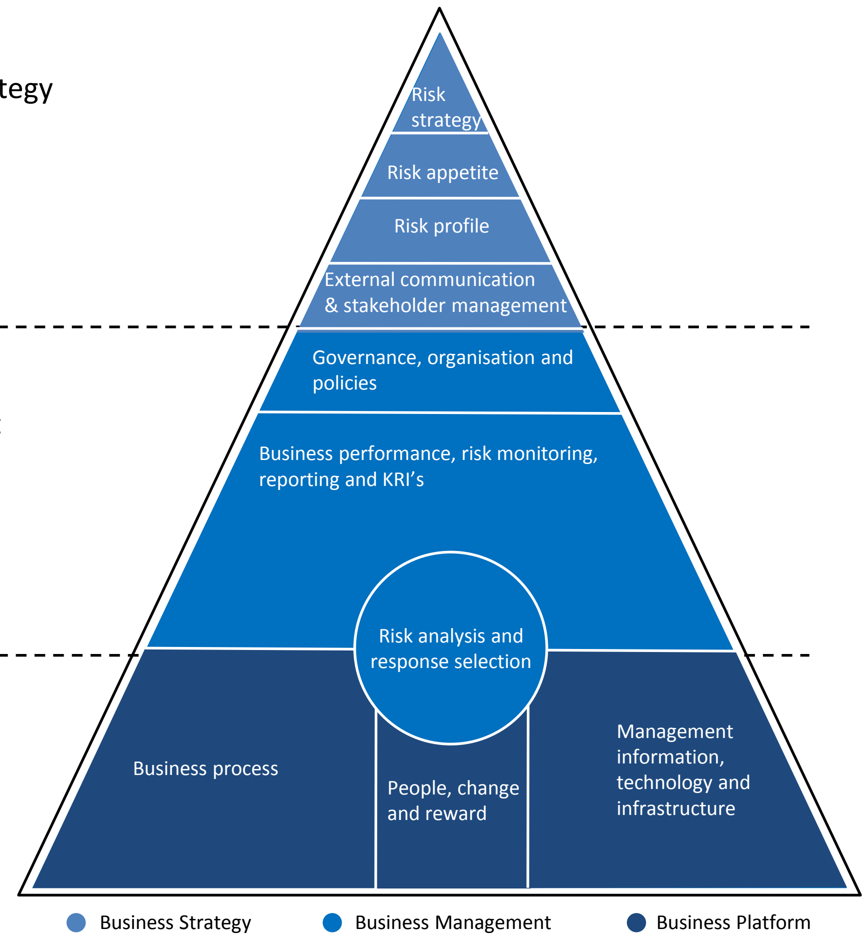
Business Strategy

06 Governance, Risk & Compliance Structure
07 Governance, Risk & Compliance Policies
08 Monitoring & Reporting
09 Key Risk Indicators
10 Risk Modelling
11 Risk Analysis Techniques

Business Management

12 Business Process Integration
13 Risk Culture
14 Performance Incentives
15 Governance, Risk & Compliance Training
16 Governance, Risk & Compliance Technology

Business Platform



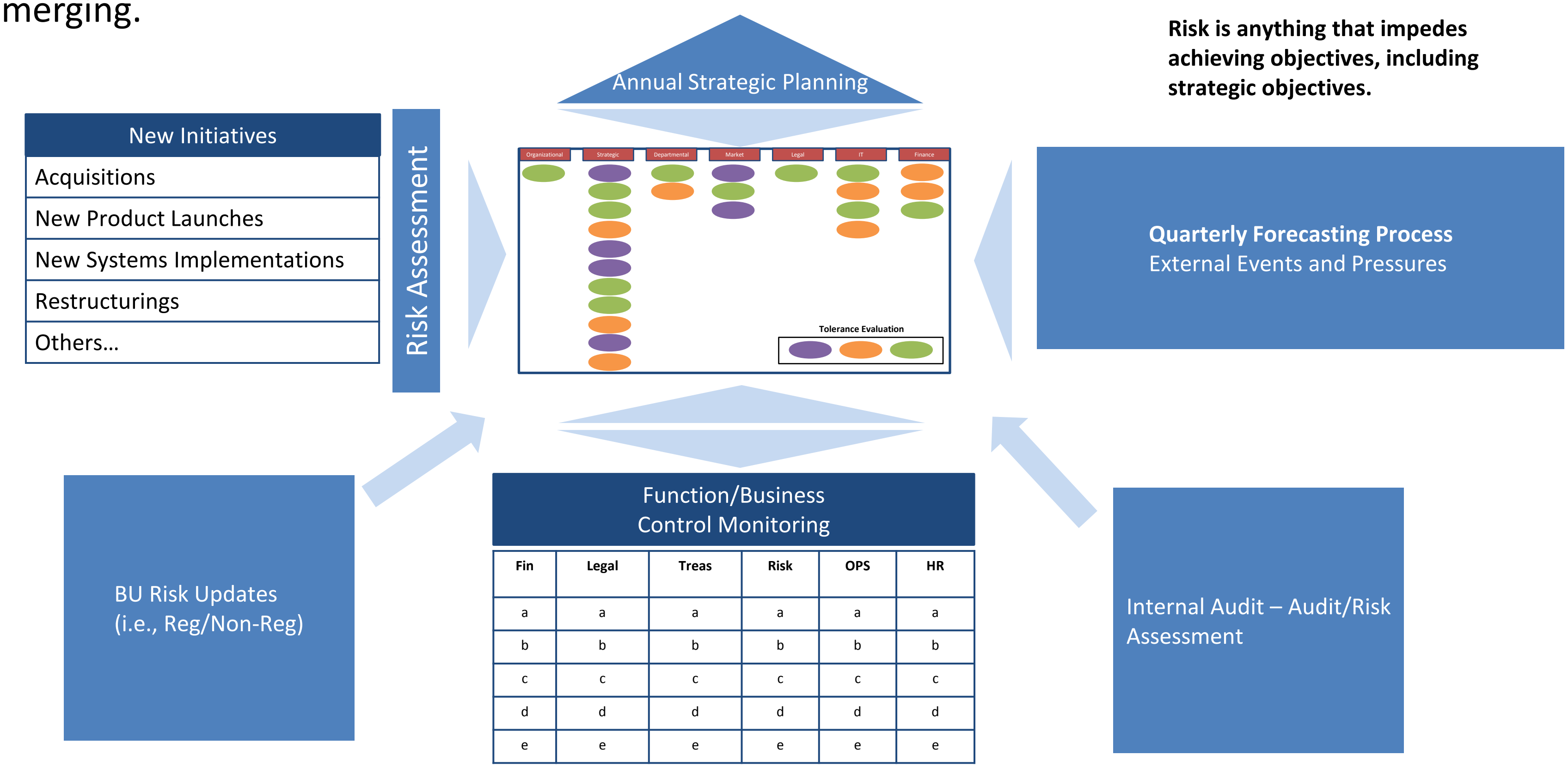
Value Linkage

			Strategy										
			Growth			Productivity			Client/Regulator				
			Market Growth	Diversified Business Model	Brand Experience	Operational Excellence	Advisor Productivity	Strong Balance Sheet Fundamentals	Products	Services	Brand/image	Clear Client Focus	Corporate Responsibilities
Risk #	Category	Risk level & direction											
Strategic & business risk													
S1	Strategic alignment	Low High ↑	H	H	H	H	H	H	H	H	H	H	H
S2	Innovation	Low High ↑	H	H	H		M		H	M	M	M	
S3	Acquisitions/ joint ventures/ diversities	Low High ↑	H	L	M	H					M		
S4	Competition	Low High ↑	H	H	H		H	L	H	H	L	H	
S5	Emerging markets	Low High ↔	H		L				M		H	M	H
S6	Reputation	Low High ↑	H			L	M	M			H	H	H

Leading Practices in ERM

Embedding ERM into the core business and planning processes allows management to effectively update the organization's risk profile and understand what risk scenarios or events may be emerging.

Risk is anything that impedes achieving objectives, including strategic objectives.



Fin	Legal	Treas	Risk	OPS	HR
a	a	a	a	a	a
b	b	b	b	b	b
c	c	c	c	c	c
d	d	d	d	d	d
e	e	e	e	e	e

Leading Practices in ERM

Practice	Points to Consider
1. Risk management is sponsored and driven by the Board, including establishing risk appetite and the policy framework for risk tolerance.	• Successful risk management programs always have engagement from the board. • The Board sets risk tolerance (what variances from policies will be accepted) and risk appetite (how much risk will the organization accept)
2. The C-Suite (including CEO, COO & CFO) is accountable and actively engaged.	• C-Suite engagement is a critical element to ensure ownership for risk response strategies is at sufficiently senior levels. • Senior leadership ensures risks are explicitly considered in key decisions and strategic planning & resources are assigned as needed to risks identified.
3. A robust, relevant and meaningful risk assessment is conducted that crosses the enterprise and considers relevant categories of risk: (e.g., strategic, operational, financial and compliance).	• Risk assessment is established as a starting point for a risk management program, not a destination or outcome. • The assessment crosses organizational silos and considers the range of risks facing the organization (inclusive of, but beyond traditional financial and compliance risks).
4. Risks are identified and linked to strategic priorities and business objectives.	• Risk assessment and management response strategies based only on "theoretical" risks are destined for failure. • Risks are defined as events that can impact the achievement of business objectives – ensuring ownership and risk response strategies that are relevant and aligned to performance planning.

Leading Practices in ERM

Practice	Points to Consider
5. A governance structure that supports oversight and execution of appropriate risk response activities is established and in place.	• Oversight is an important component of an effective risk management capability, but is only one element of establishing a sustainable capability. • Successful risk management programs have an operating execution layer that ensures risk response strategies are effectively implemented and monitored.
6. Risk ownership is established and management accountability clearly identified.	• Absence of explicit risk ownership often results in persistent gaps in risk identified and risk response execution, particularly where specific risks cross organizational silos. • Risk ownership ensures that as strategies evolve and organizational dynamics change that risks will continue to be appropriately addressed.
7. A consistent risk vocabulary and risk measurement model is adopted and in place.	• To be effective, enterprise risk programs must apply a consistent risk vocabulary and measurement model. • Consistency ensures that limited resources are allocated to the risk activities that truly warrant response or mitigation.
8. Scenario planning capability is developed and applied to help determine risk impacts and to evaluate impact of broader, strategic risks (emerging risks). 9. Risk management is developed as an organizational capability and integrated in management development planning, not viewed as an ancillary function.	• Scenario planning should be applied to help address the complexities and inter-dependencies among multiple risk events. • Scenario planning often includes financial modeling capabilities to help organizations get more explicit about their risk tolerance and the impact of certain events on busines models and strategy. • Risk management as an add-on function or a department tends to become a compliance or reporting function – sometimes failing under the weight of bureaucratic processes and documentation. • Long term integration of risk management capability require development of risk management capability within talent – elevating risk from a department function to a priority in talent development.

Typical challenges to overcome with ERM

- The Board's role in ERM has become increasingly challenging as expectations for their engagement are at all time highs
- Leadership doesn't buy in to a formal ERM process because "enterprise risk is handled by management as part of their day-to-day responsibilities"
- When implemented, ERM tends to be bureaucratic and an annual event that is not well integrated with existing strategic planning and other business processes
- Enterprise risk assessments are often superficial and don't highlight the real risks and their interconnections
- Risks are identified and managed inconsistently within silos – organizational interdependencies are not fully understood

To overcome these challenges:

- ***Align ERM with existing business activities***
- ***Provide periodic reporting that is tailored and brings value to the audience***