Identify

Assess

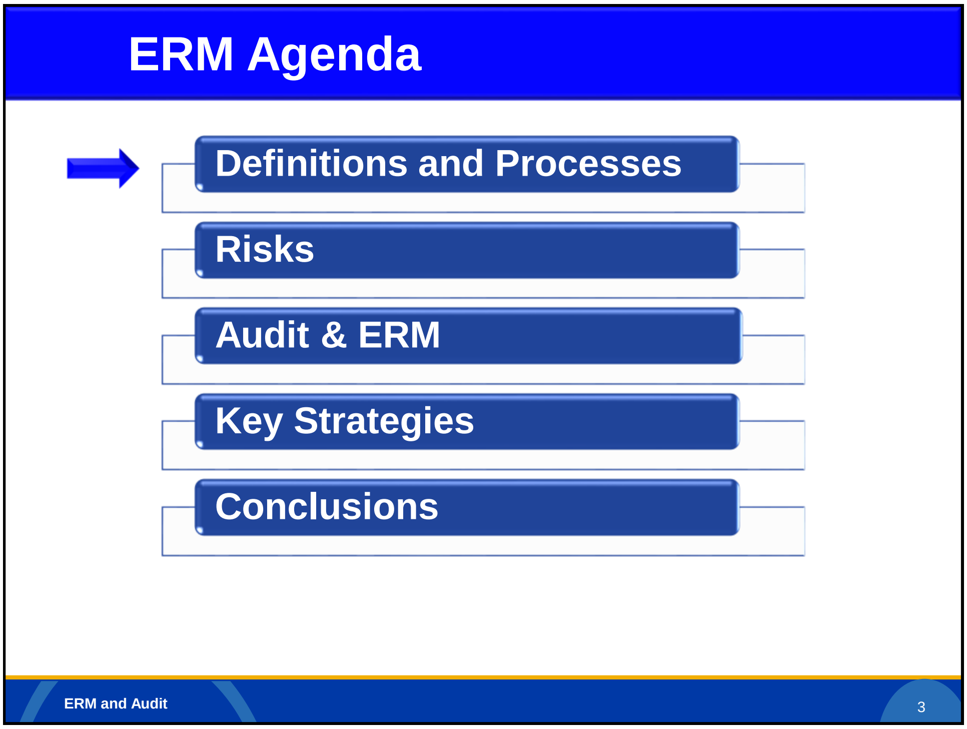
Mitigate

Control

Act

ERM and Audit

2

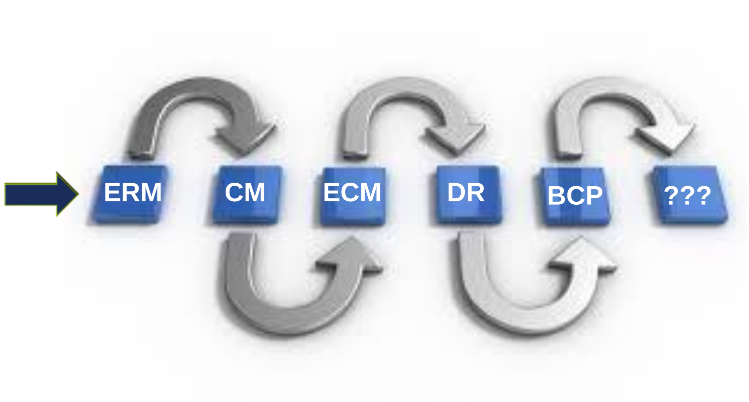


ERM Agenda

- Definitions and Processes
- Risks
- Audit & ERM
- Key Strategies
- Conclusions

ERM and Audit

3



ERM → CM → ECM → DR → BCP → ???

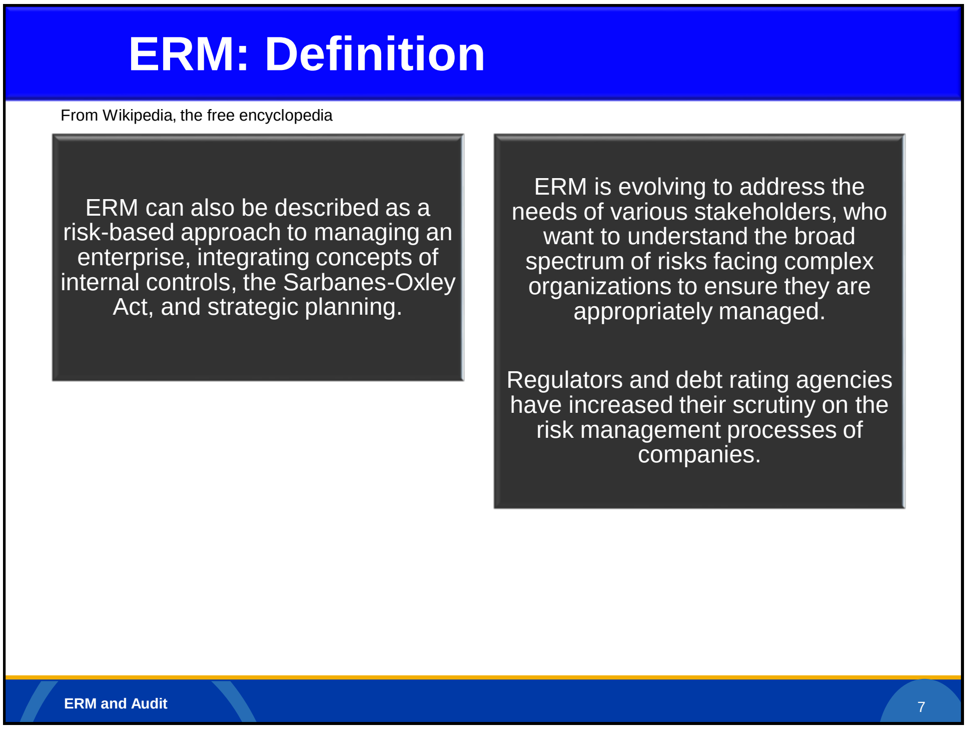
ERM: Definition

From Wikipedia, the free encyclopedia

ERM in business includes the methods and processes used by organizations to manage risks and seize opportunities related to the achievement of their objectives

ERM provides a framework for risk management, which typically involves:

- identifying particular events or circumstances relevant to the organization's objectives (risks and opportunities)
- assessing them in terms of likelihood and magnitude of impact
- determining a response strategy
- monitoring progress



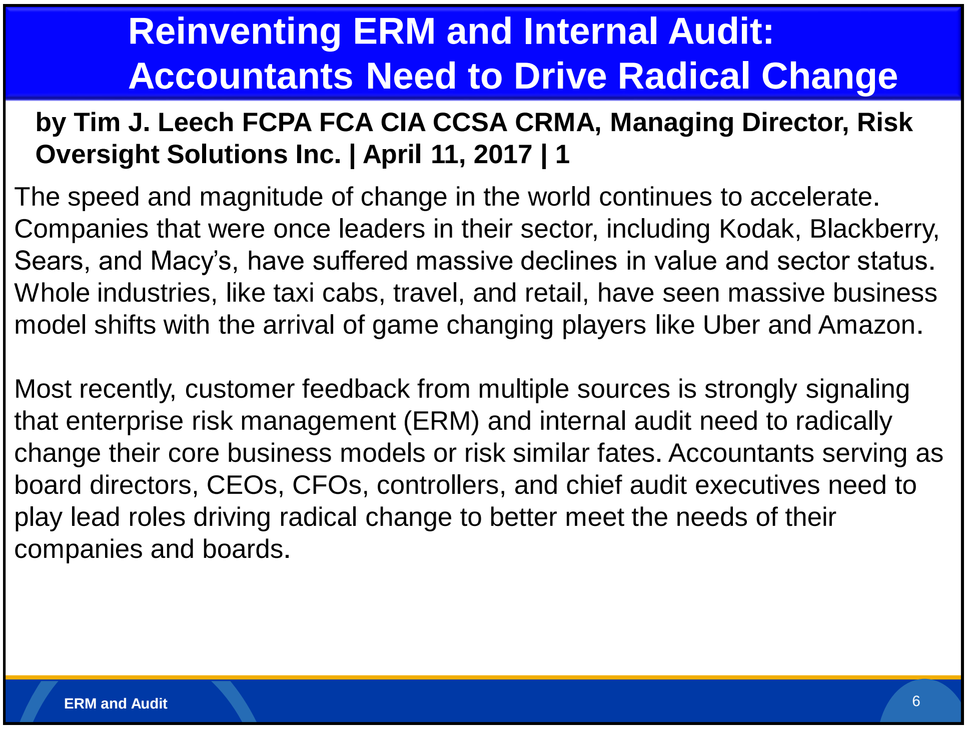
ERM: Definition

From Wikipedia, the free encyclopedia

ERM can also be described as a risk-based approach to managing an enterprise, integrating concepts of internal controls, the Sarbanes-Oxley Act, and strategic planning.

ERM is evolving to address the needs of various stakeholders, who want to understand the broad spectrum of risks facing complex organizations to ensure they are appropriately managed.

Regulators and debt rating agencies have increased their scrutiny on the risk management processes of companies.



Reinventing ERM and Internal Audit: Accountants Need to Drive Radical Change

by Tim J. Leech FCPA FCA CIA CCSA CRMA, Managing Director, Risk Oversight Solutions Inc. | April 11, 2017 | 1

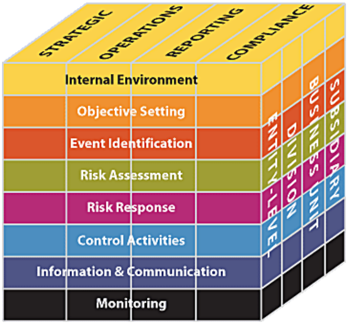
The speed and magnitude of change in the world continues to accelerate. Companies that were once leaders in their sector, including Kodak, Blackberry, Sears, and Macy’s, have suffered massive declines in value and sector status. Whole industries, like taxi cabs, travel, and retail, have seen massive business model shifts with the arrival of game changing players like Uber and Amazon.

Most recently, customer feedback from multiple sources is strongly signaling that enterprise risk management (ERM) and internal audit need to radically change their core business models or risk similar fates. Accountants serving as board directors, CEOs, CFOs, controllers, and chief audit executives need to play lead roles driving radical change to better meet the needs of their companies and boards.

The ERM Framework

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

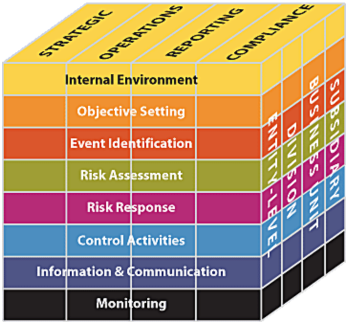
- Strategic
- Operations
- Reporting
- Compliance

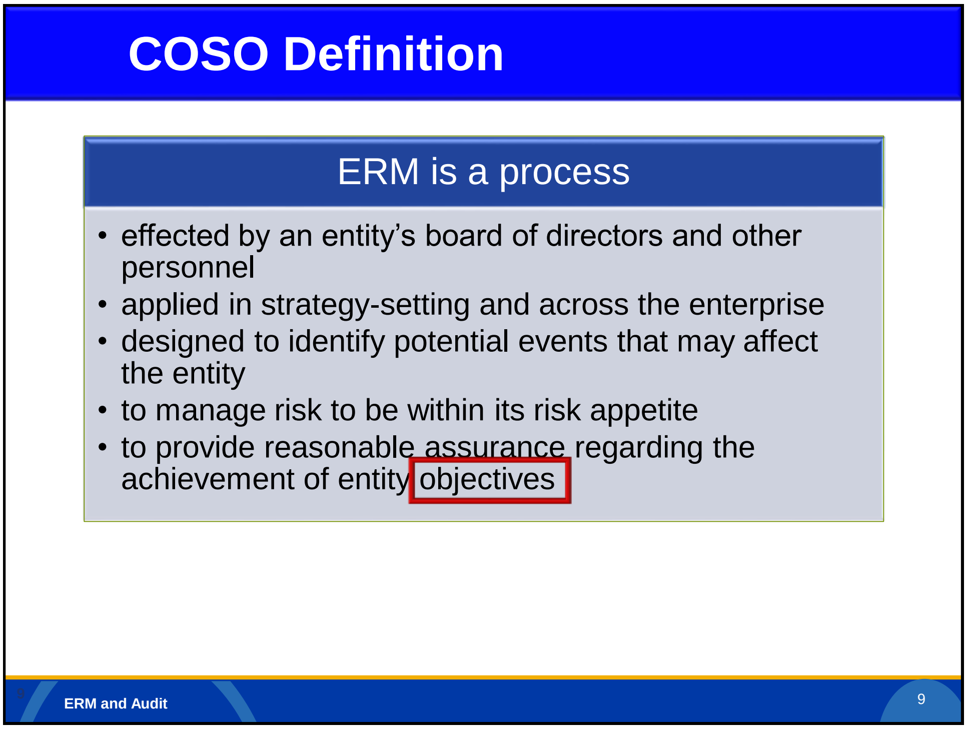


The ERM Framework

ERM considers activities at all levels of the organization:

- Enterprise-level
- Division or subsidiary
- Business unit processes

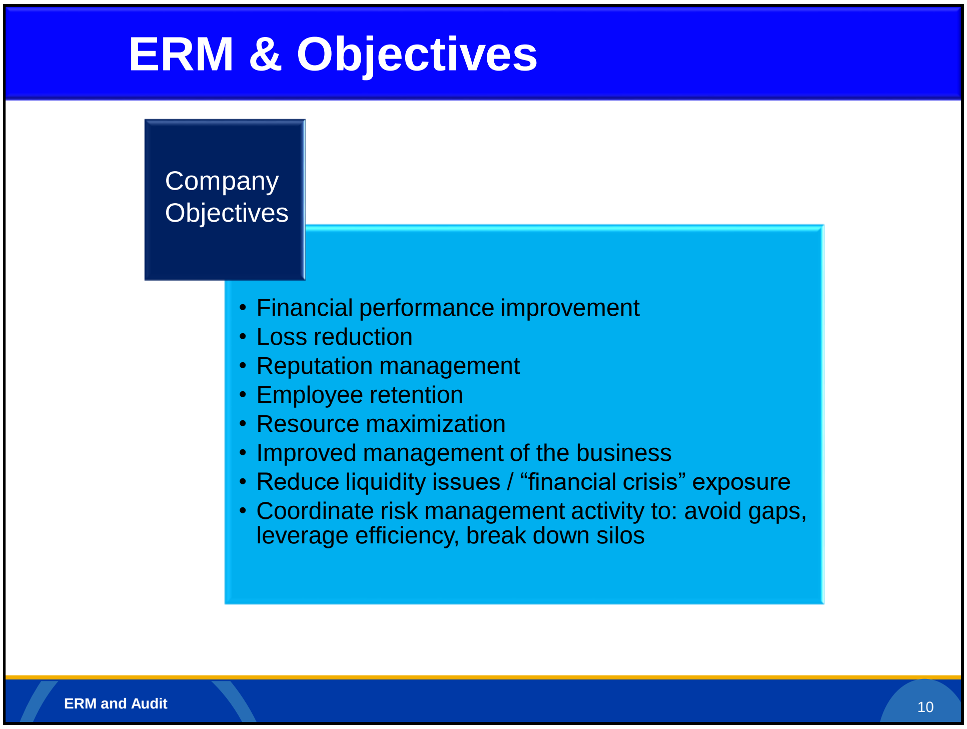




COSO Definition

ERM is a process

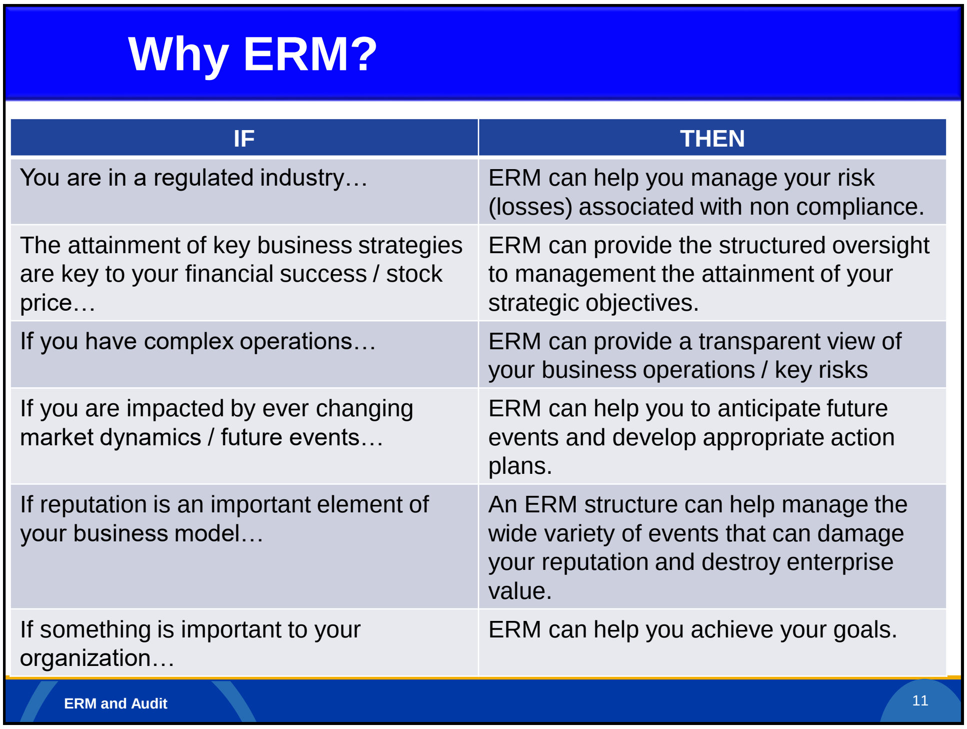
- effected by an entity’s board of directors and other personnel
- applied in strategy-setting and across the enterprise
- designed to identify potential events that may affect the entity
- to manage risk to be within its risk appetite
- to provide reasonable assurance regarding the achievement of entity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



ERM & Objectives

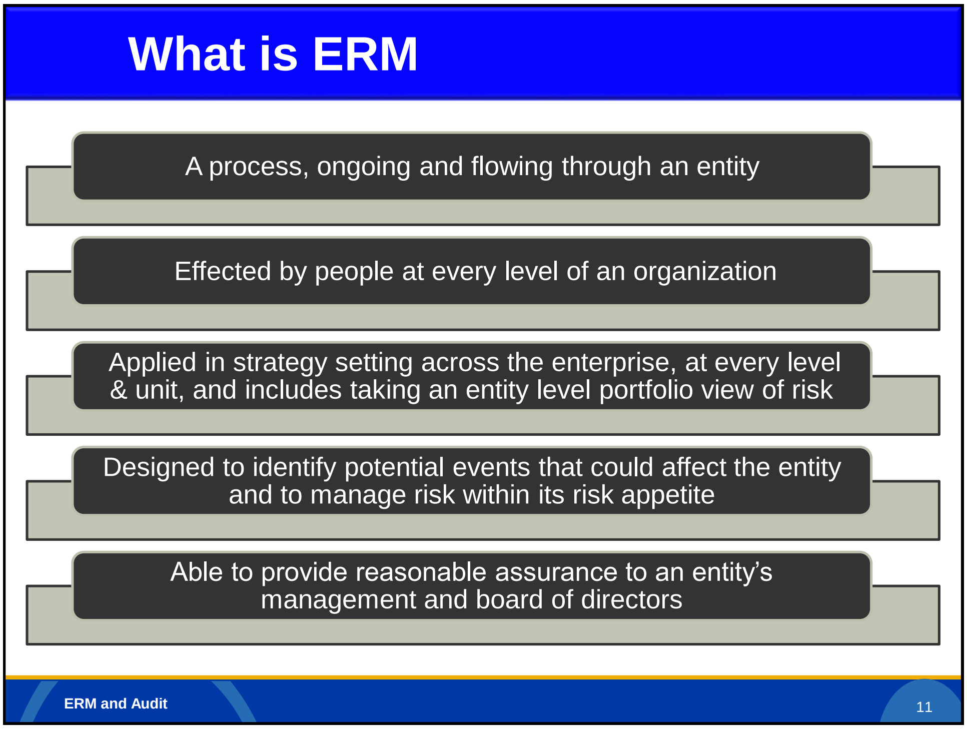
Company Objectives

- Financial performance improvement
- Loss reduction
- Reputation management
- Employee retention
- Resource maximization
- Improved management of the business
- Reduce liquidity issues / “financial crisis” exposure
- Coordinate risk management activity to: avoid gaps, leverage efficiency, break down silos



Why ERM?

IF	THEN
You are in a regulated industry…	ERM can help you manage your risk (losses) associated with non compliance.
The attainment of key business strategies are key to your financial success / stock price…	ERM can provide the structured oversight to management the attainment of your strategic objectives.
If you have complex operations…	ERM can provide a transparent view of your business operations / key risks
If you are impacted by ever changing market dynamics / future events…	ERM can help you to anticipate future events and develop appropriate action plans.
If reputation is an important element of your business model…	An ERM structure can help manage the wide variety of events that can damage your reputation and destroy enterprise value.
If something is important to your organization…	ERM can help you achieve your goals.



What is ERM

A process, ongoing and flowing through an entity

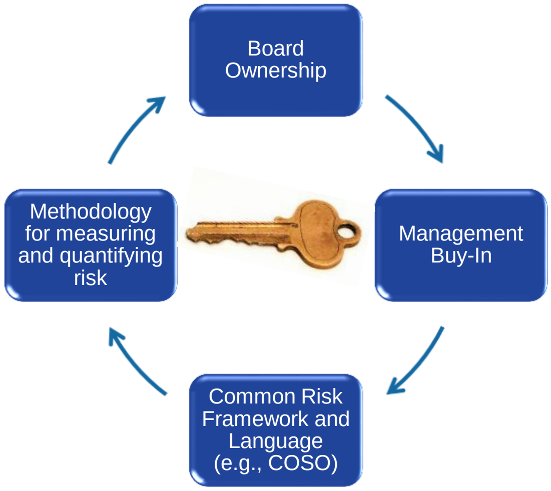
Effected by people at every level of an organization

Applied in strategy setting across the enterprise, at every level & unit, and includes taking an entity level portfolio view of risk

Designed to identify potential events that could affect the entity and to manage risk within its risk appetite

Able to provide reasonable assurance to an entity's management and board of directors

ERM Program – Key Elements



Board Ownership

Management Buy-In

Common Risk Framework and Language (e.g., COSO)

Methodology for measuring and quantifying risk

ERM Charter

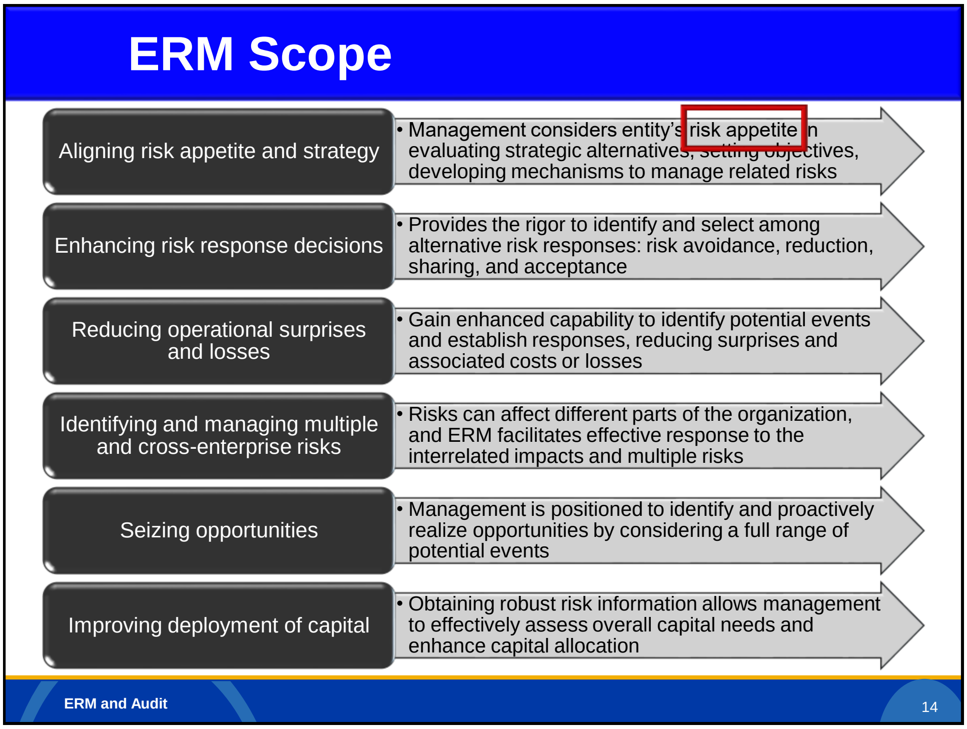
Board ownership of enterprise risks

Responsibilities for identifying, assessing and reporting on risks

Risk definitions and terminology

Measurement/ranking methodology

Reporting frequency and standards

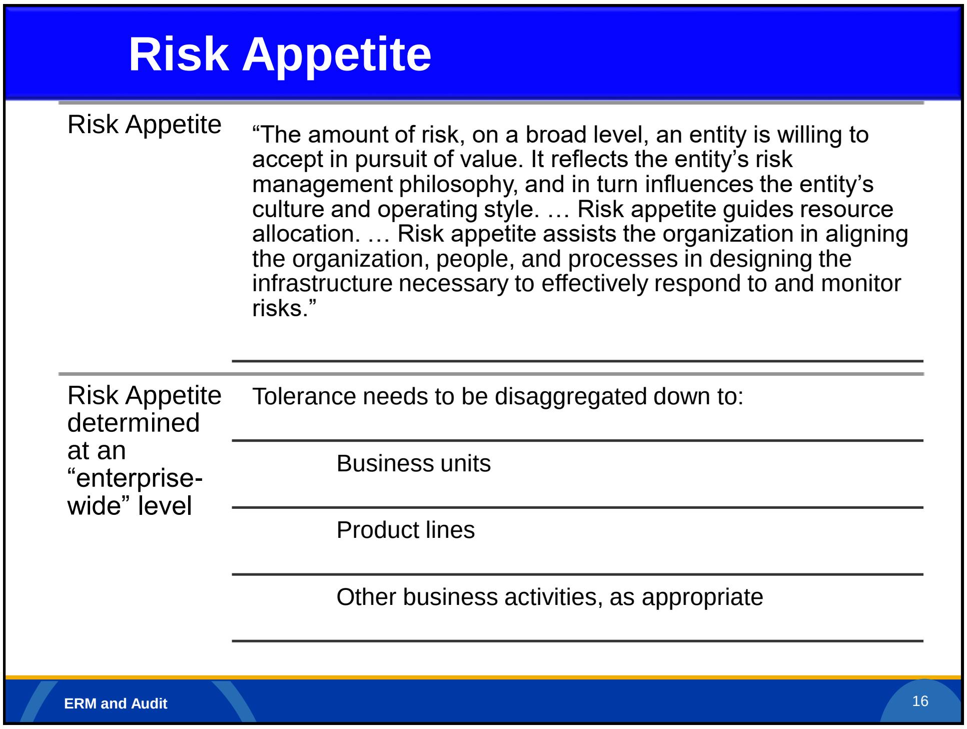


ERM Scope

Aligning risk appetite and strategy	• Management considers entity's risk appetite in evaluating strategic alternatives, setting objectives, developing mechanisms to manage related risks
Enhancing risk response decisions	• Provides the rigor to identify and select among alternative risk responses: risk avoidance, reduction, sharing, and acceptance
Reducing operational surprises and losses	• Gain enhanced capability to identify potential events and establish responses, reducing surprises and associated costs or losses
Identifying and managing multiple and cross-enterprise risks	• Risks can affect different parts of the organization, and ERM facilitates effective response to the interrelated impacts and multiple risks
Seizing opportunities	• Management is positioned to identify and proactively realize opportunities by considering a full range of potential events
Improving deployment of capital	• Obtaining robust risk information allows management to effectively assess overall capital needs and enhance capital allocation

ERM and Audit

14



Risk Appetite

Risk Appetite

"The amount of risk, on a broad level, an entity is willing to accept in pursuit of value. It reflects the entity's risk management philosophy, and in turn influences the entity's culture and operating style. … Risk appetite guides resource allocation. … Risk appetite assists the organization in aligning the organization, people, and processes in designing the infrastructure necessary to effectively respond to and monitor risks."

Risk Appetite determined at an "enterprise-wide" level

Tolerance needs to be disaggregated down to:

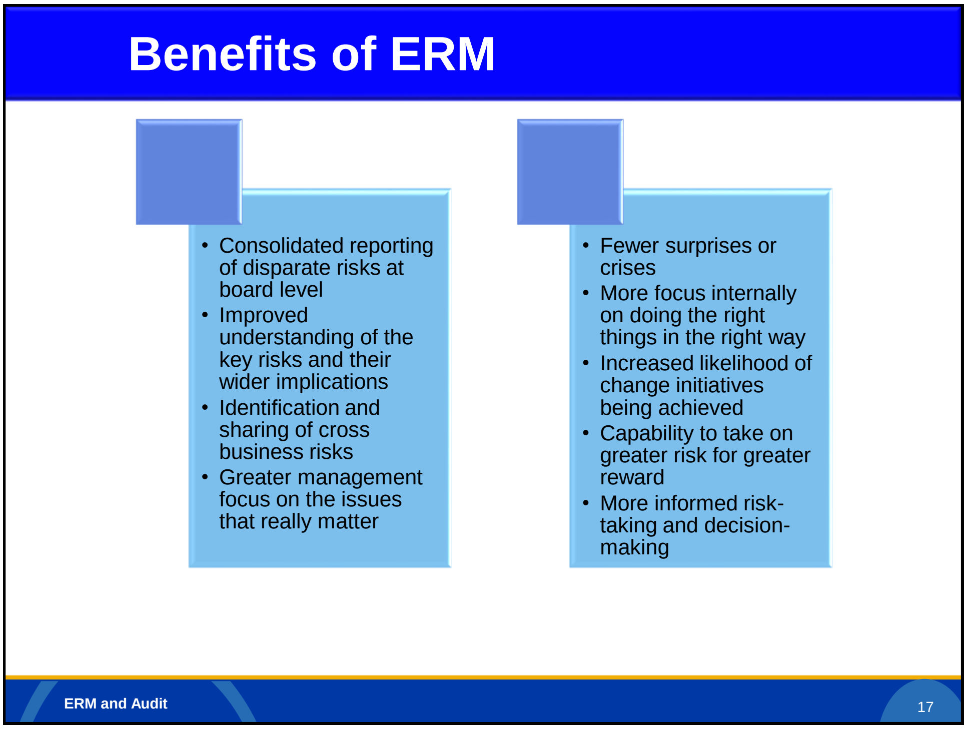
Business units

Product lines

Other business activities, as appropriate

ERM and Audit

16



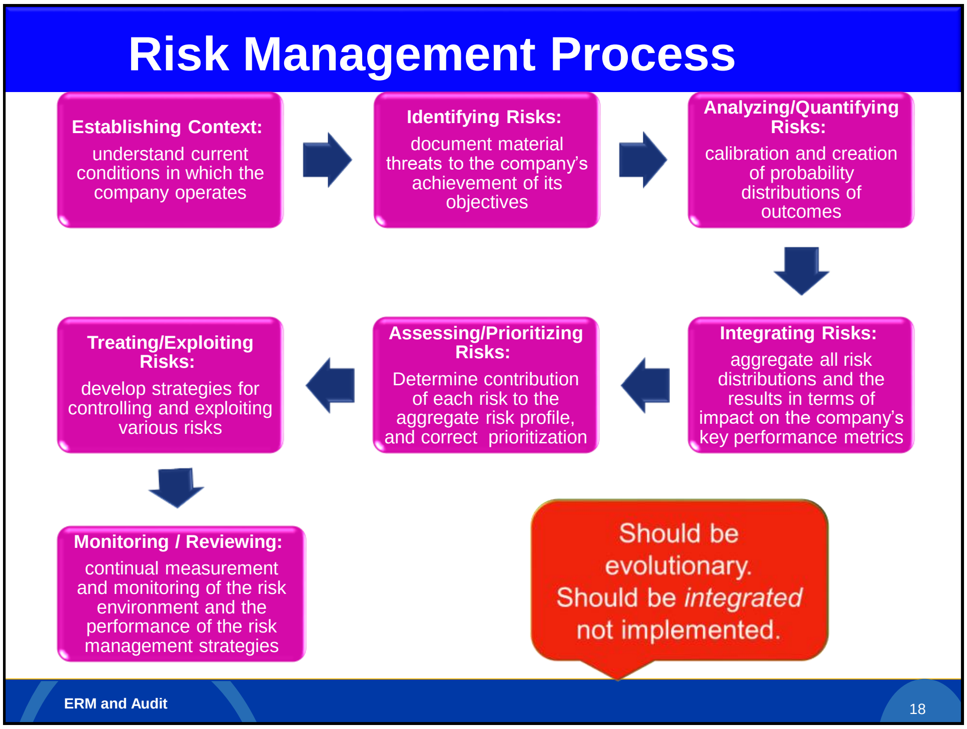
Benefits of ERM

- Consolidated reporting of disparate risks at board level
- Improved understanding of the key risks and their wider implications
- Identification and sharing of cross business risks
- Greater management focus on the issues that really matter

- Fewer surprises or crises
- More focus internally on doing the right things in the right way
- Increased likelihood of change initiatives being achieved
- Capability to take on greater risk for greater reward
- More informed risk-taking and decision-making

ERM and Audit

17



Risk Management Process

Establishing Context: understand current conditions in which the company operates

Identifying Risks: document material threats to the company's achievement of its objectives

Analyzing/Quantifying Risks: calibration and creation of probability distributions of outcomes

Integrating Risks: aggregate all risk distributions and the results in terms of impact on the company's key performance metrics

Assessing/Prioritizing Risks: Determine contribution of each risk to the aggregate risk profile, and correct prioritization

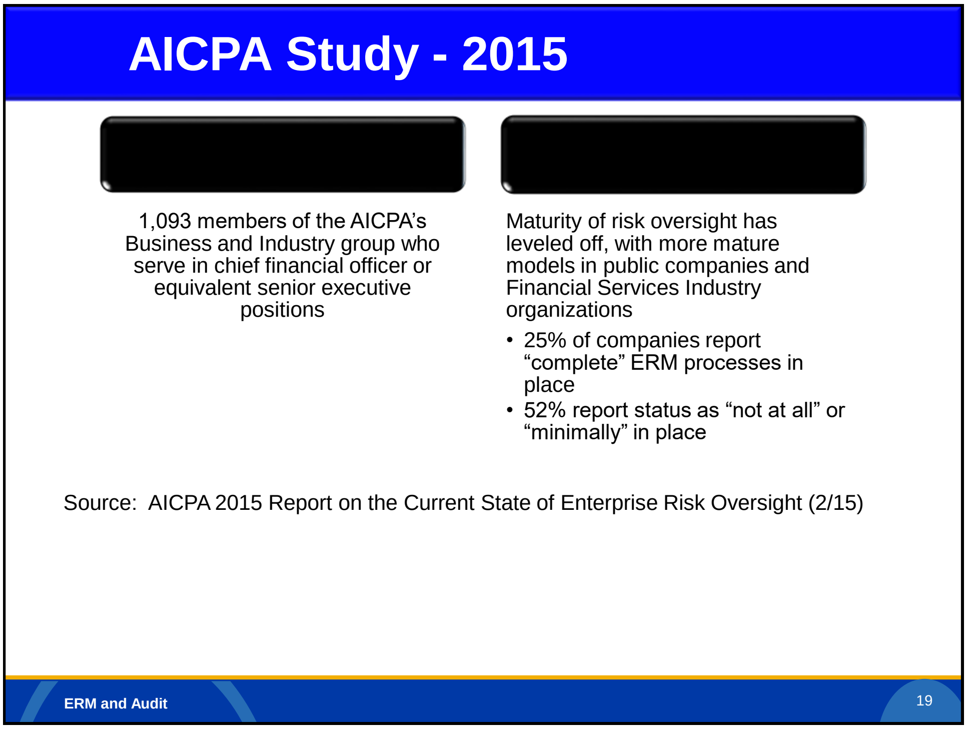
Treating/Exploiting Risks: develop strategies for controlling and exploiting various risks

Monitoring / Reviewing: continual measurement and monitoring of the risk environment and the performance of the risk management strategies

Should be evolutionary.
Should be *integrated* not implemented.

ERM and Audit

18



AICPA Study - 2015

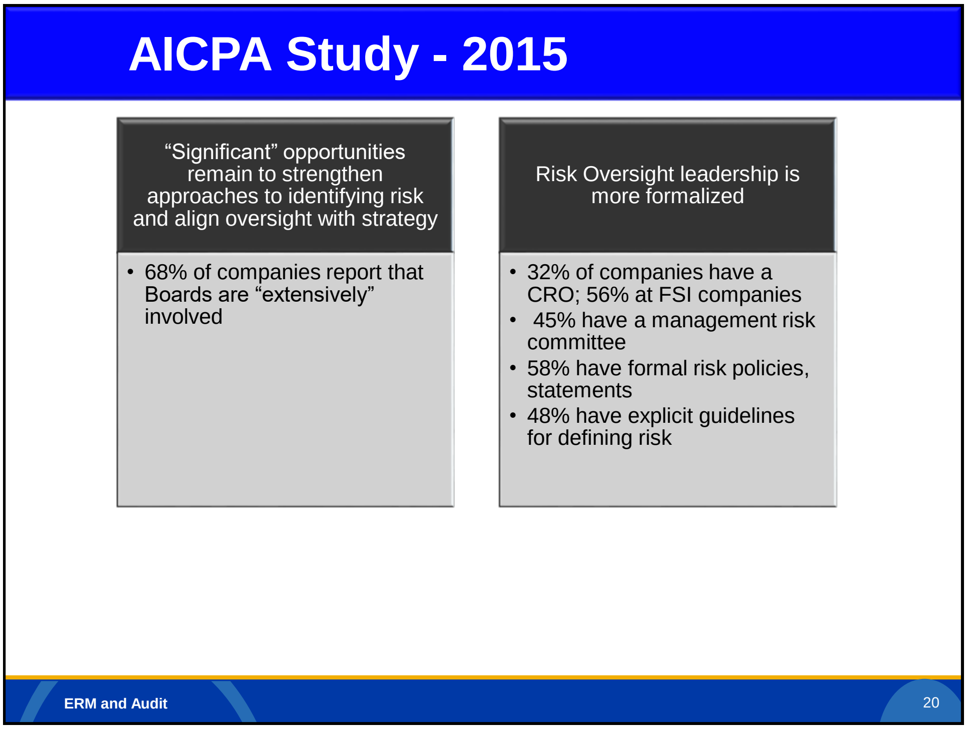
1,093 members of the AICPA's Business and Industry group who serve in chief financial officer or equivalent senior executive positions

Maturity of risk oversight has leveled off, with more mature models in public companies and Financial Services Industry organizations

- 25% of companies report "complete" ERM processes in place
- 52% report status as "not at all" or "minimally" in place

Source: AICPA 2015 Report on the Current State of Enterprise Risk Oversight (2/15)

ERM and Audit 19



AICPA Study - 2015

"Significant" opportunities remain to strengthen approaches to identifying risk and align oversight with strategy

- 68% of companies report that Boards are "extensively" involved

Risk Oversight leadership is more formalized

- 32% of companies have a CRO; 56% at FSI companies
- 45% have a management risk committee
- 58% have formal risk policies, statements
- 48% have explicit guidelines for defining risk

ERM and Audit 20

A Missing Element

Shows the board and management that the goal of risk management should be to increase certainty that organizations will achieve their strategic objectives, and not get unexpected/bad surprises

Ownership

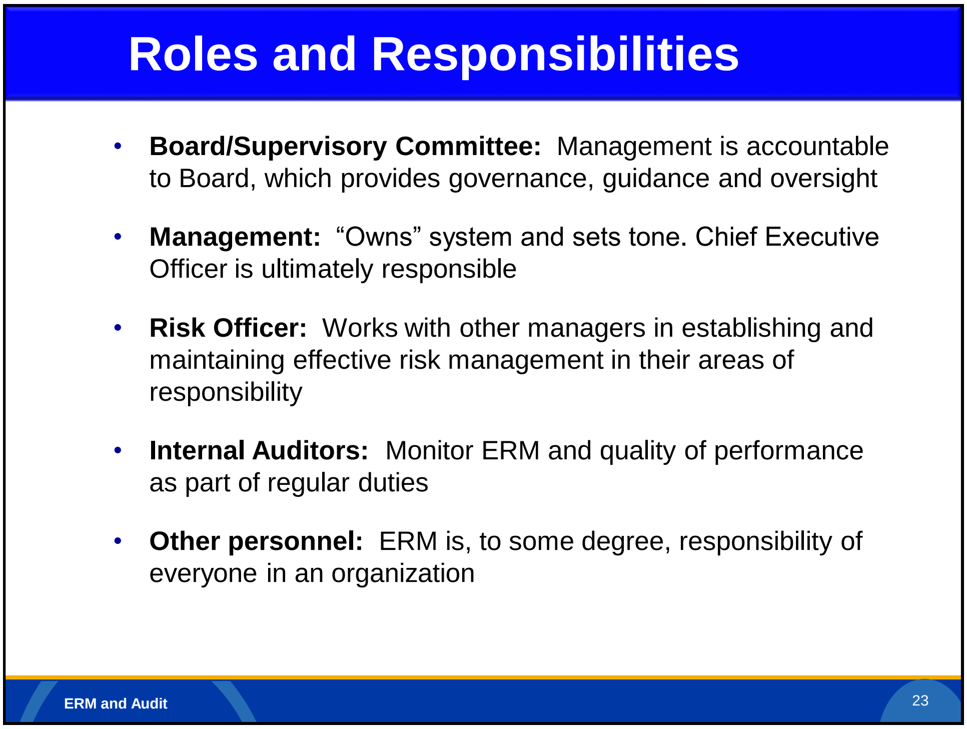
Ownership begins at the top with executive management

Filters down to unit and functional managers

Board of Directors provides oversight

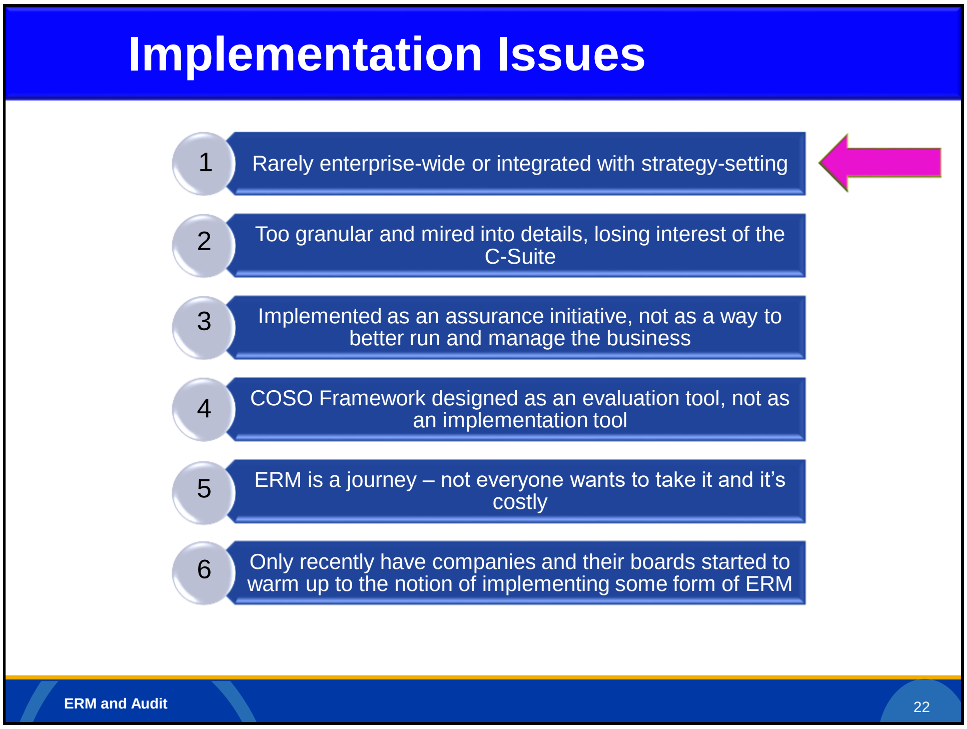
Corporate Risk Officer should be in place

Everyone in organization has responsibility for ERM



Roles and Responsibilities

- **Board/Supervisory Committee:** Management is accountable to Board, which provides governance, guidance and oversight
- **Management:** "Owns" system and sets tone. Chief Executive Officer is ultimately responsible
- **Risk Officer:** Works with other managers in establishing and maintaining effective risk management in their areas of responsibility
- **Internal Auditors:** Monitor ERM and quality of performance as part of regular duties
- **Other personnel:** ERM is, to some degree, responsibility of everyone in an organization



Implementation Issues

1 Rarely enterprise-wide or integrated with strategy-setting

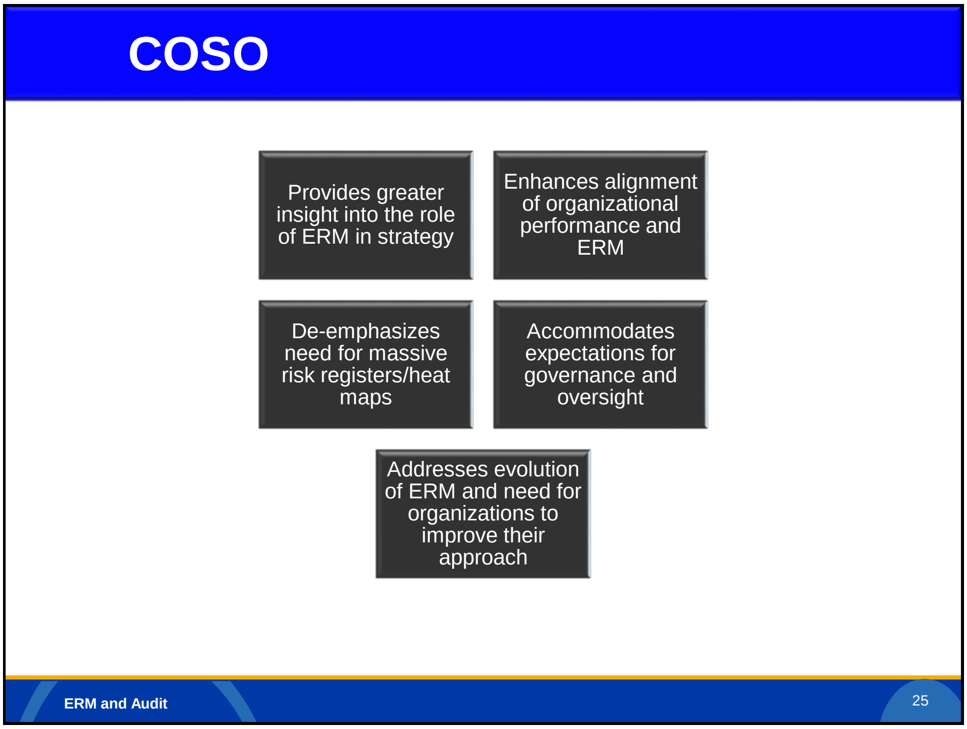
2 Too granular and mired into details, losing interest of the C-Suite

3 Implemented as an assurance initiative, not as a way to better run and manage the business

4 COSO Framework designed as an evaluation tool, not as an implementation tool

5 ERM is a journey – not everyone wants to take it and it's costly

6 Only recently have companies and their boards started to warm up to the notion of implementing some form of ERM



COSO

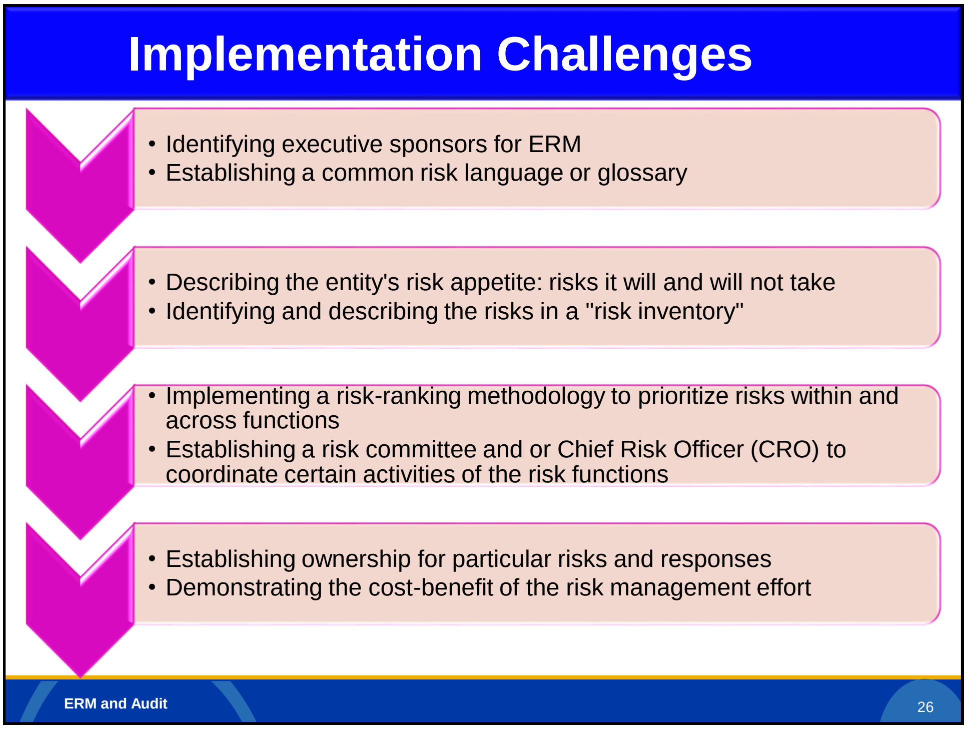
Provides greater insight into the role of ERM in strategy

Enhances alignment of organizational performance and ERM

De-emphasizes need for massive risk registers/heat maps

Accommodates expectations for governance and oversight

Addresses evolution of ERM and need for organizations to improve their approach



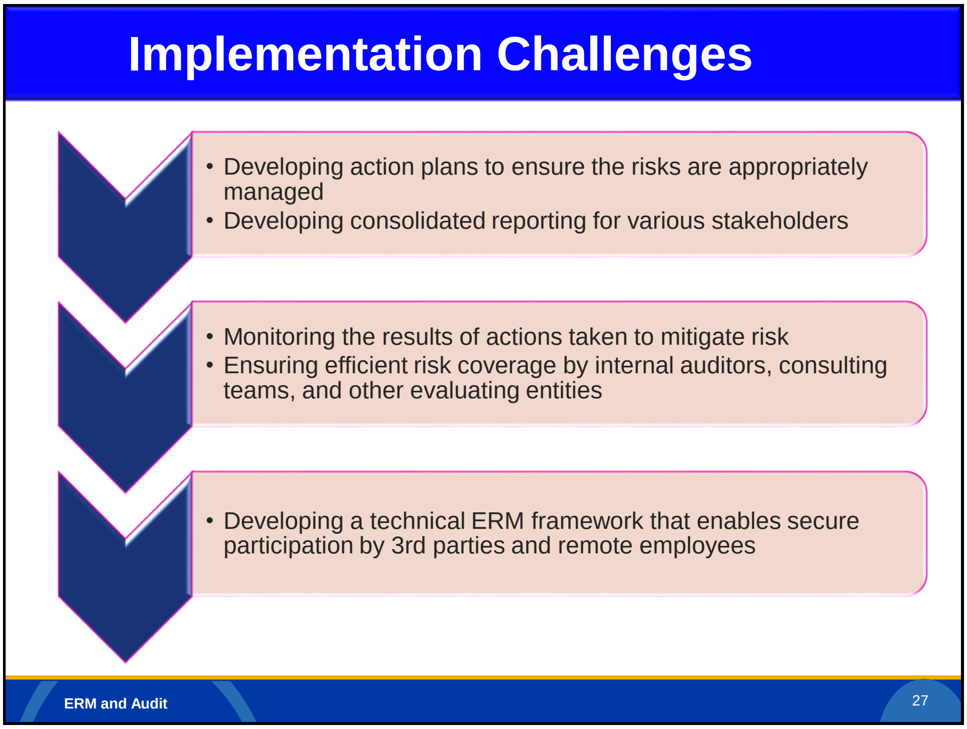
Implementation Challenges

- Identifying executive sponsors for ERM
- Establishing a common risk language or glossary

- Describing the entity's risk appetite: risks it will and will not take
- Identifying and describing the risks in a "risk inventory"

- Implementing a risk-ranking methodology to prioritize risks within and across functions
- Establishing a risk committee and or Chief Risk Officer (CRO) to coordinate certain activities of the risk functions

- Establishing ownership for particular risks and responses
- Demonstrating the cost-benefit of the risk management effort



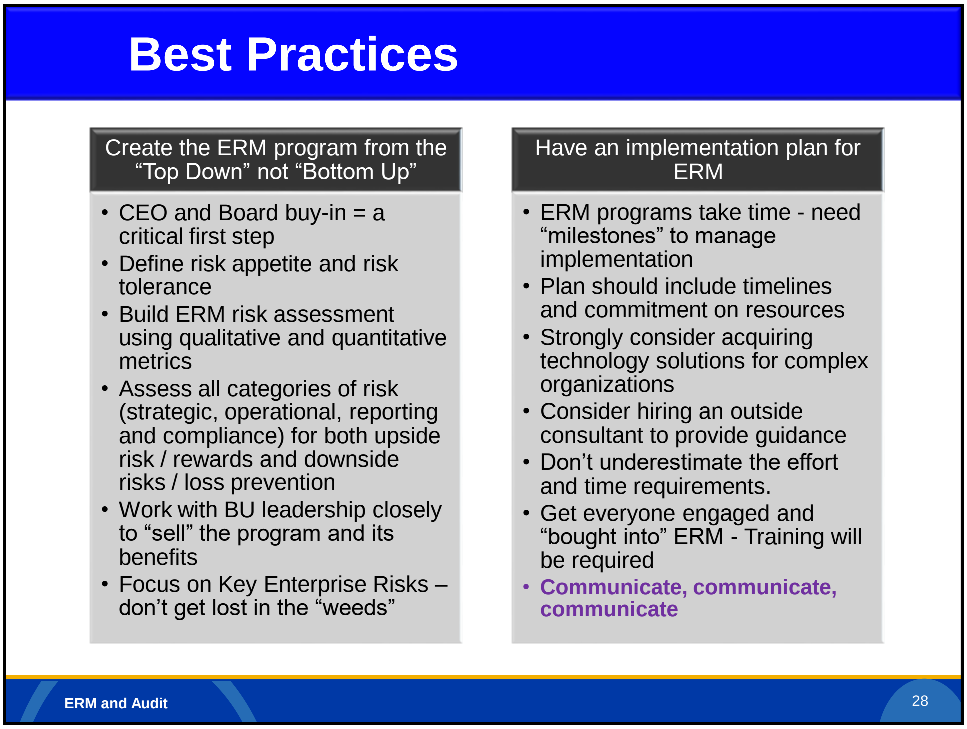
Implementation Challenges

- Developing action plans to ensure the risks are appropriately managed
- Developing consolidated reporting for various stakeholders

- Monitoring the results of actions taken to mitigate risk
- Ensuring efficient risk coverage by internal auditors, consulting teams, and other evaluating entities

- Developing a technical ERM framework that enables secure participation by 3rd parties and remote employees

ERM and Audit 27



Best Practices

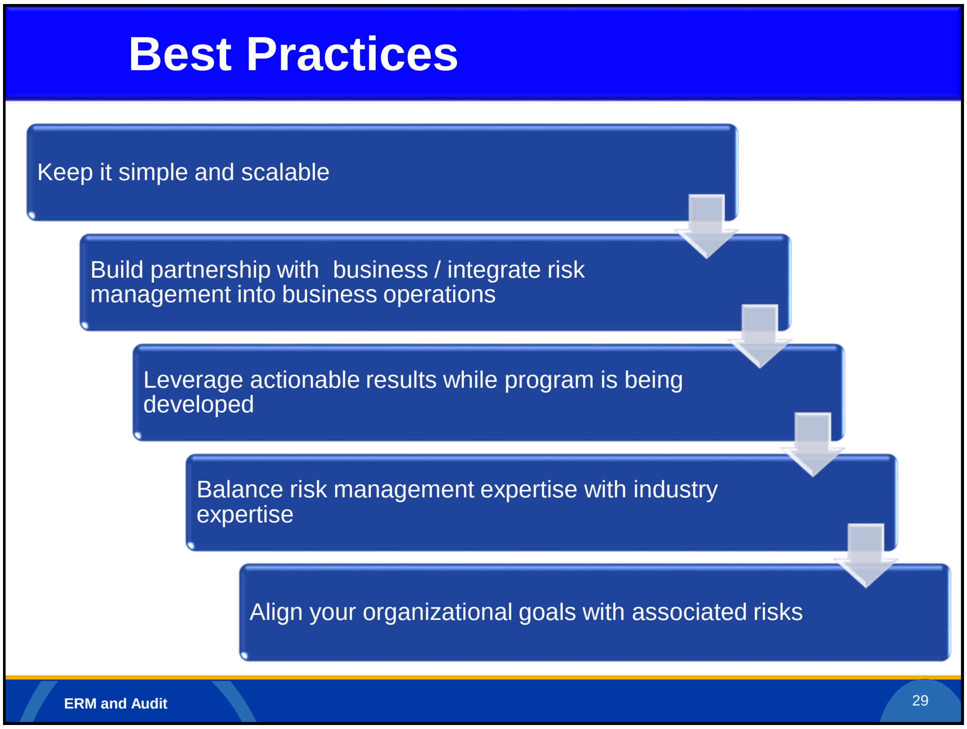
Create the ERM program from the "Top Down" not "Bottom Up"

- CEO and Board buy-in = a critical first step
- Define risk appetite and risk tolerance
- Build ERM risk assessment using qualitative and quantitative metrics
- Assess all categories of risk (strategic, operational, reporting and compliance) for both upside risk / rewards and downside risks / loss prevention
- Work with BU leadership closely to "sell" the program and its benefits
- Focus on Key Enterprise Risks – don't get lost in the "weeds"

Have an implementation plan for ERM

- ERM programs take time - need "milestones" to manage implementation
- Plan should include timelines and commitment on resources
- Strongly consider acquiring technology solutions for complex organizations
- Consider hiring an outside consultant to provide guidance
- Don't underestimate the effort and time requirements.
- Get everyone engaged and "bought into" ERM - Training will be required
- **Communicate, communicate, communicate**

ERM and Audit 28



Best Practices

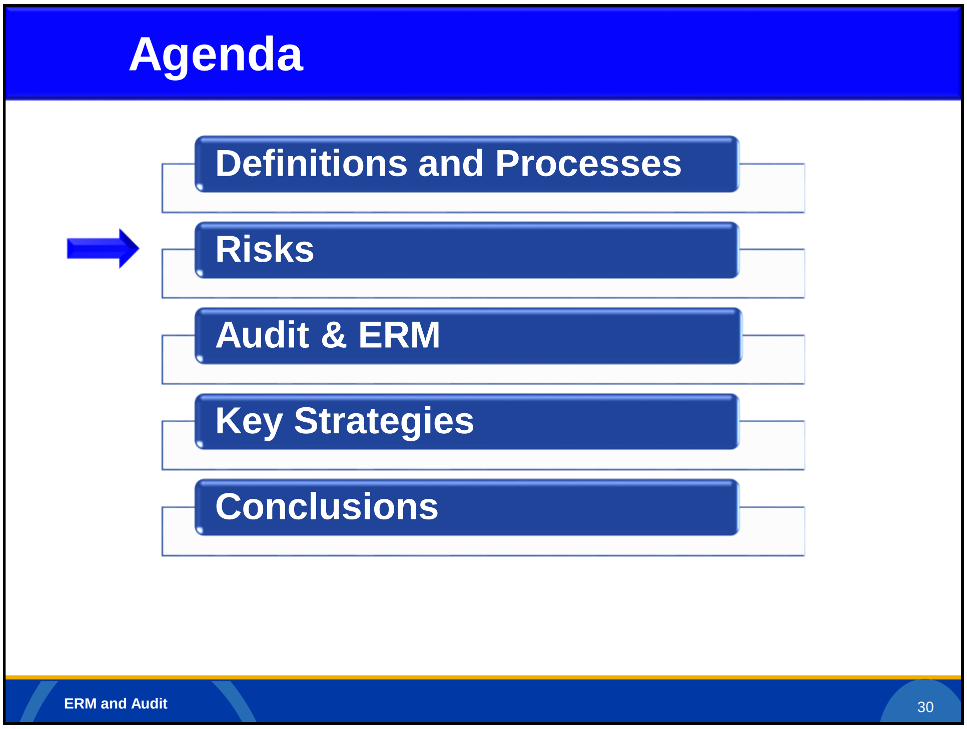
Keep it simple and scalable

Build partnership with business / integrate risk management into business operations

Leverage actionable results while program is being developed

Balance risk management expertise with industry expertise

Align your organizational goals with associated risks



Agenda

Definitions and Processes

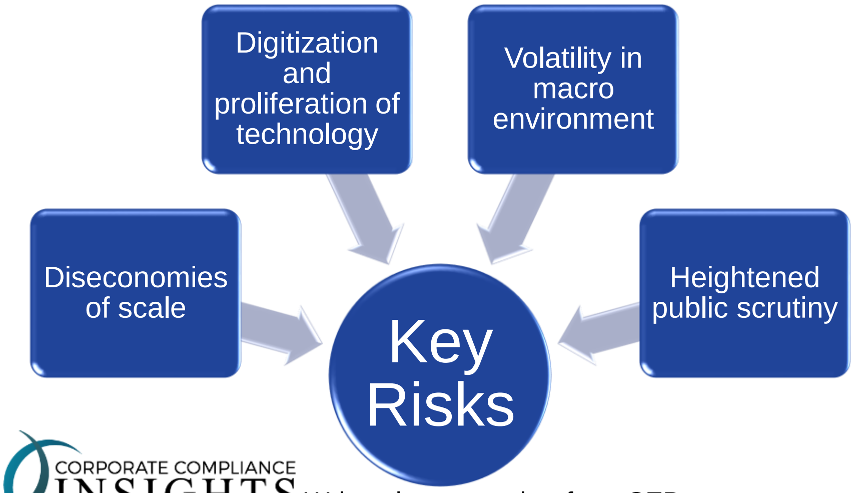
Risks

Audit & ERM

Key Strategies

Conclusions

2017 Risk Themes for IA

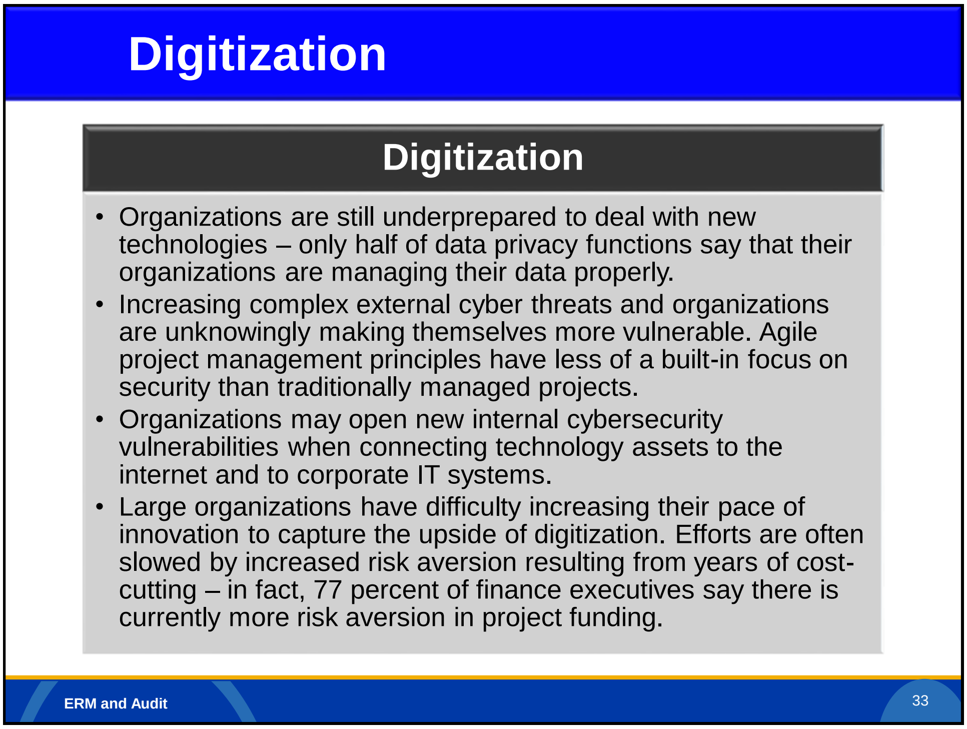

Digitization and proliferation of technology
Volatility in macro environment
Diseconomies of scale
Key Risks
Heightened public scrutiny

CORPORATE COMPLIANCE INSIGHTS Written by researcher from CEB

Diseconomies

Diseconomies

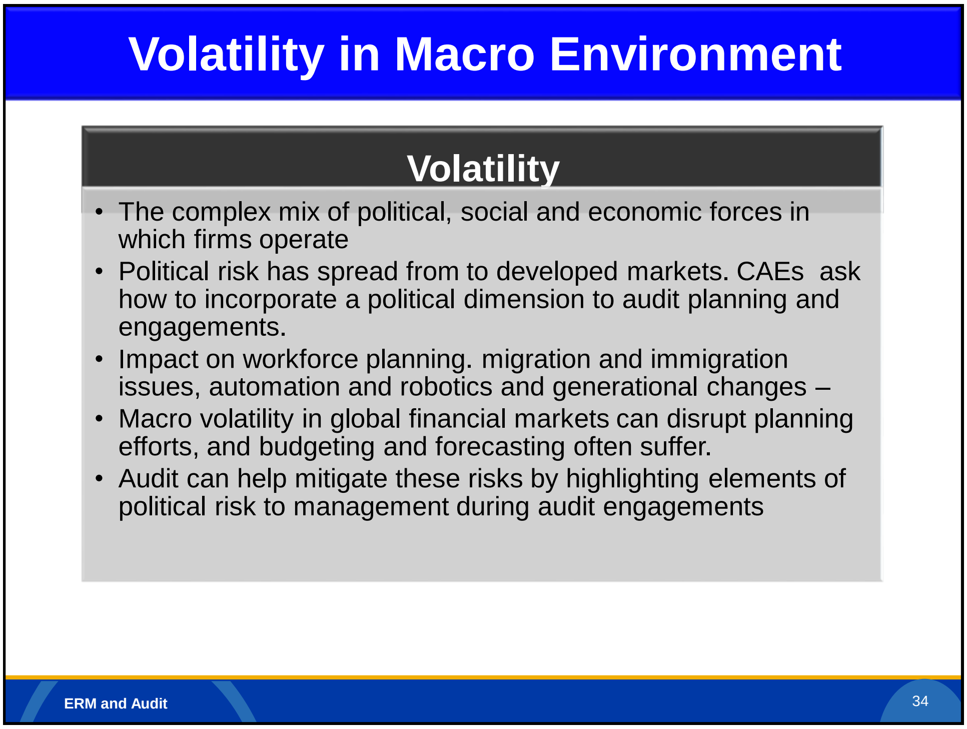
- Organizations are larger and that leads to greater complexity and an increased cost of coordinating activities.
- These are often seen only by functions with a central viewpoint, such as audit.
- This year, they contribute to three risks CAEs are tracking: third-party relationships, strategic decision-making and execution and change fatigue.



Digitization

Digitization

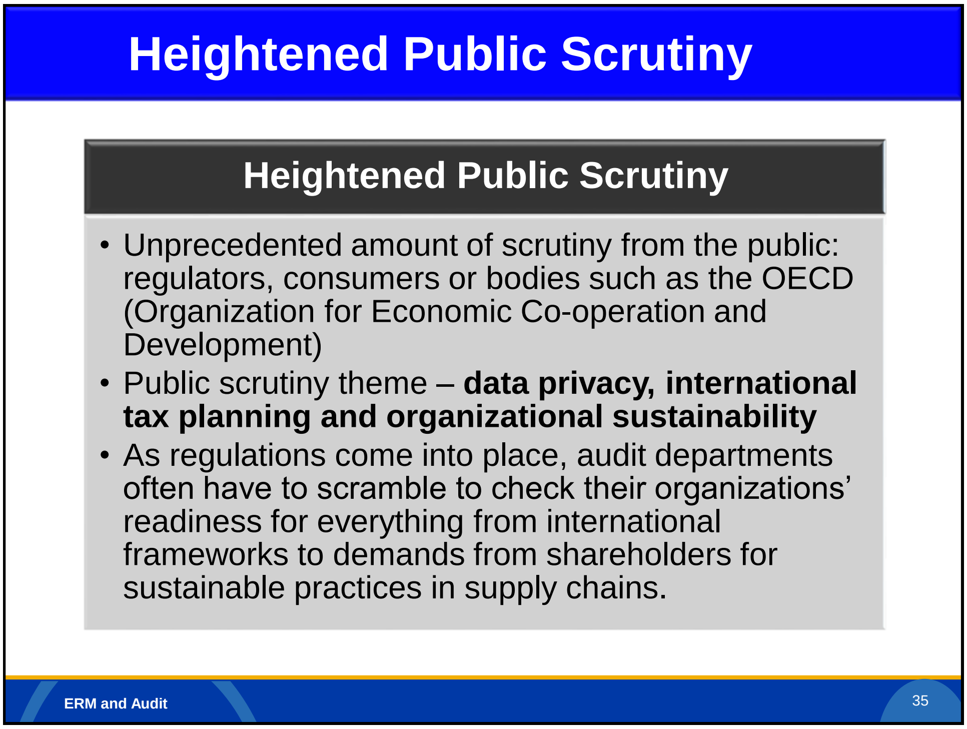
- Organizations are still underprepared to deal with new technologies – only half of data privacy functions say that their organizations are managing their data properly.
- Increasing complex external cyber threats and organizations are unknowingly making themselves more vulnerable. Agile project management principles have less of a built-in focus on security than traditionally managed projects.
- Organizations may open new internal cybersecurity vulnerabilities when connecting technology assets to the internet and to corporate IT systems.
- Large organizations have difficulty increasing their pace of innovation to capture the upside of digitization. Efforts are often slowed by increased risk aversion resulting from years of cost-cutting – in fact, 77 percent of finance executives say there is currently more risk aversion in project funding.



Volatility in Macro Environment

Volatility

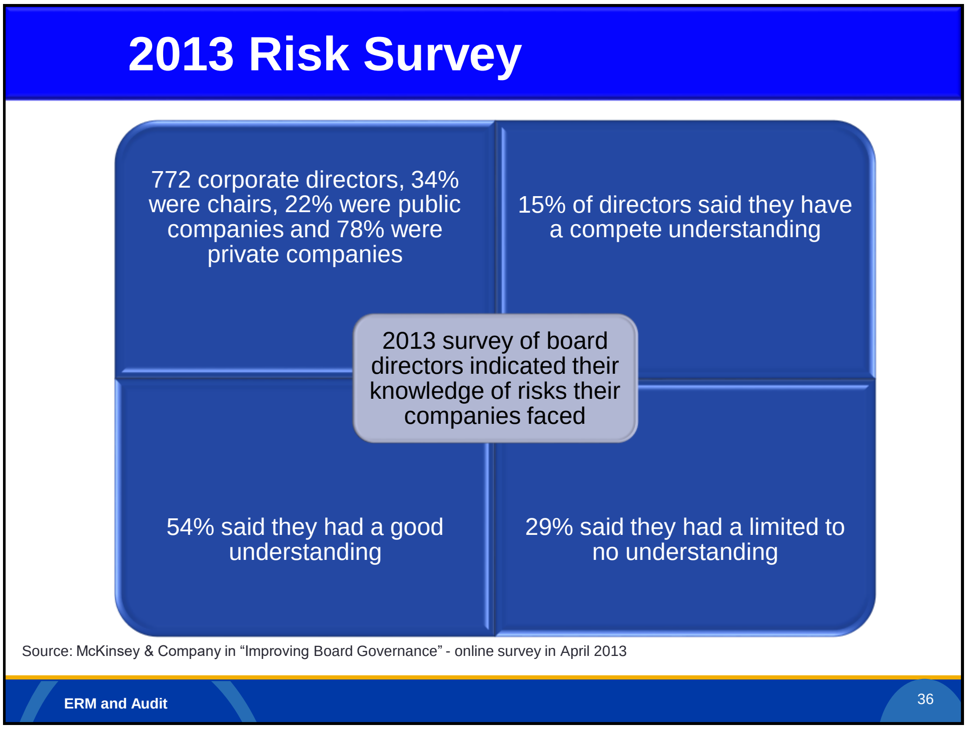
- The complex mix of political, social and economic forces in which firms operate
- Political risk has spread from to developed markets. CAEs ask how to incorporate a political dimension to audit planning and engagements.
- Impact on workforce planning. migration and immigration issues, automation and robotics and generational changes –
- Macro volatility in global financial markets can disrupt planning efforts, and budgeting and forecasting often suffer.
- Audit can help mitigate these risks by highlighting elements of political risk to management during audit engagements



Heightened Public Scrutiny

Heightened Public Scrutiny

- Unprecedented amount of scrutiny from the public: regulators, consumers or bodies such as the OECD (Organization for Economic Co-operation and Development)
- Public scrutiny theme – **data privacy, international tax planning and organizational sustainability**
- As regulations come into place, audit departments often have to scramble to check their organizations' readiness for everything from international frameworks to demands from shareholders for sustainable practices in supply chains.



2013 Risk Survey

2013 survey of board directors indicated their knowledge of risks their companies faced

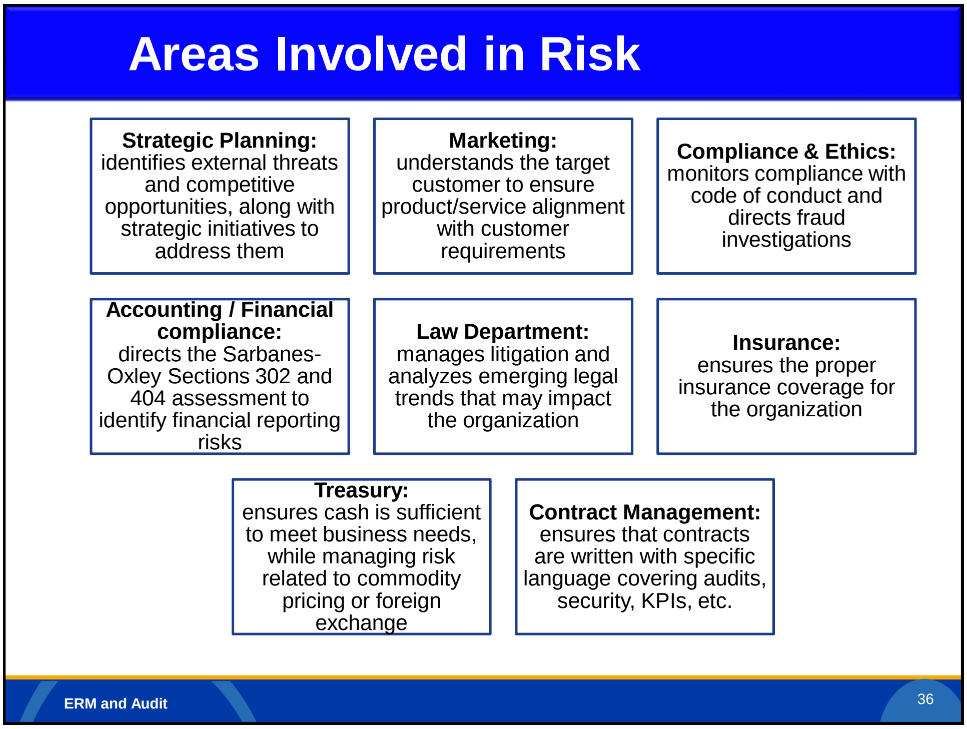
772 corporate directors, 34% were chairs, 22% were public companies and 78% were private companies

15% of directors said they have a compete understanding

54% said they had a good understanding

29% said they had a limited to no understanding

Source: McKinsey & Company in "Improving Board Governance" - online survey in April 2013



Areas Involved in Risk

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 Sections 302 and 404 assessment to identify financial reporting risks

Law Department: manages litigation and analyzes emerging legal trends that may impact the organization

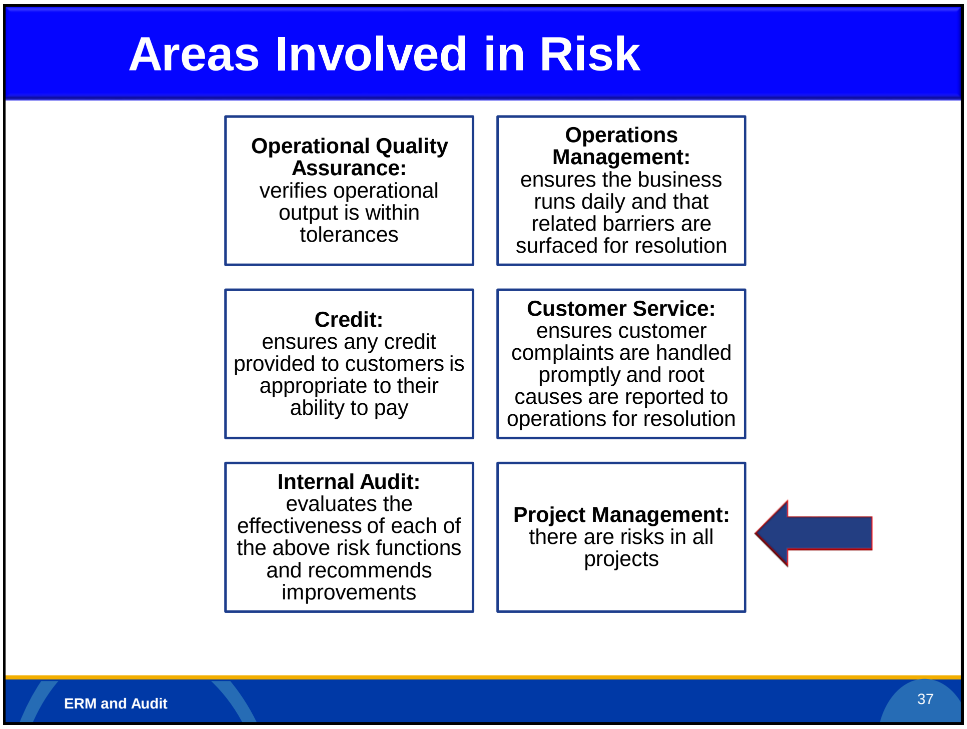
Insurance: ensures the proper insurance coverage for the organization

Treasury: ensures cash is sufficient to meet business needs, while managing risk related to commodity pricing or foreign exchange

Contract Management: ensures that contracts are written with specific language covering audits, security, KPIs, etc.

ERM and Audit

36



Areas Involved in Risk

Operational Quality Assurance: verifies operational output is within tolerances

Operations Management: ensures the business runs daily and that related barriers are surfaced for resolution

Credit: ensures any credit provided to customers is appropriate to their ability to pay

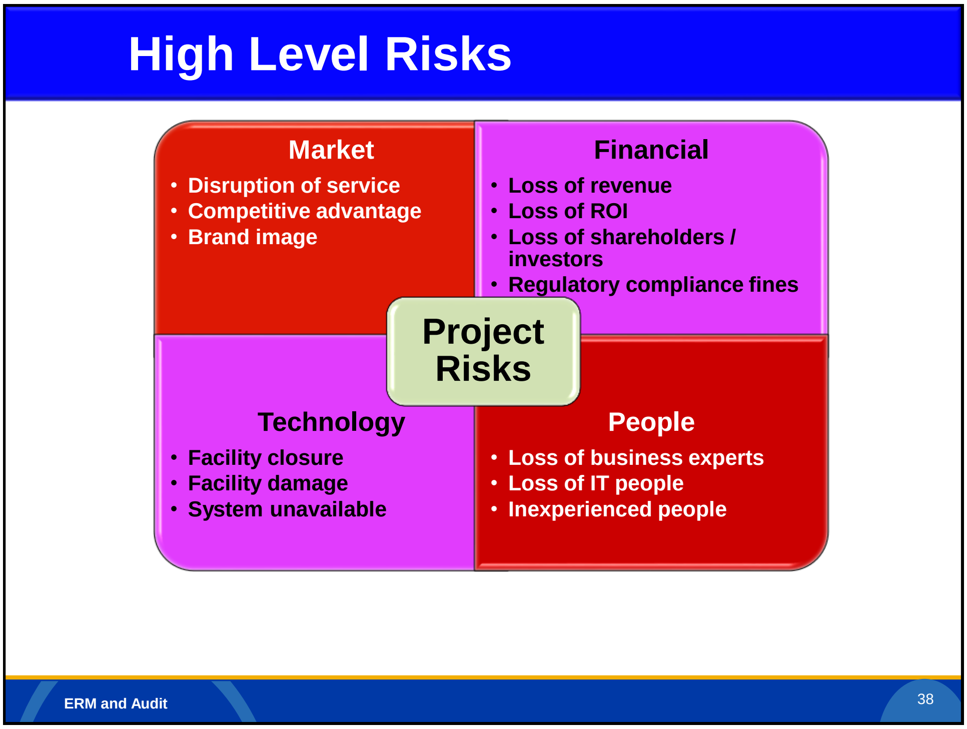
Customer Service: ensures customer complaints are handled promptly and root causes are reported to operations for resolution

Internal Audit: evaluates the effectiveness of each of the above risk functions and recommends improvements

Project Management: there are risks in all projects

ERM and Audit

37



High Level Risks

Project Risks

Market

- Disruption of service
- Competitive advantage
- Brand image

Financial

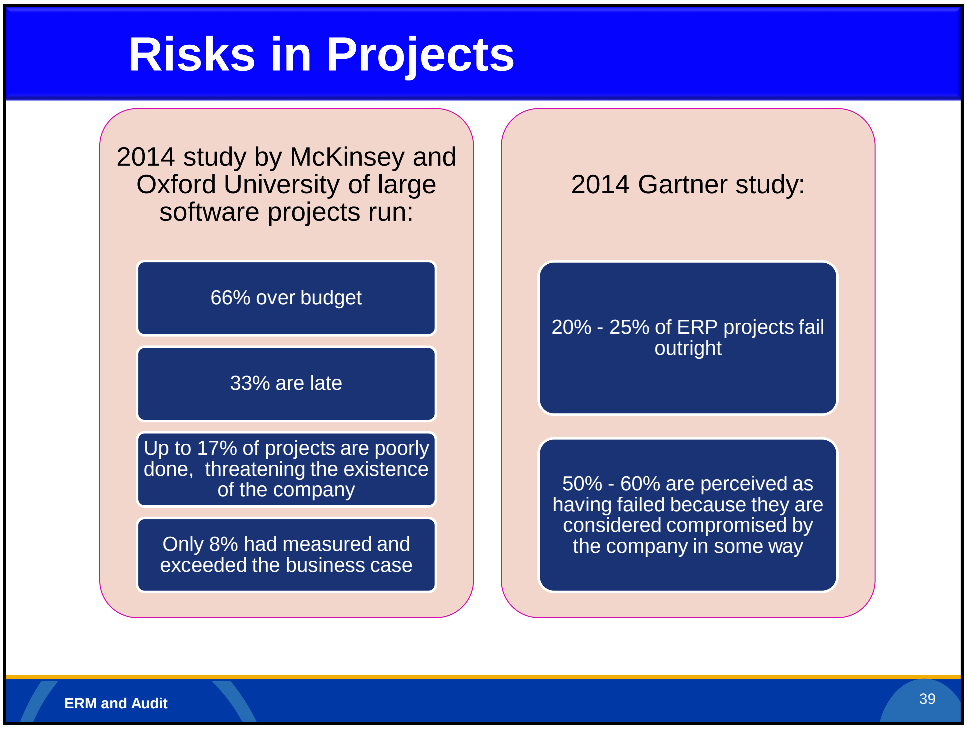
- Loss of revenue
- Loss of ROI
- Loss of shareholders / investors
- Regulatory compliance fines

Technology

- Facility closure
- Facility damage
- System unavailable

People

- Loss of business experts
- Loss of IT people
- Inexperienced people



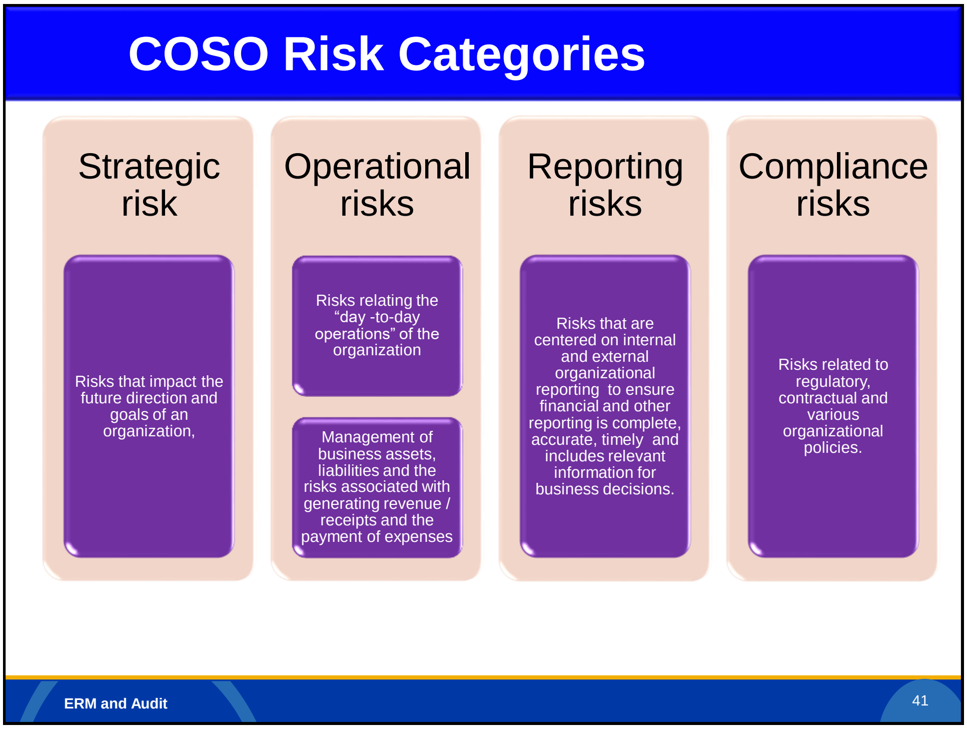
Risks in Projects

2014 study by McKinsey and Oxford University of large software projects run:

- 66% over budget
- 33% are late
- Up to 17% of projects are poorly done, threatening the existence of the company
- Only 8% had measured and exceeded the business case

2014 Gartner study:

- 20% - 25% of ERP projects fail outright
- 50% - 60% are perceived as having failed because they are considered compromised by the company in some way



COSO Risk Categories

Strategic risk

Risks that impact the future direction and goals of an organization,

Operational risks

Risks relating the “day -to-day operations” of the organization

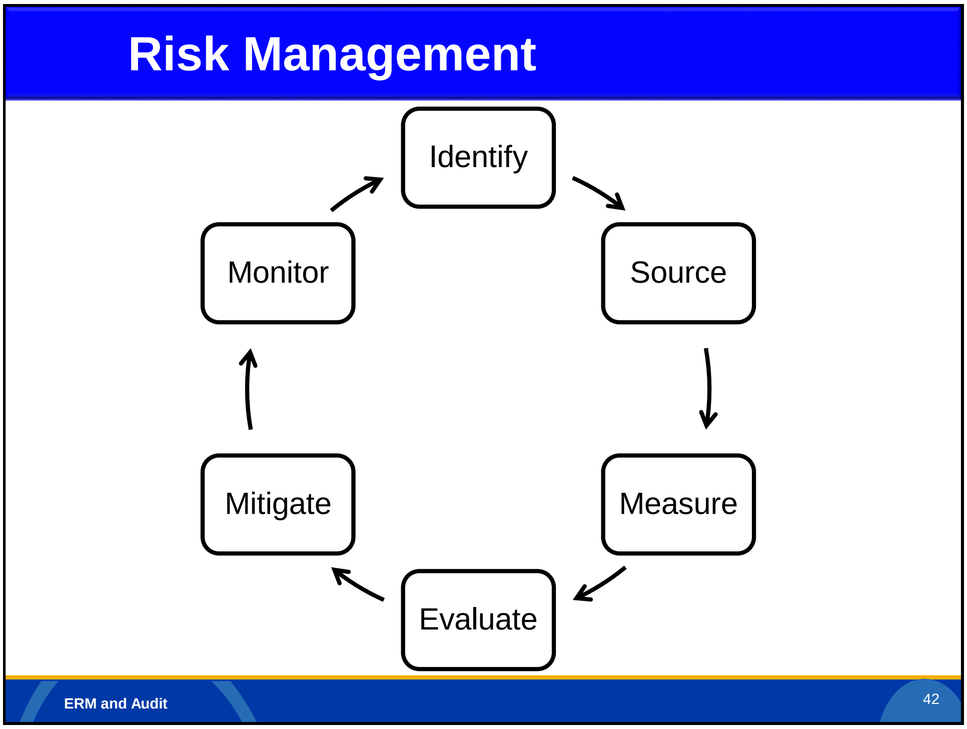
Management of business assets, liabilities and the risks associated with generating revenue / receipts and the payment of expenses

Reporting risks

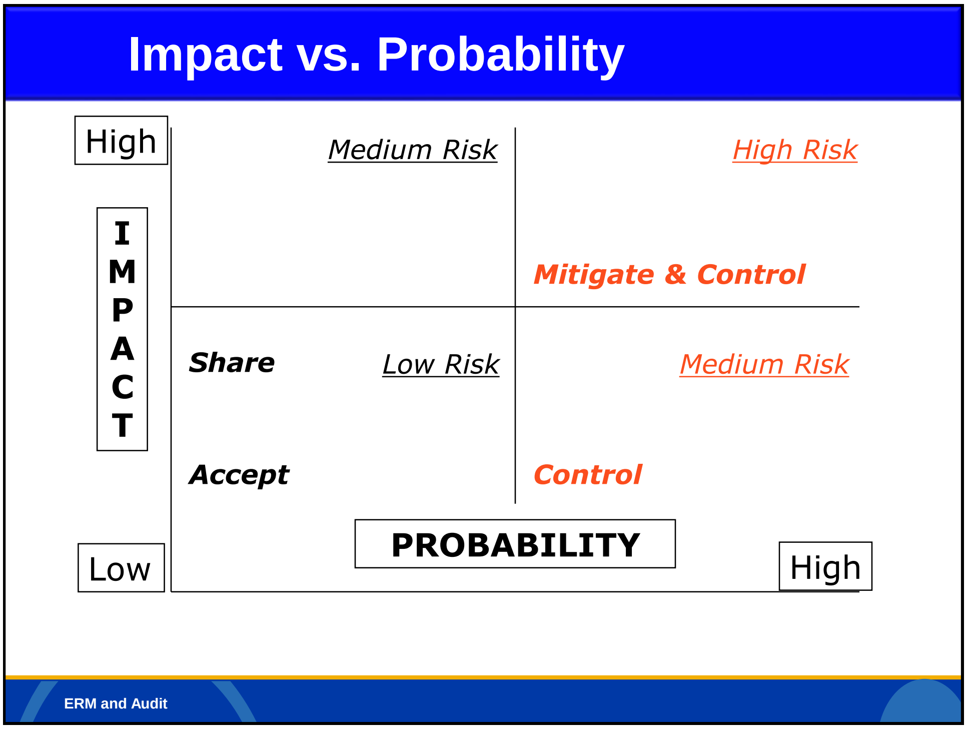
Risks that are centered on internal and external organizational reporting to ensure financial and other reporting is complete, accurate, timely and includes relevant information for business decisions.

Compliance risks

Risks related to regulatory, contractual and various organizational policies.



Risk Management



Impact vs. Probability

High

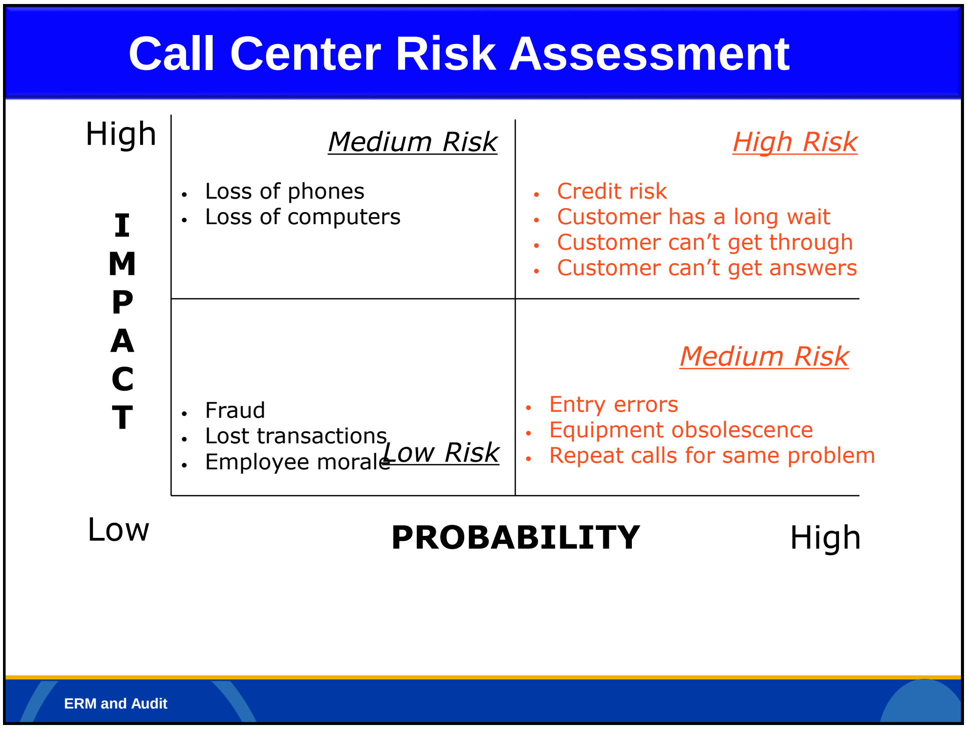
IMPACT

Low

High	*Medium Risk*	*High Risk* ***Mitigate & Control***
Low	***Share*** *Low Risk* ***Accept***	*Medium Risk* ***Control***

Low **PROBABILITY** High

ERM and Audit



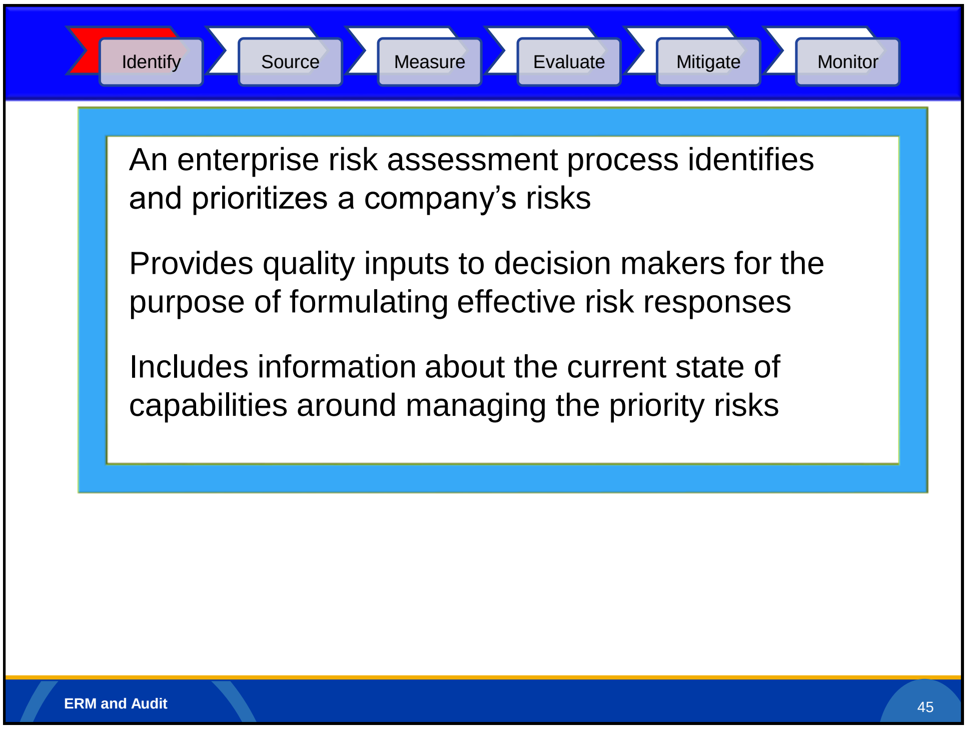
Call Center Risk Assessment

High	*Medium Risk* • Loss of phones • Loss of computers	*High Risk* • Credit risk • Customer has a long wait • Customer can't get through • Customer can't get answers
Low	*Low Risk* • Fraud • Lost transactions • Employee morale	*Medium Risk* • Entry errors • Equipment obsolescence • Repeat calls for same problem

IMPACT

Low **PROBABILITY** High

ERM and Audit



Identify | Source | Measure | Evaluate | Mitigate | Monitor

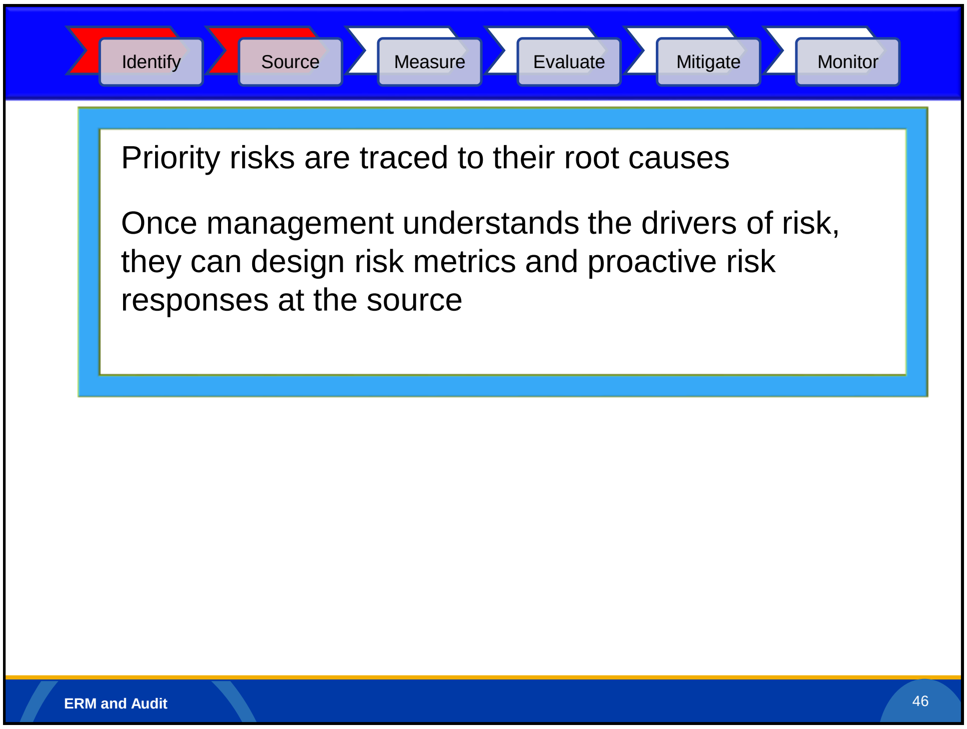
An enterprise risk assessment process identifies and prioritizes a company's risks

Provides quality inputs to decision makers for the purpose of formulating effective risk responses

Includes information about the current state of capabilities around managing the priority risks

ERM and Audit

45



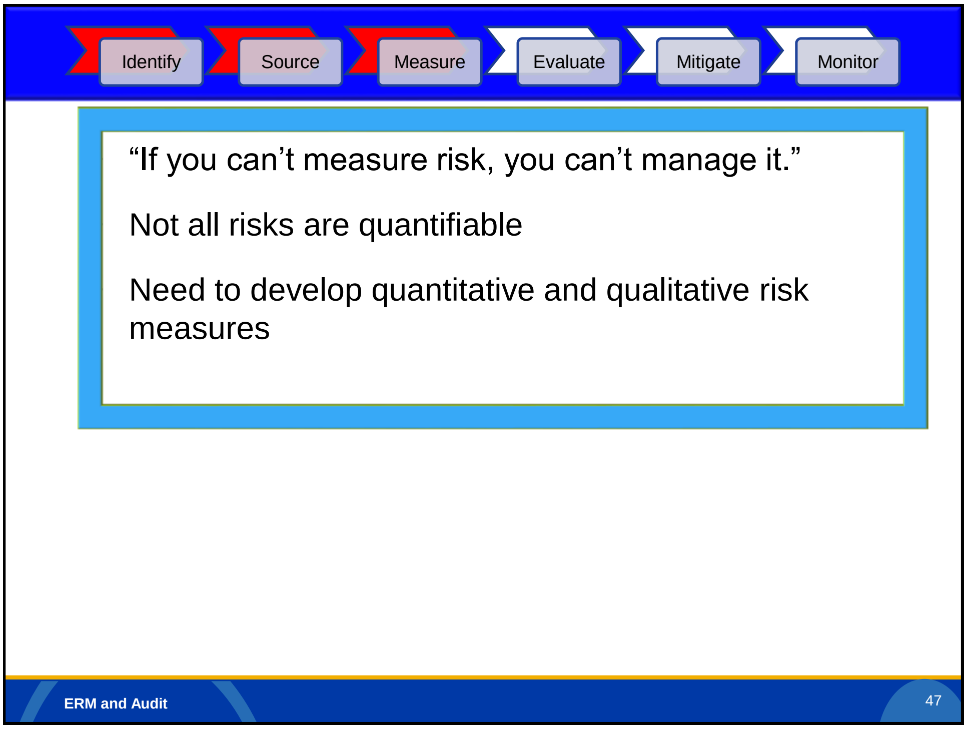
Identify | Source | Measure | Evaluate | Mitigate | Monitor

Priority risks are traced to their root causes

Once management understands the drivers of risk, they can design risk metrics and proactive risk responses at the source

ERM and Audit

46

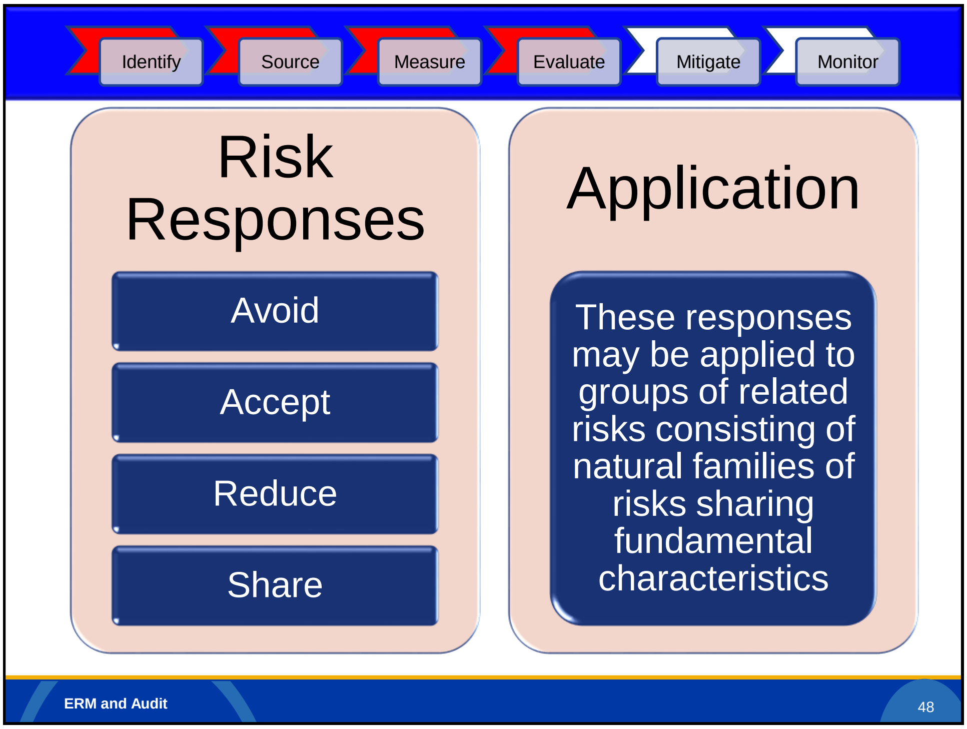


Identify Source Measure Evaluate Mitigate Monitor

"If you can't measure risk, you can't manage it."

Not all risks are quantifiable

Need to develop quantitative and qualitative risk measures



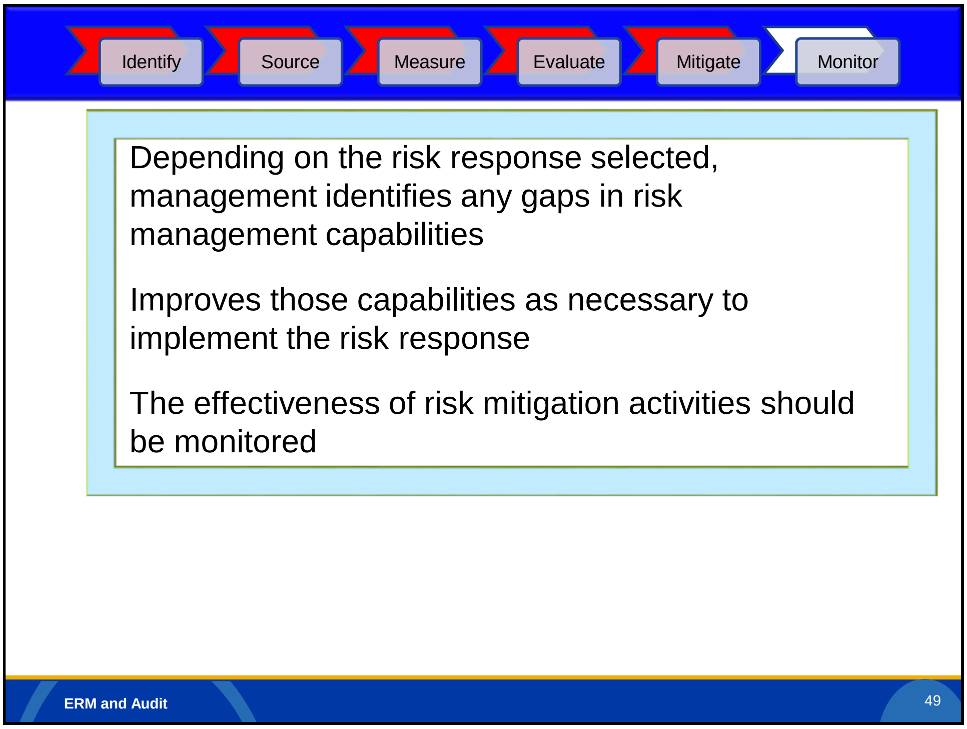
Identify Source Measure Evaluate Mitigate Monitor

Risk Responses

- Avoid
- Accept
- Reduce
- Share

Application

These responses may be applied to groups of related risks consisting of natural families of risks sharing fundamental characteristics



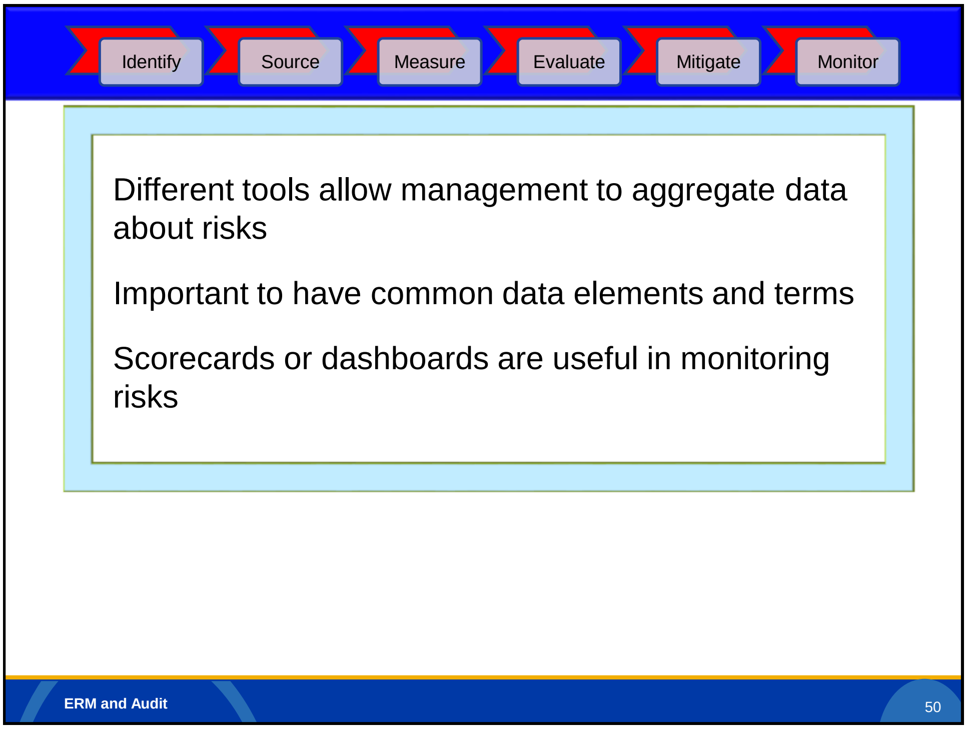
Identify Source Measure Evaluate Mitigate Monitor

Depending on the risk response selected, management identifies any gaps in risk management capabilities

Improves those capabilities as necessary to implement the risk response

The effectiveness of risk mitigation activities should be monitored

ERM and Audit 49



Identify Source Measure Evaluate Mitigate Monitor

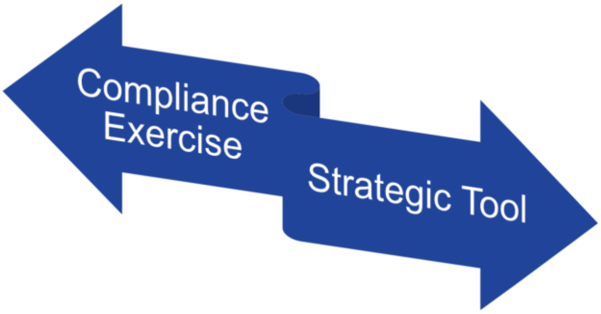
Different tools allow management to aggregate data about risks

Important to have common data elements and terms

Scorecards or dashboards are useful in monitoring risks

ERM and Audit 50

ERM in Your Company



Compliance Exercise

Strategic Tool

CEOs and BODs Realities

Events will happen: the fundamentals of your business will change

It is not what you know that counts - what you don’t know makes the difference between winning and losing

Your business is not an island

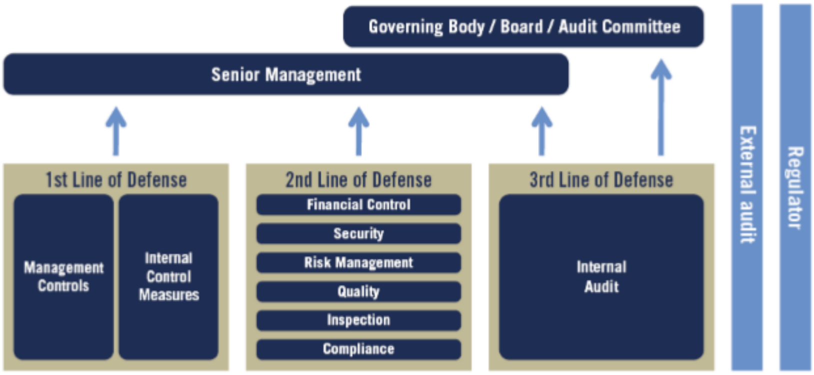
It is connected to many others and at some point, your company will be tested by a crisis

Management has trouble differentiating between risk management and risk oversight

The available frameworks may not help business leaders advance the dialogue

IIA Lines of Defense

The Three Lines of Defense Model



Governing Body / Board / Audit Committee

Senior Management

1st Line of Defense

Management Controls

Internal Control Measures

2nd Line of Defense

Financial Control

Security

Risk Management

Quality

Inspection

Compliance

3rd Line of Defense

Internal Audit

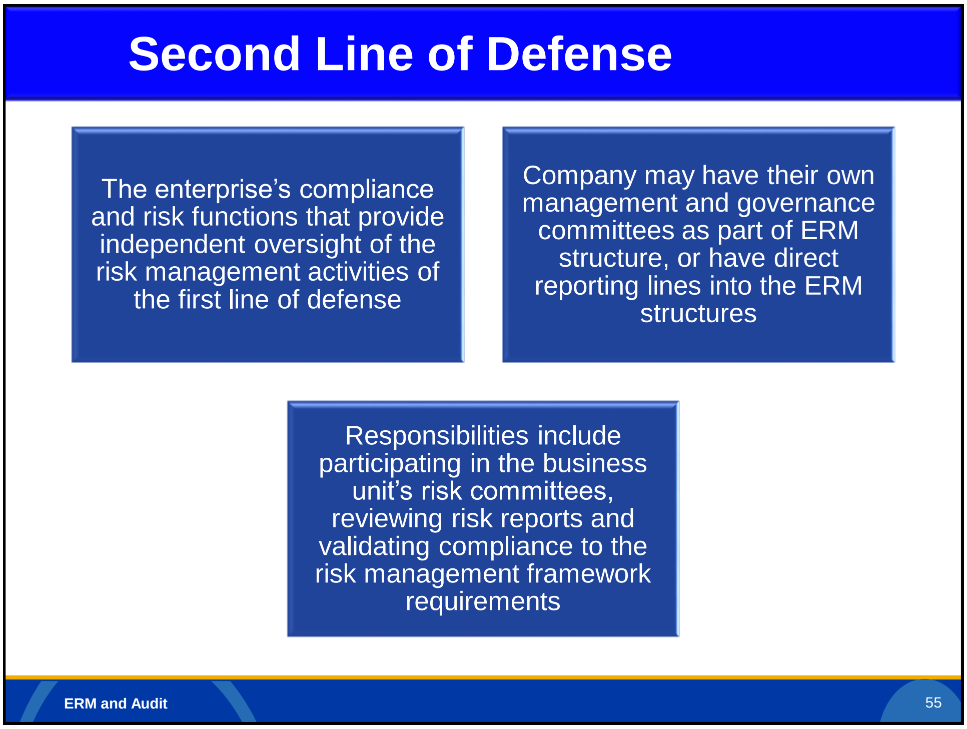
External audit

Regulator

Adapted from ECIIA/FERMA *Guidance on the 8th EU Company Law Directive, article 41*

First Line of Defense

- Front-line employees must understand their roles and responsibilities about processing transactions
- Employees must follow a systematic risk process and apply internal controls and other risk responses to treat the risks associated with those transactions



Second Line of Defense

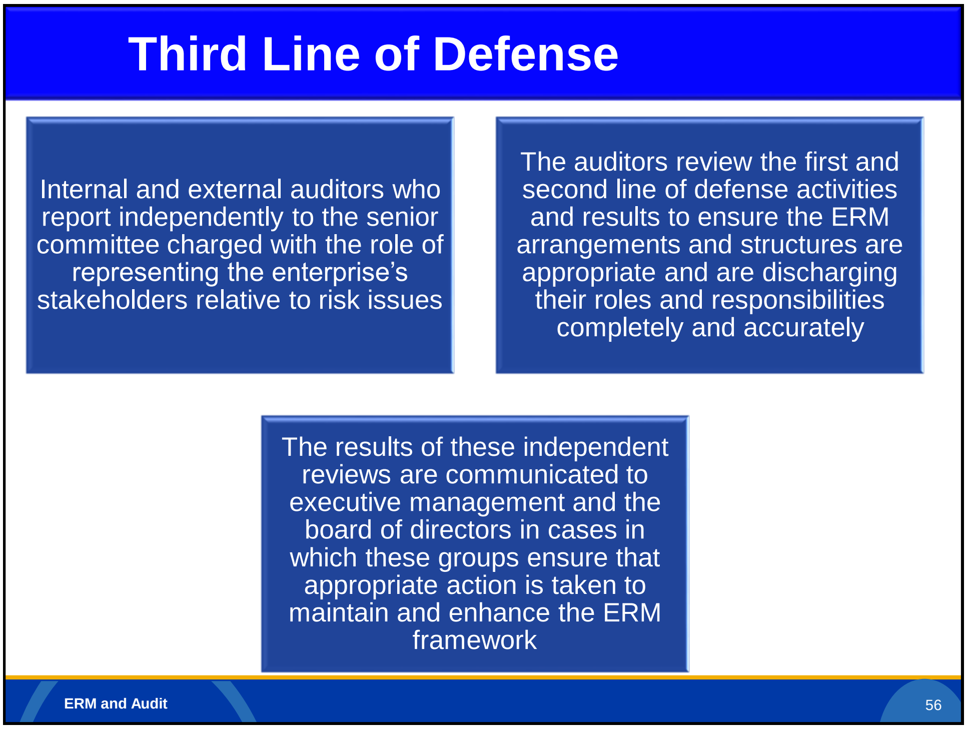
The enterprise’s compliance and risk functions that provide independent oversight of the risk management activities of the first line of defense

Company may have their own management and governance committees as part of ERM structure, or have direct reporting lines into the ERM structures

Responsibilities include participating in the business unit’s risk committees, reviewing risk reports and validating compliance to the risk management framework requirements

ERM and Audit

55



Third Line of Defense

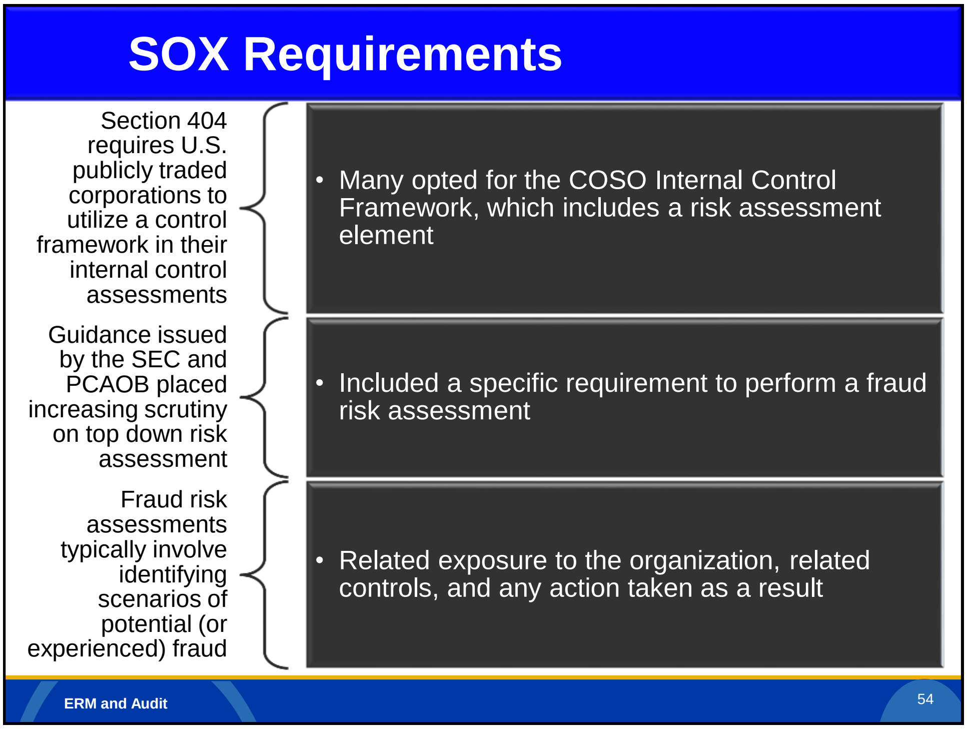
Internal and external auditors who report independently to the senior committee charged with the role of representing the enterprise’s stakeholders relative to risk issues

The auditors review the first and second line of defense activities and results to ensure the ERM arrangements and structures are appropriate and are discharging their roles and responsibilities completely and accurately

The results of these independent reviews are communicated to executive management and the board of directors in cases in which these groups ensure that appropriate action is taken to maintain and enhance the ERM framework

ERM and Audit

56



SOX Requirements

Section 404 requires U.S. publicly traded corporations to utilize a control framework in their internal control assessments

- Many opted for the COSO Internal Control Framework, which includes a risk assessment element

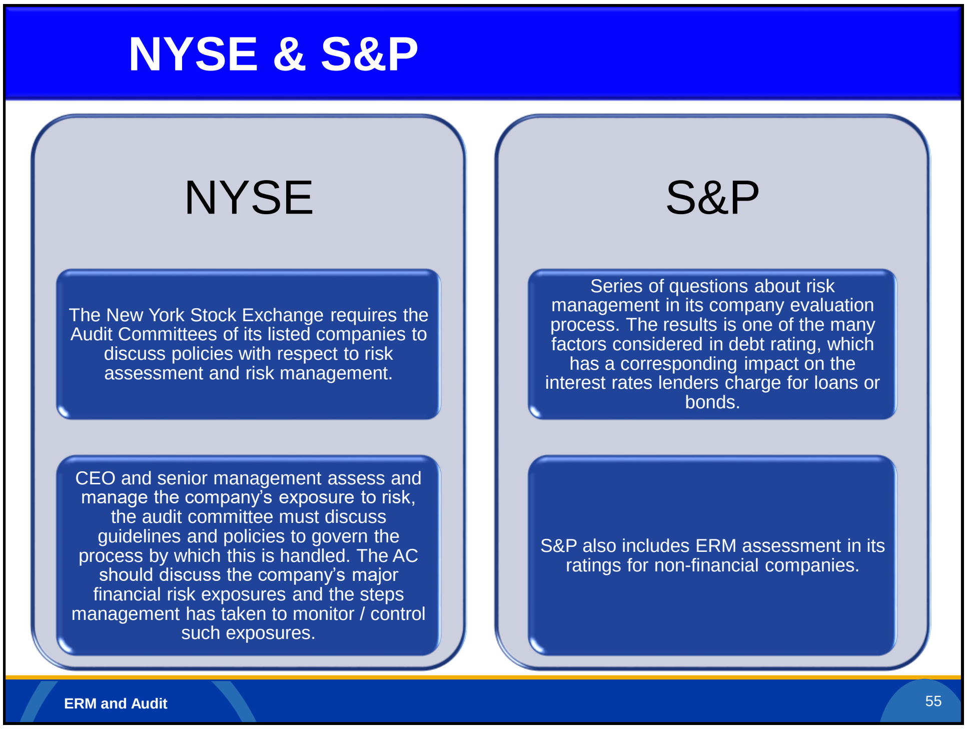
Guidance issued by the SEC and PCAOB placed increasing scrutiny on top down risk assessment

- Included a specific requirement to perform a fraud risk assessment

Fraud risk assessments typically involve identifying scenarios of potential (or experienced) fraud

- Related exposure to the organization, related controls, and any action taken as a result

ERM and Audit 54



NYSE & S&P

NYSE

The New York Stock Exchange requires the Audit Committees of its listed companies to discuss policies with respect to risk assessment and risk management.

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

S&P

Series of questions about risk management in its company evaluation process. The results is one of the many factors considered in debt rating, which has a corresponding impact on the interest rates lenders charge for loans or bonds.

S&P also includes ERM assessment in its ratings for non-financial companies.

ERM and Audit 55

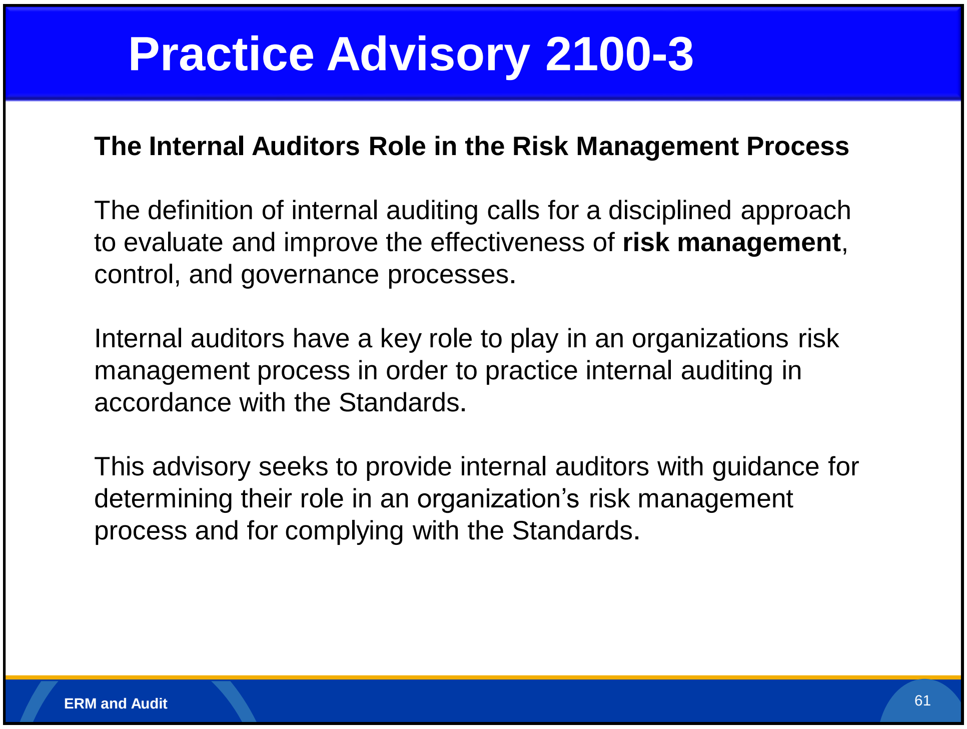
Agenda

- Definitions and Processes
- Risks
- ➡ Audit & ERM
- Key Strategies
- Conclusions

Definition from The IIA

Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

The majority of internal auditors today have not received much training on formal risk assessment methods. The harsh truth is that the majority of internal auditors today have received very little training on how to complete formal risk assessments on value creation and preservation objectives that use the type of methods promoted by the world’s global risk management standard, ISO 31000



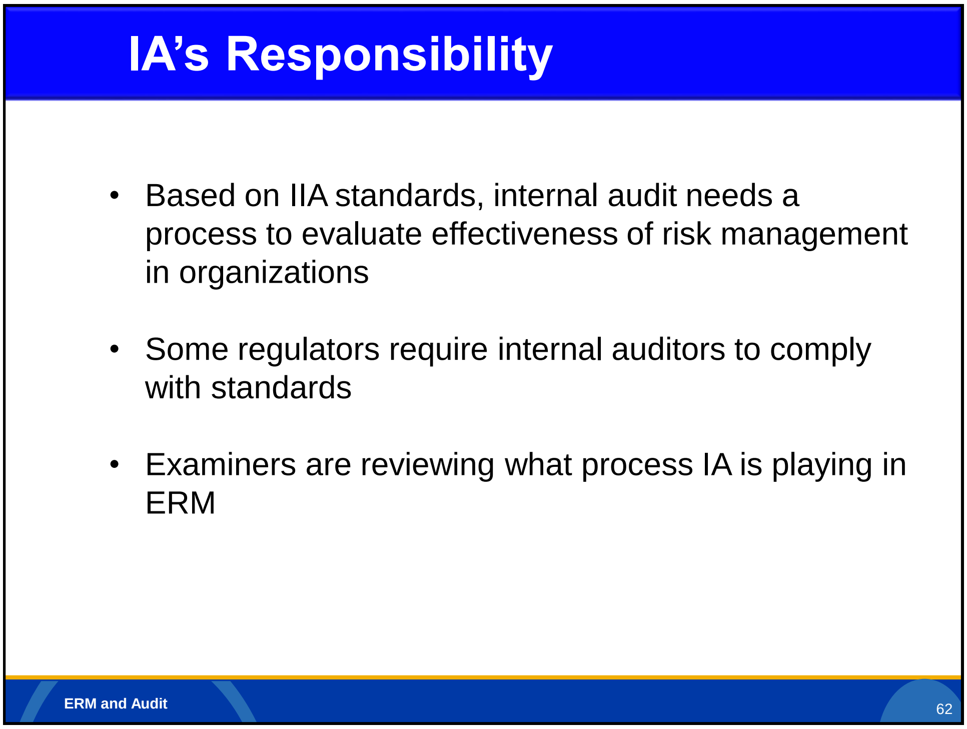
Practice Advisory 2100-3

The Internal Auditors Role in the Risk Management Process

The definition of internal auditing calls for a disciplined approach to evaluate and improve the effectiveness of **risk management**, control, and governance processes.

Internal auditors have a key role to play in an organizations risk management process in order to practice internal auditing in accordance with the Standards.

This advisory seeks to provide internal auditors with guidance for determining their role in an organization’s risk management process and for complying with the Standards.



IA’s Responsibility

- Based on IIA standards, internal audit needs a process to evaluate effectiveness of risk management in organizations
- Some regulators require internal auditors to comply with standards
- Examiners are reviewing what process IA is playing in ERM

IA Adds Value By:

- Reviewing critical control systems and risk management processes.
- Performing an effectiveness review of management's risk assessments and the internal controls.
- Providing advice in the design and improvement of control systems and risk mitigation strategies.
- Implementing a risk-based approach to planning and executing the internal audit process.
- Ensuring that internal auditing's resources are directed at those areas most important to the organization.
- Challenging the basis of management's risk assessments and evaluating the adequacy and effectiveness of risk treatment strategies.

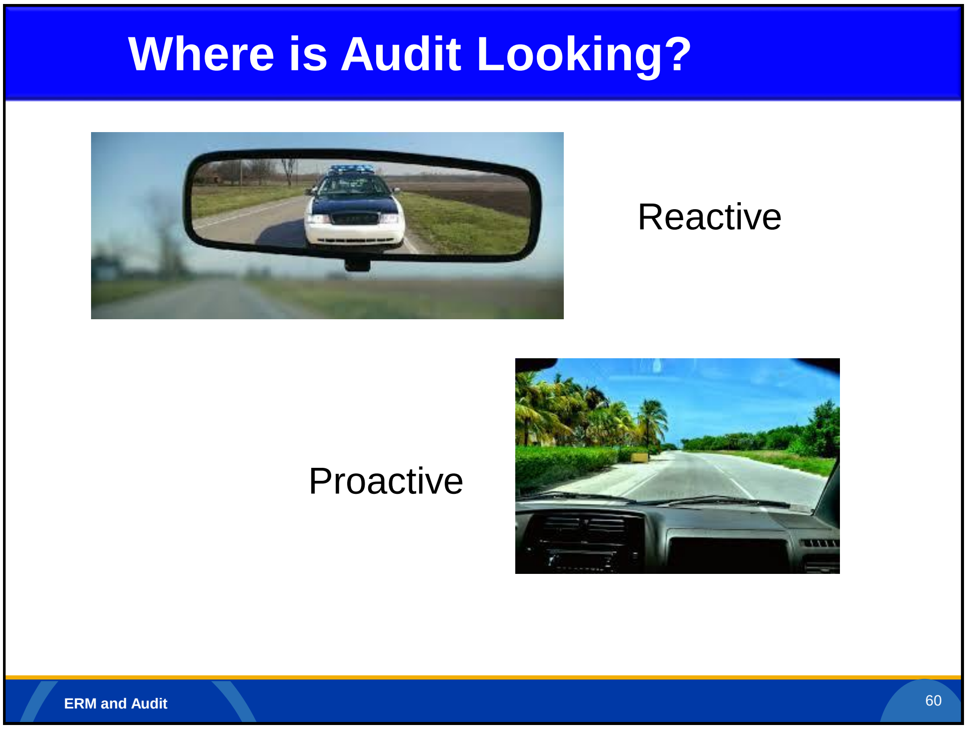
2016 Study

AICPA and North Carolina State University

Only 30 per cent of the organizations surveyed have boards that 'mostly' or 'extensively' review the top risk exposures facing the organization when the board discusses the organization's strategic plan.

Investors are not only demanding more details on the organization's long-term value creation plans, they want more and better information on the risks that threaten the achievement of those plans and they want board review of those risks.

In large organizations with revenues in excess of $1 billion, 87% of respondents want more information from senior executives on risks impacting core growth strategies.

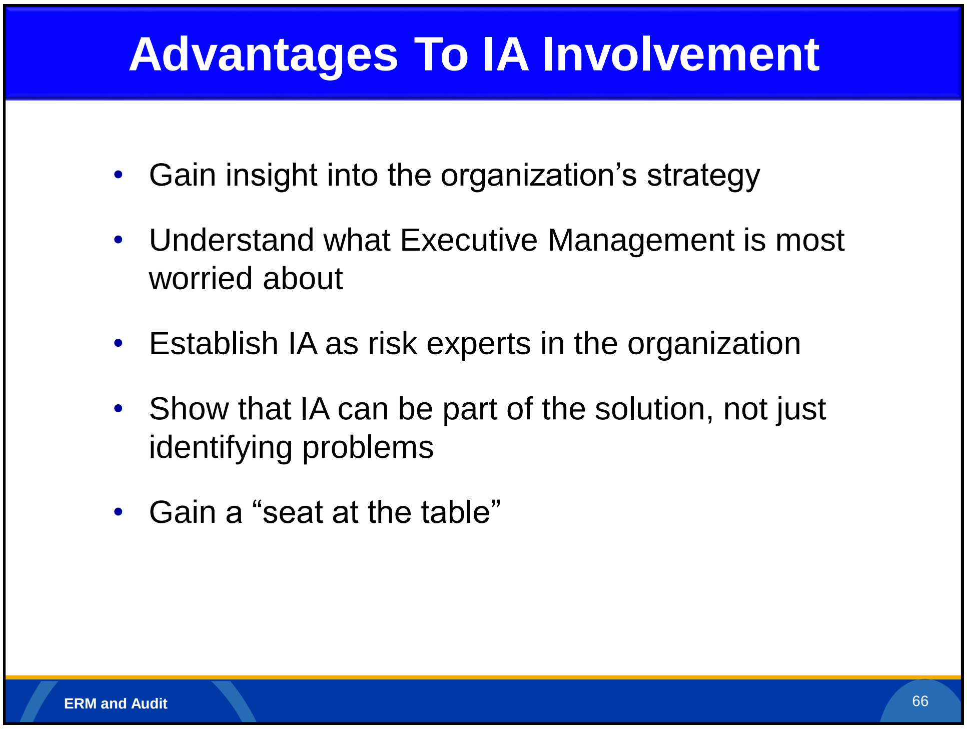


Where is Audit Looking?

Reactive

Proactive

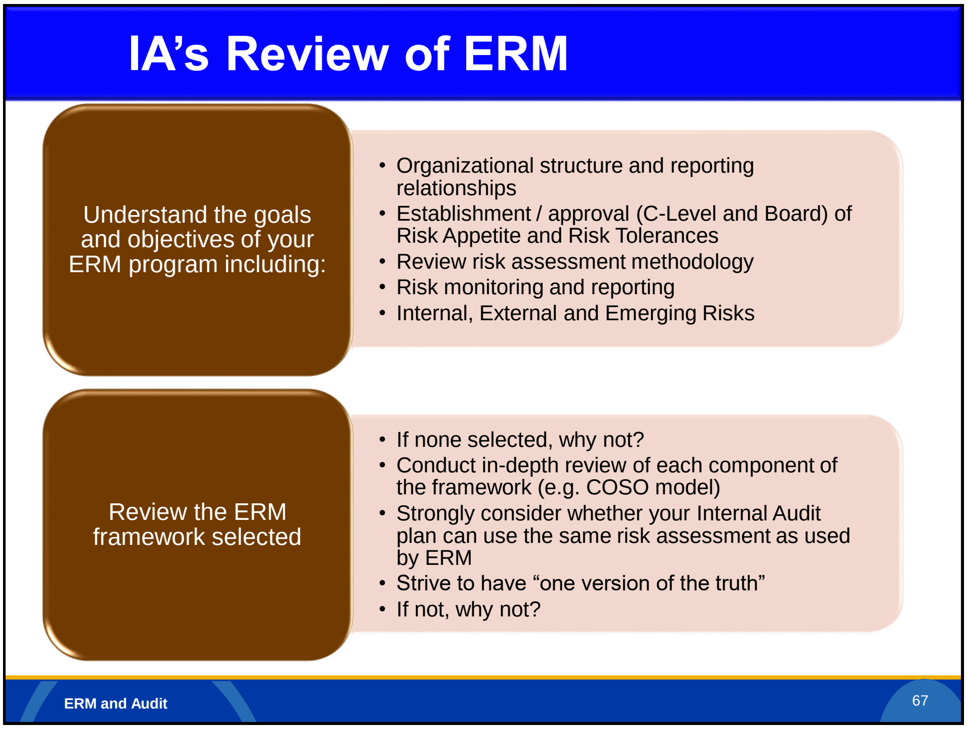
ERM and Audit 60



Advantages To IA Involvement

- Gain insight into the organization’s strategy
- Understand what Executive Management is most worried about
- Establish IA as risk experts in the organization
- Show that IA can be part of the solution, not just identifying problems
- Gain a “seat at the table”

ERM and Audit 66



IA’s Review of ERM

Understand the goals and objectives of your ERM program including:

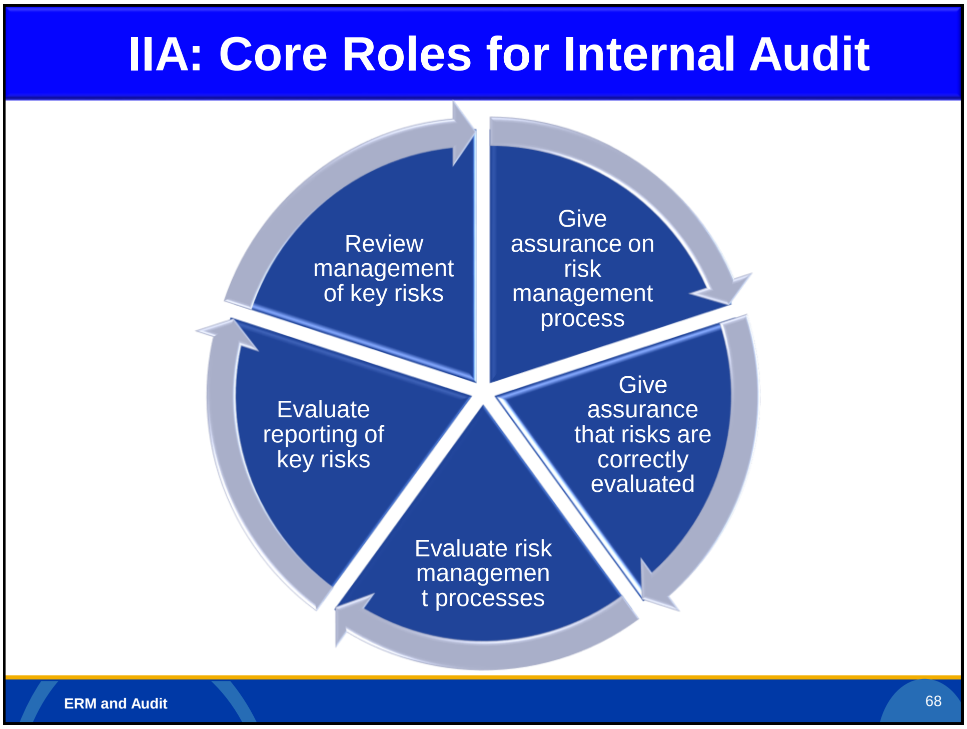
- Organizational structure and reporting relationships
- Establishment / approval (C-Level and Board) of Risk Appetite and Risk Tolerances
- Review risk assessment methodology
- Risk monitoring and reporting
- Internal, External and Emerging Risks

Review the ERM framework selected

- If none selected, why not?
- Conduct in-depth review of each component of the framework (e.g. COSO model)
- Strongly consider whether your Internal Audit plan can use the same risk assessment as used by ERM
- Strive to have “one version of the truth”
- If not, why not?

ERM and Audit

67



IIA: Core Roles for Internal Audit

Review management of key risks

Give assurance on risk management process

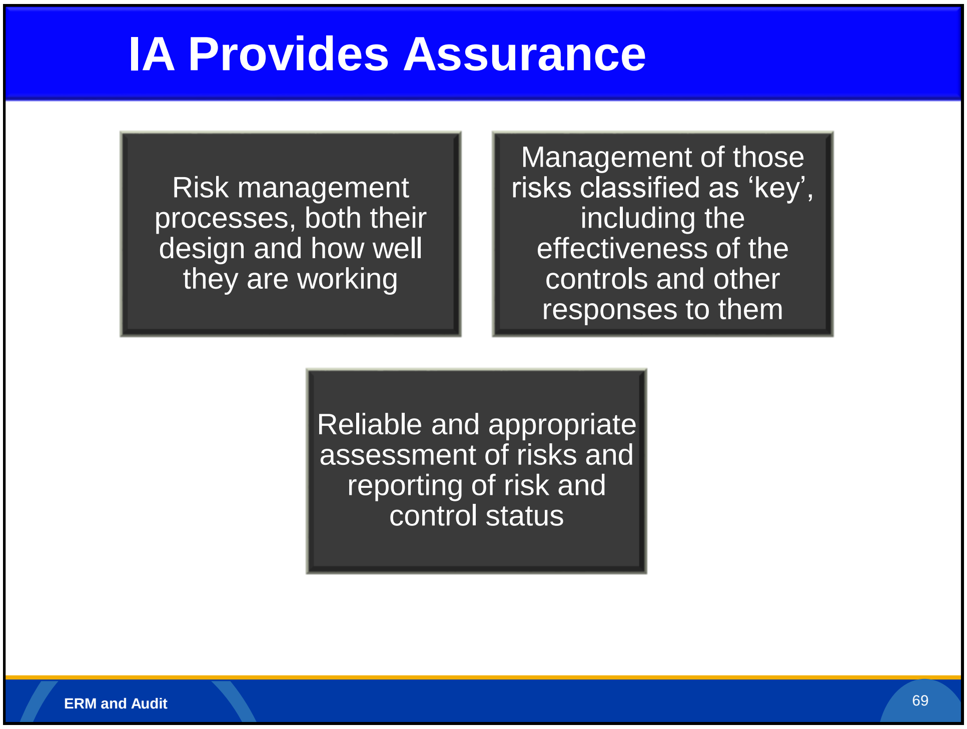
Give assurance that risks are correctly evaluated

Evaluate risk managemen t processes

Evaluate reporting of key risks

ERM and Audit

68

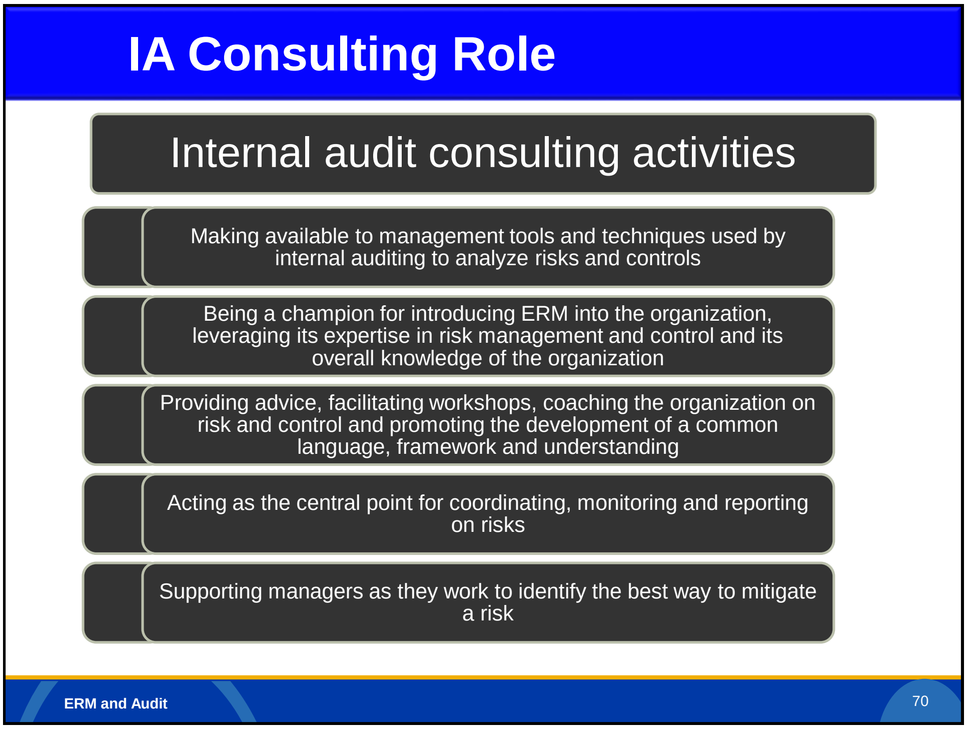


IA Provides Assurance

Risk management processes, both their design and how well they are working

Management of those risks classified as ‘key’, including the effectiveness of the controls and other responses to them

Reliable and appropriate assessment of risks and reporting of risk and control status

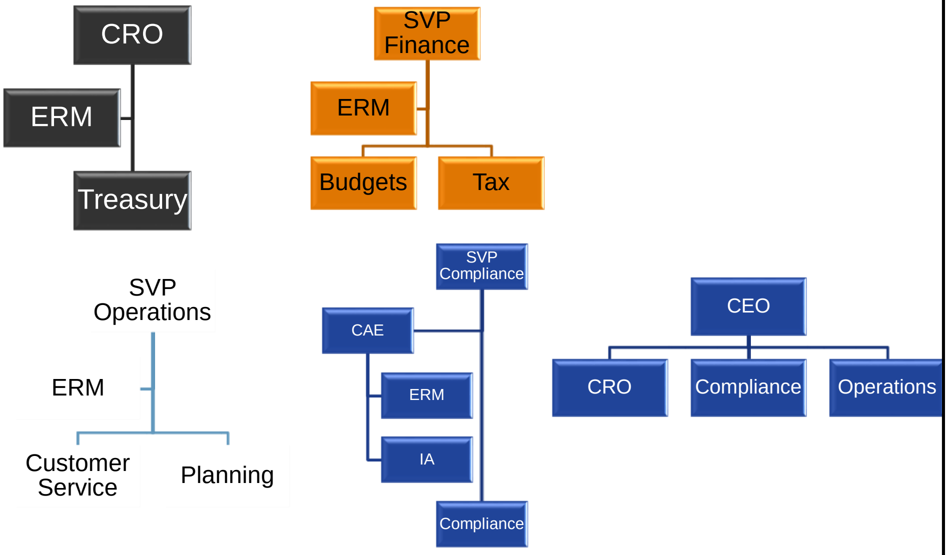


IA Consulting Role

Internal audit consulting activities

- Making available to management tools and techniques used by internal auditing to analyze risks and controls
- Being a champion for introducing ERM into the organization, leveraging its expertise in risk management and control and its overall knowledge of the organization
- Providing advice, facilitating workshops, coaching the organization on risk and control and promoting the development of a common language, framework and understanding
- Acting as the central point for coordinating, monitoring and reporting on risks
- Supporting managers as they work to identify the best way to mitigate a risk

Where is ERM Situated?



CRO

ERM

Treasury

SVP Finance

ERM

Budgets

Tax

SVP Operations

ERM

Customer Service

Planning

SVP Compliance

CAE

ERM

IA

Compliance

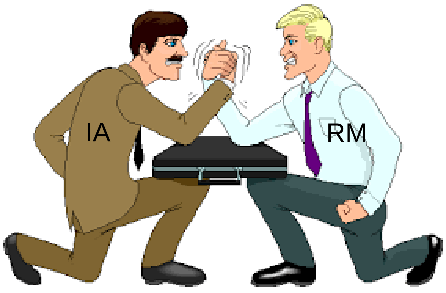
CEO

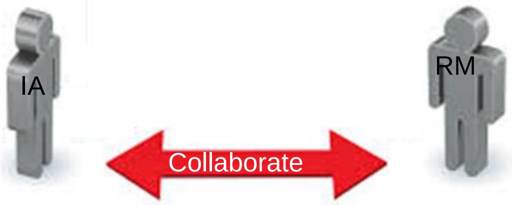
CRO

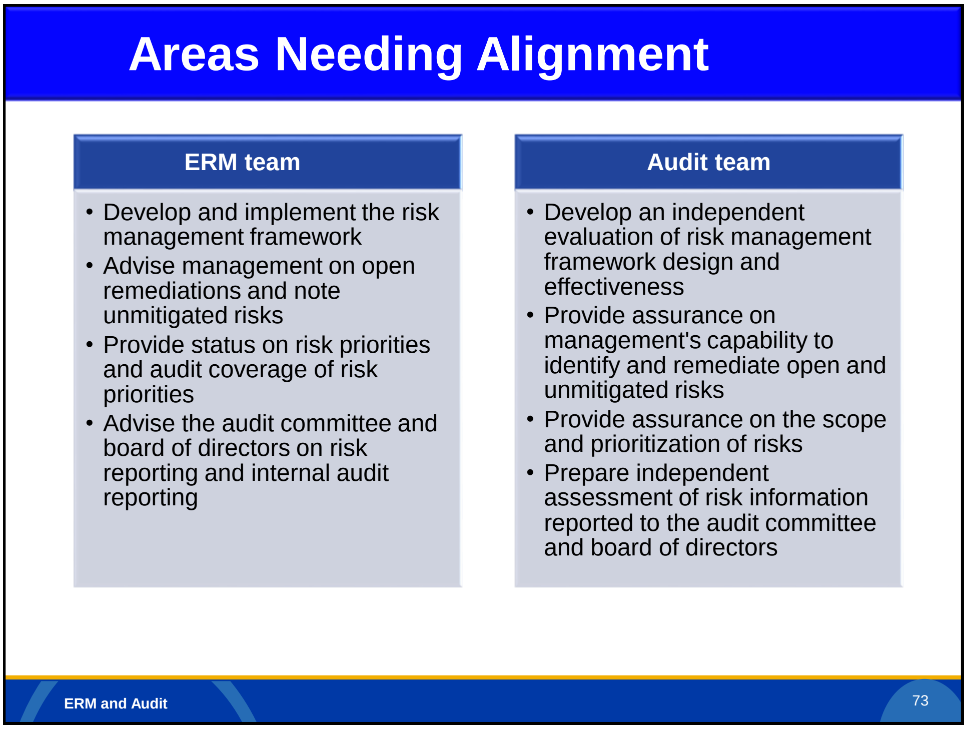
Compliance

Operations

IA and Risk Managers Aligned?







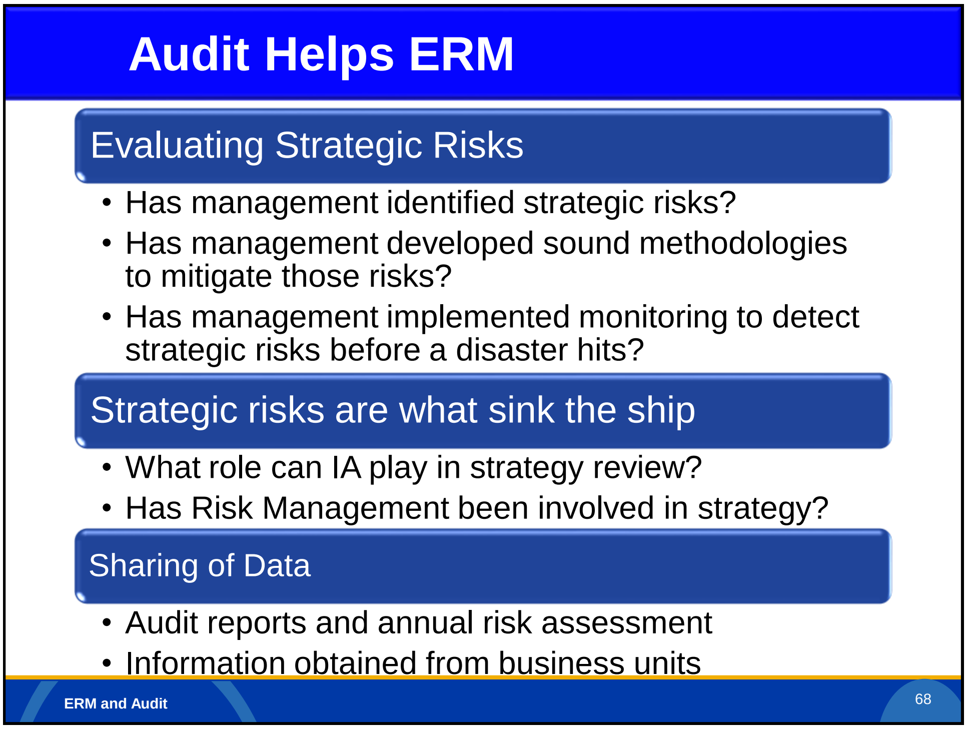
Areas Needing Alignment

ERM team

- Develop and implement the risk management framework
- Advise management on open remediations and note unmitigated risks
- Provide status on risk priorities and audit coverage of risk priorities
- Advise the audit committee and board of directors on risk reporting and internal audit reporting

Audit team

- Develop an independent evaluation of risk management framework design and effectiveness
- Provide assurance on management's capability to identify and remediate open and unmitigated risks
- Provide assurance on the scope and prioritization of risks
- Prepare independent assessment of risk information reported to the audit committee and board of directors



Audit Helps ERM

Evaluating Strategic Risks

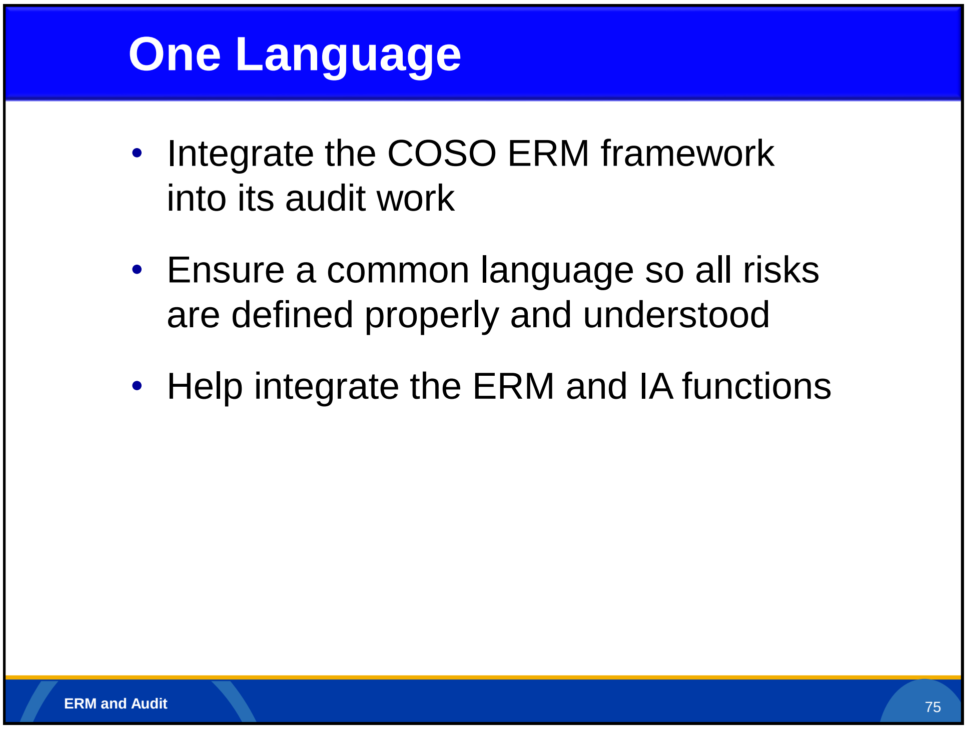
- Has management identified strategic risks?
- Has management developed sound methodologies to mitigate those risks?
- Has management implemented monitoring to detect strategic risks before a disaster hits?

Strategic risks are what sink the ship

- What role can IA play in strategy review?
- Has Risk Management been involved in strategy?

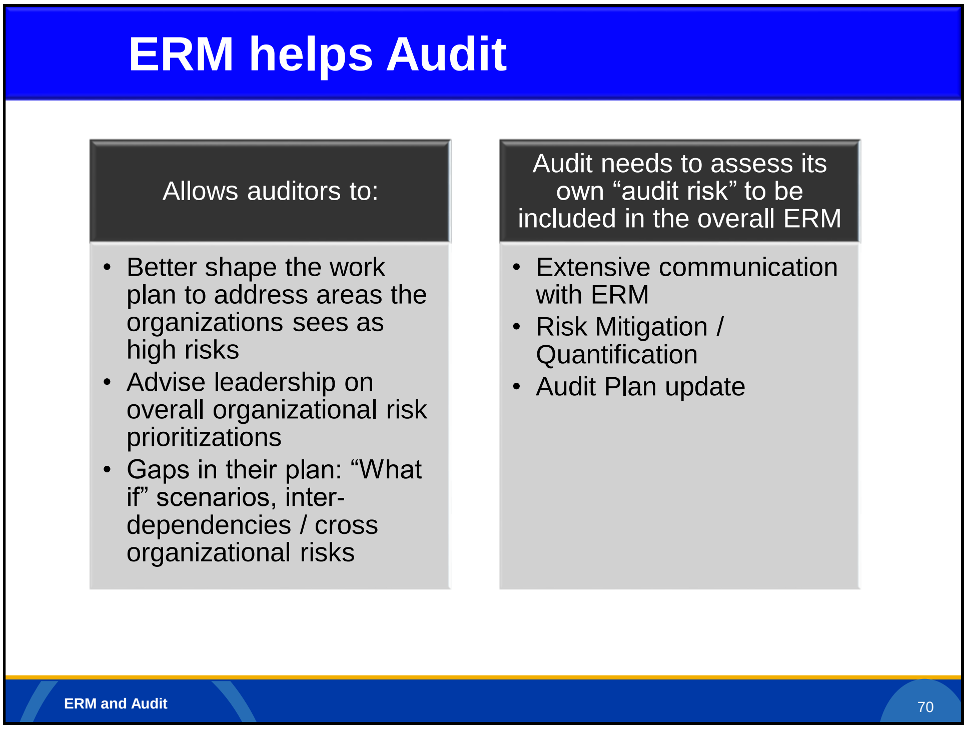
Sharing of Data

- Audit reports and annual risk assessment
- Information obtained from business units



One Language

- Integrate the COSO ERM framework into its audit work
- Ensure a common language so all risks are defined properly and understood
- Help integrate the ERM and IA functions



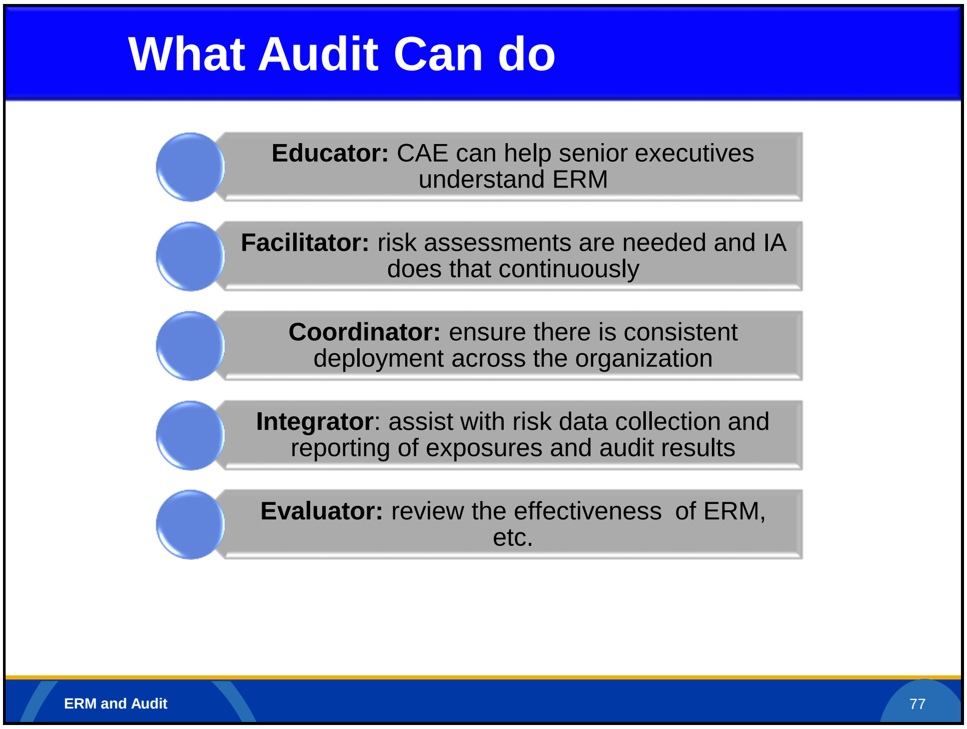
ERM helps Audit

Allows auditors to:

- Better shape the work plan to address areas the organizations sees as high risks
- Advise leadership on overall organizational risk prioritizations
- Gaps in their plan: “What if” scenarios, inter-dependencies / cross organizational risks

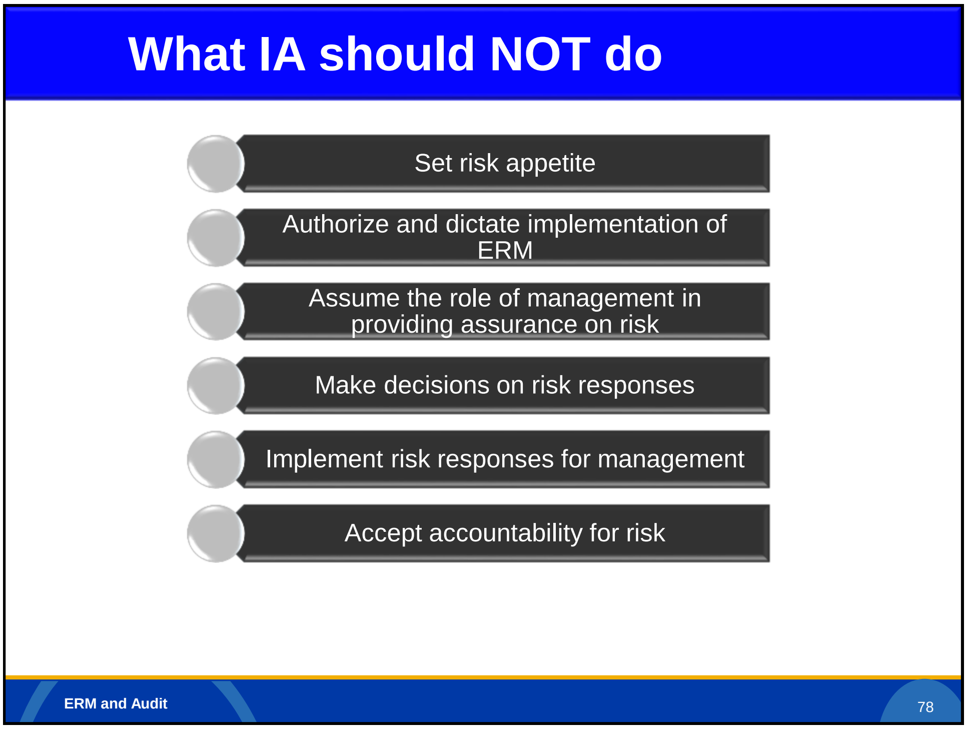
Audit needs to assess its own “audit risk” to be included in the overall ERM

- Extensive communication with ERM
- Risk Mitigation / Quantification
- Audit Plan update



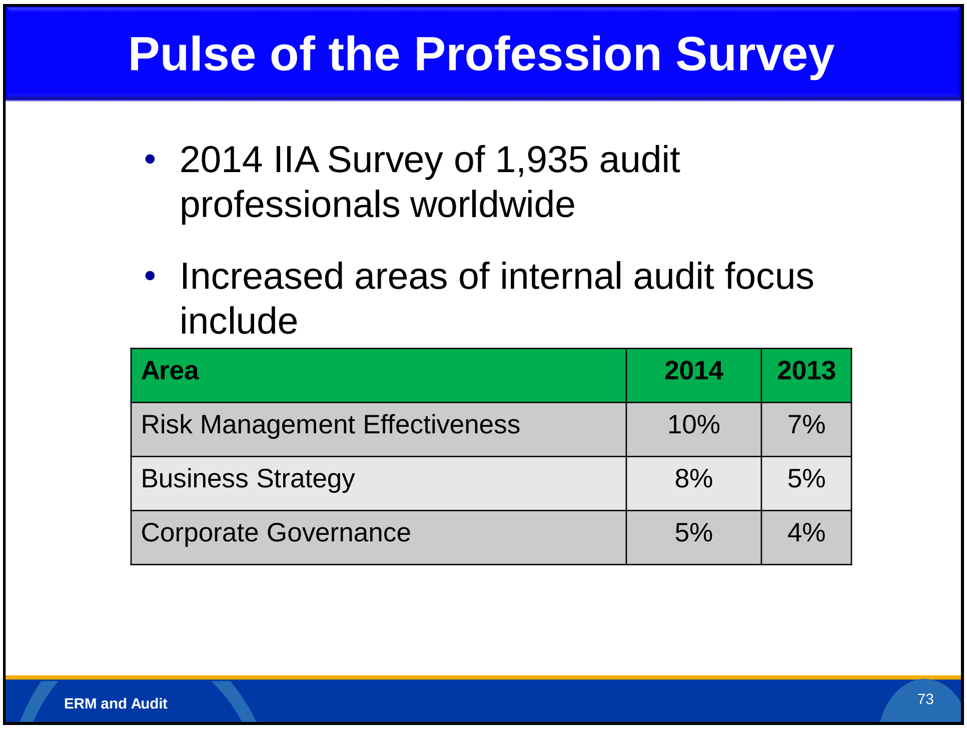
What Audit Can do

- **Educator:** CAE can help senior executives understand ERM
- **Facilitator:** risk assessments are needed and IA does that continuously
- **Coordinator:** ensure there is consistent deployment across the organization
- **Integrator**: assist with risk data collection and reporting of exposures and audit results
- **Evaluator:** review the effectiveness of ERM, etc.



What IA should NOT do

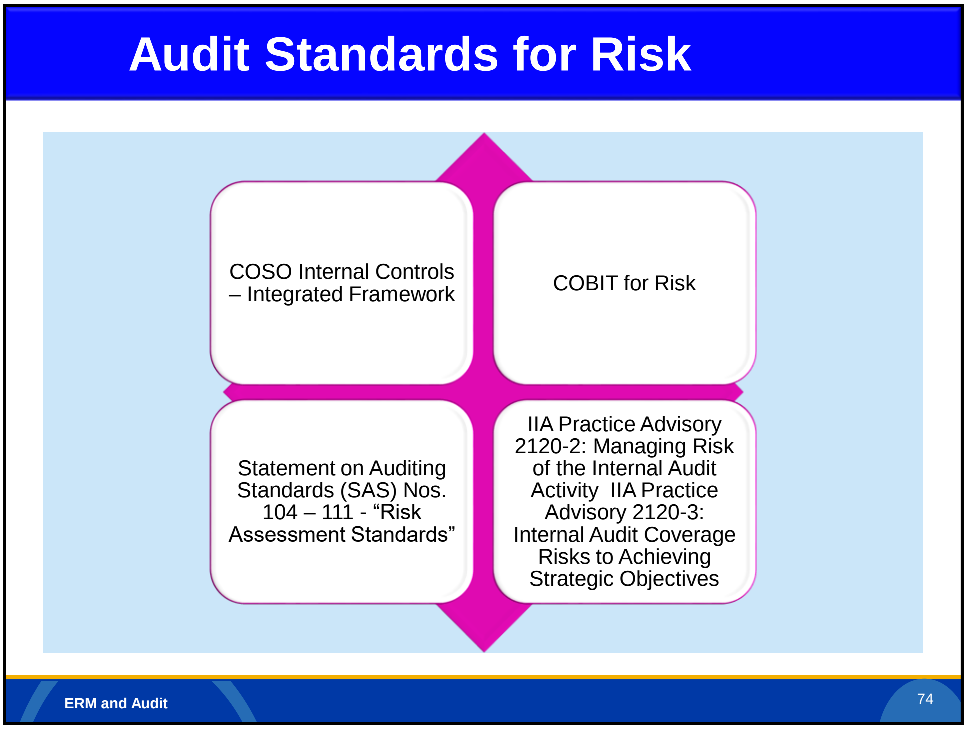
- Set risk appetite
- Authorize and dictate implementation of ERM
- Assume the role of management in providing assurance on risk
- Make decisions on risk responses
- Implement risk responses for management
- Accept accountability for risk



Pulse of the Profession Survey

- 2014 IIA Survey of 1,935 audit professionals worldwide
- Increased areas of internal audit focus include

Area	2014	2013
Risk Management Effectiveness	10%	7%
Business Strategy	8%	5%
Corporate Governance	5%	4%



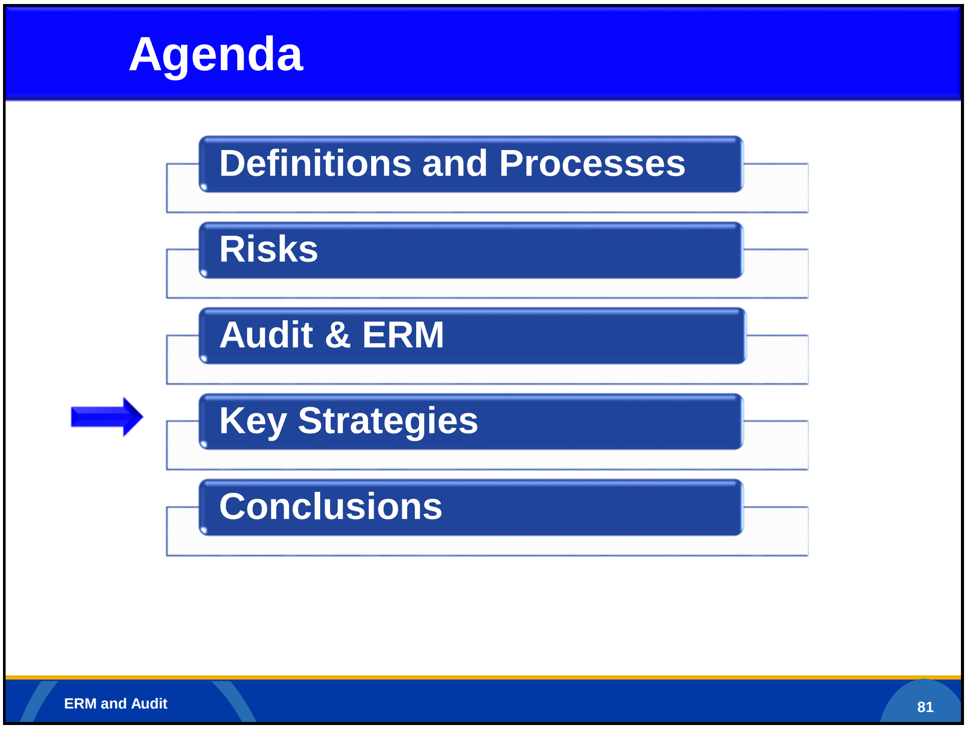
Audit Standards for Risk

COSO Internal Controls – Integrated Framework

COBIT for Risk

Statement on Auditing Standards (SAS) Nos. 104 – 111 - "Risk Assessment Standards"

IIA Practice Advisory 2120-2: Managing Risk of the Internal Audit Activity IIA Practice Advisory 2120-3: Internal Audit Coverage Risks to Achieving Strategic Objectives

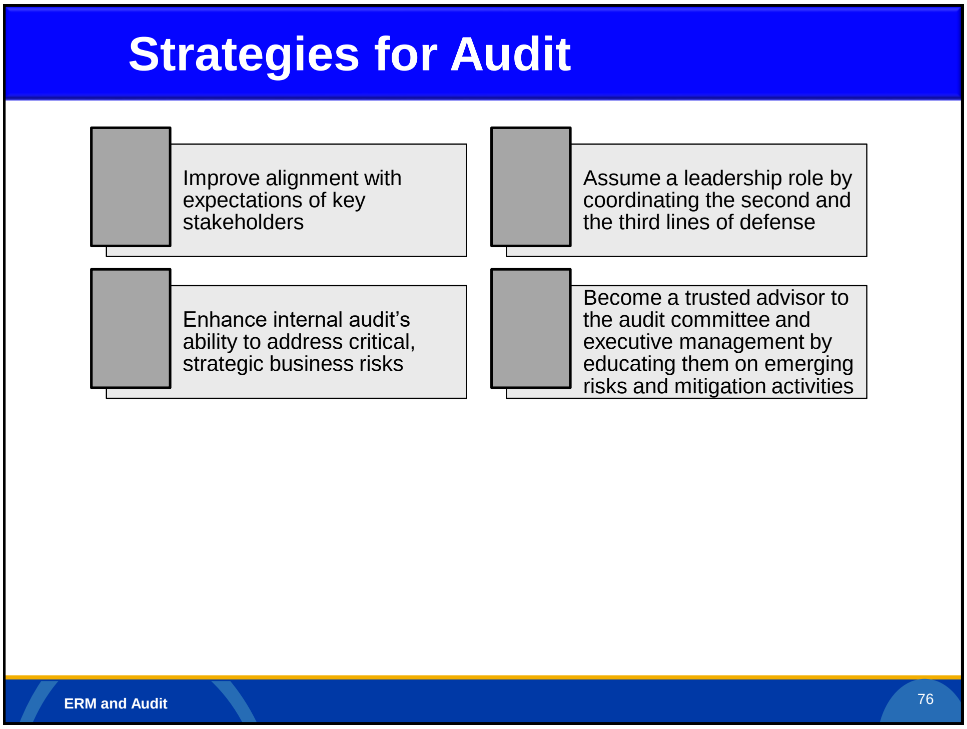


Agenda

- Definitions and Processes
- Risks
- Audit & ERM
- ➡ Key Strategies
- Conclusions

ERM and Audit

81

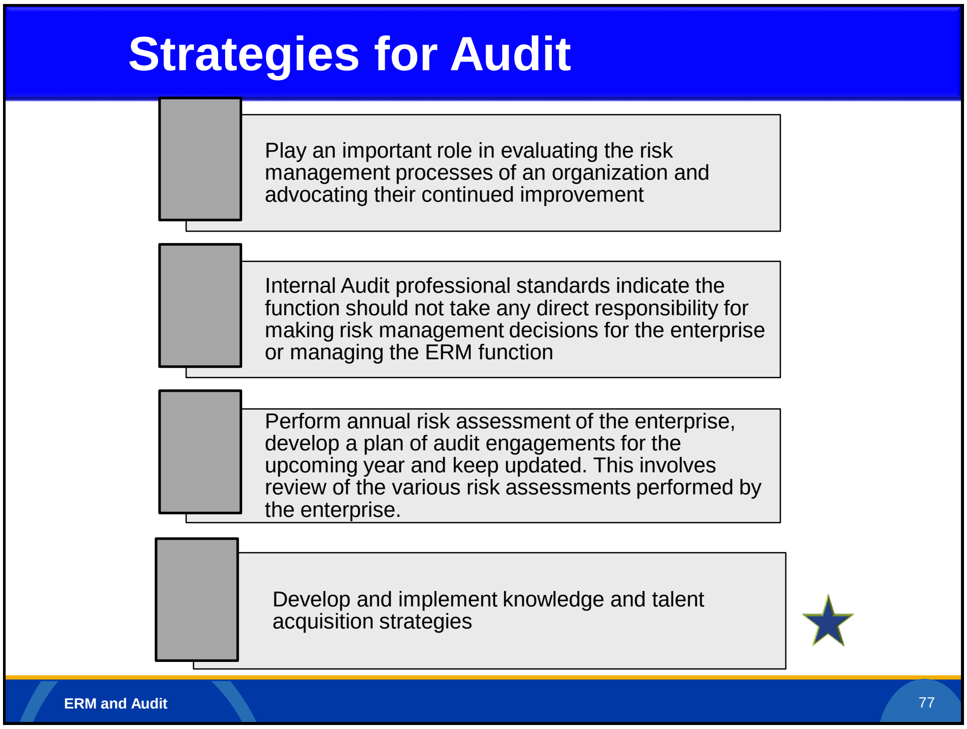


Strategies for Audit

- Improve alignment with expectations of key stakeholders
- Assume a leadership role by coordinating the second and the third lines of defense
- Enhance internal audit's ability to address critical, strategic business risks
- Become a trusted advisor to the audit committee and executive management by educating them on emerging risks and mitigation activities

ERM and Audit

76



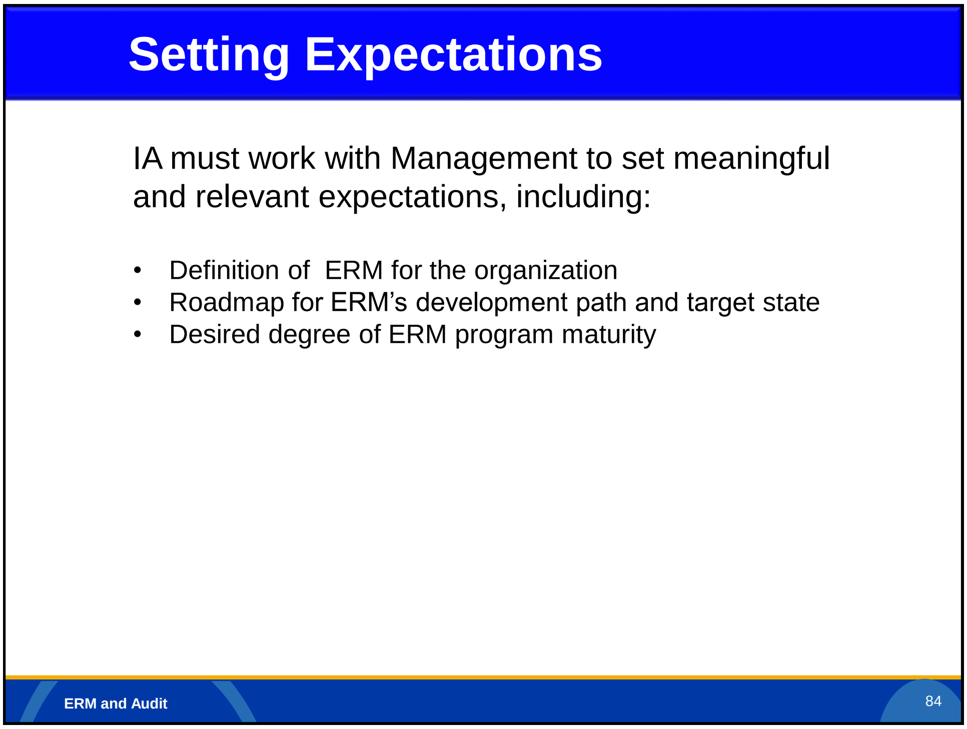
Strategies for Audit

Play an important role in evaluating the risk management processes of an organization and advocating their continued improvement

Internal Audit professional standards indicate the function should not take any direct responsibility for making risk management decisions for the enterprise or managing the ERM function

Perform annual risk assessment of the enterprise, develop a plan of audit engagements for the upcoming year and keep updated. This involves review of the various risk assessments performed by the enterprise.

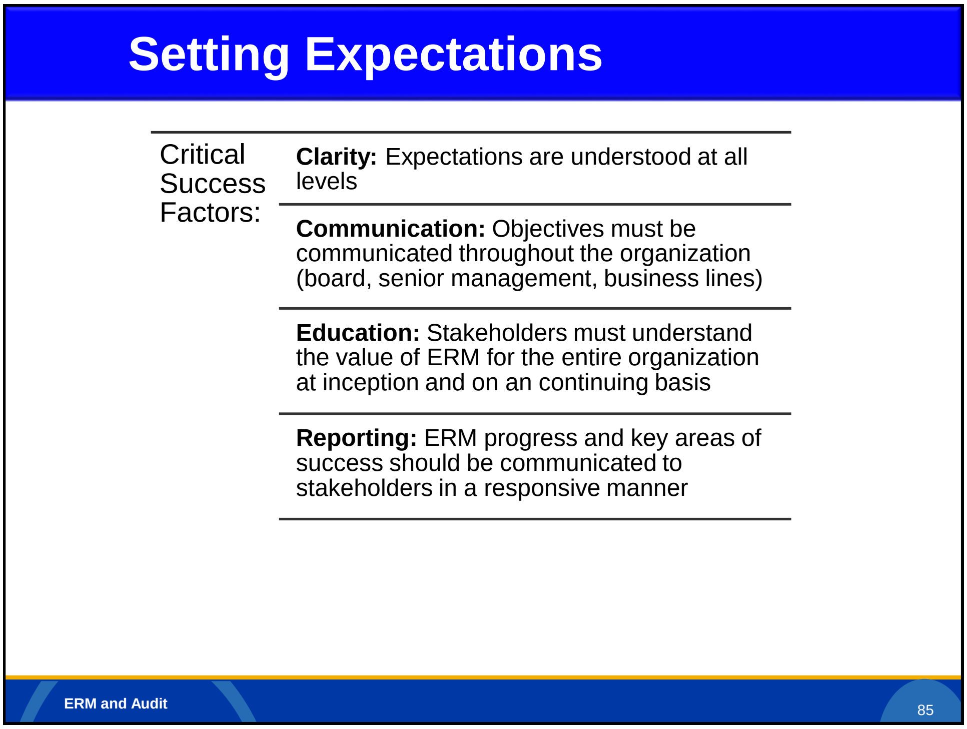
Develop and implement knowledge and talent acquisition strategies ★



Setting Expectations

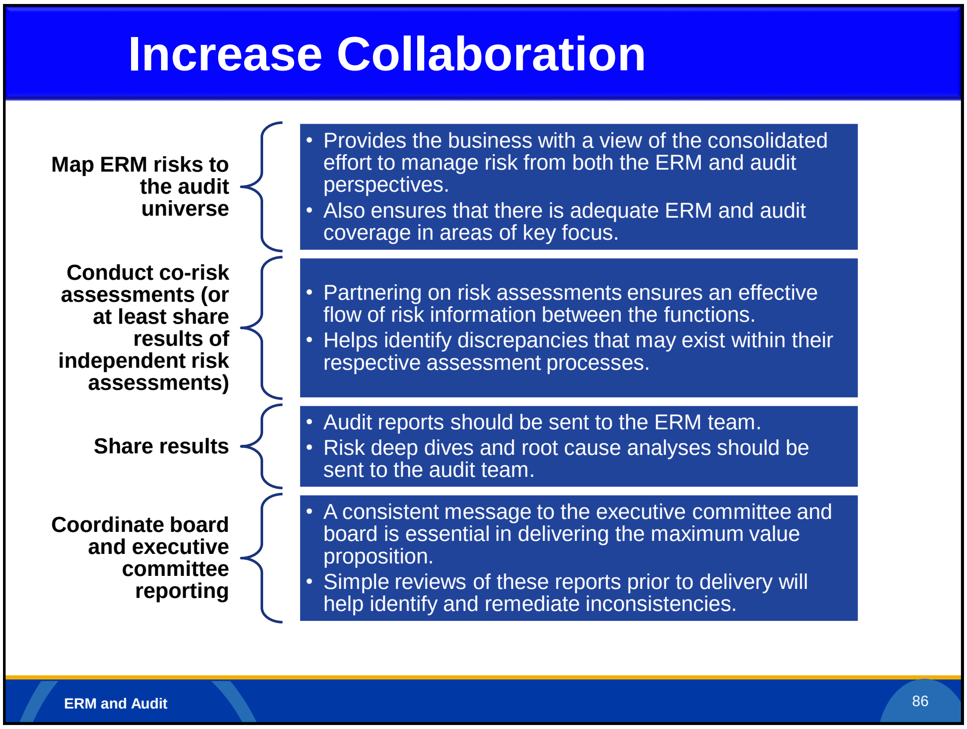
IA must work with Management to set meaningful and relevant expectations, including:

- Definition of ERM for the organization
- Roadmap for ERM’s development path and target state
- Desired degree of ERM program maturity



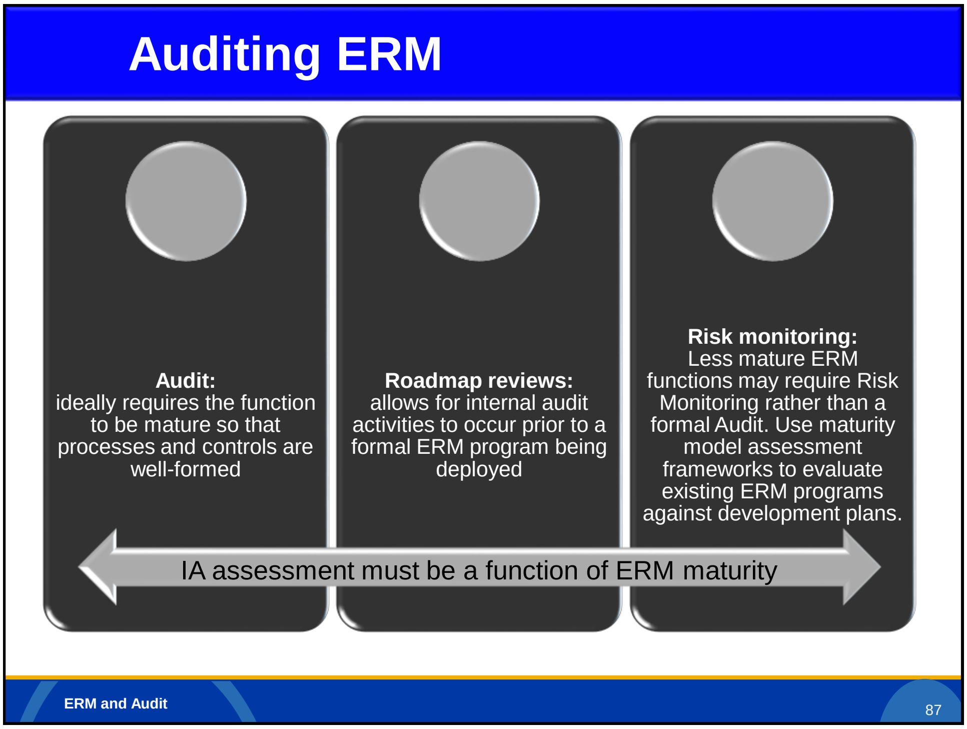
Setting Expectations

Critical Success Factors:	**Clarity:** Expectations are understood at all levels
	Communication: Objectives must be communicated throughout the organization (board, senior management, business lines)
	Education: Stakeholders must understand the value of ERM for the entire organization at inception and on an continuing basis
	Reporting: ERM progress and key areas of success should be communicated to stakeholders in a responsive manner



Increase Collaboration

Map ERM risks to the audit universe	• Provides the business with a view of the consolidated effort to manage risk from both the ERM and audit perspectives. • Also ensures that there is adequate ERM and audit coverage in areas of key focus.
Conduct co-risk assessments (or at least share results of independent risk assessments)	• Partnering on risk assessments ensures an effective flow of risk information between the functions. • Helps identify discrepancies that may exist within their respective assessment processes.
Share results	• Audit reports should be sent to the ERM team. • Risk deep dives and root cause analyses should be sent to the audit team.
Coordinate board and executive committee reporting	• A consistent message to the executive committee and board is essential in delivering the maximum value proposition. • Simple reviews of these reports prior to delivery will help identify and remediate inconsistencies.



Auditing ERM

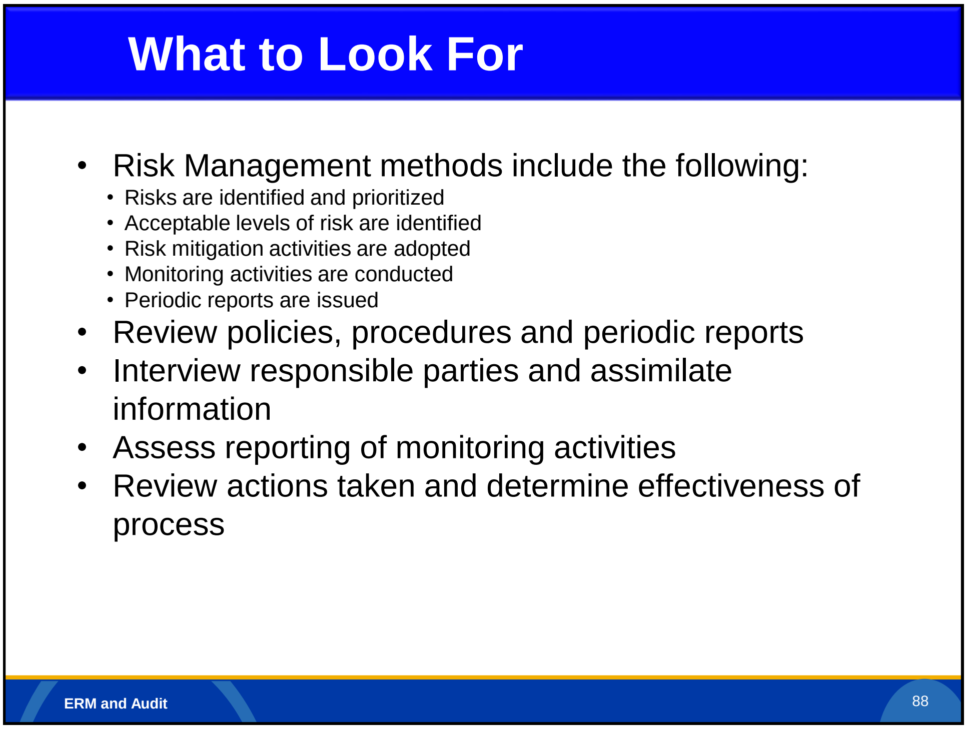
Audit:
ideally requires the function to be mature so that processes and controls are well-formed

Roadmap reviews:
allows for internal audit activities to occur prior to a formal ERM program being deployed

Risk monitoring:
Less mature ERM functions may require Risk Monitoring rather than a formal Audit. Use maturity model assessment frameworks to evaluate existing ERM programs against development plans.

IA assessment must be a function of ERM maturity

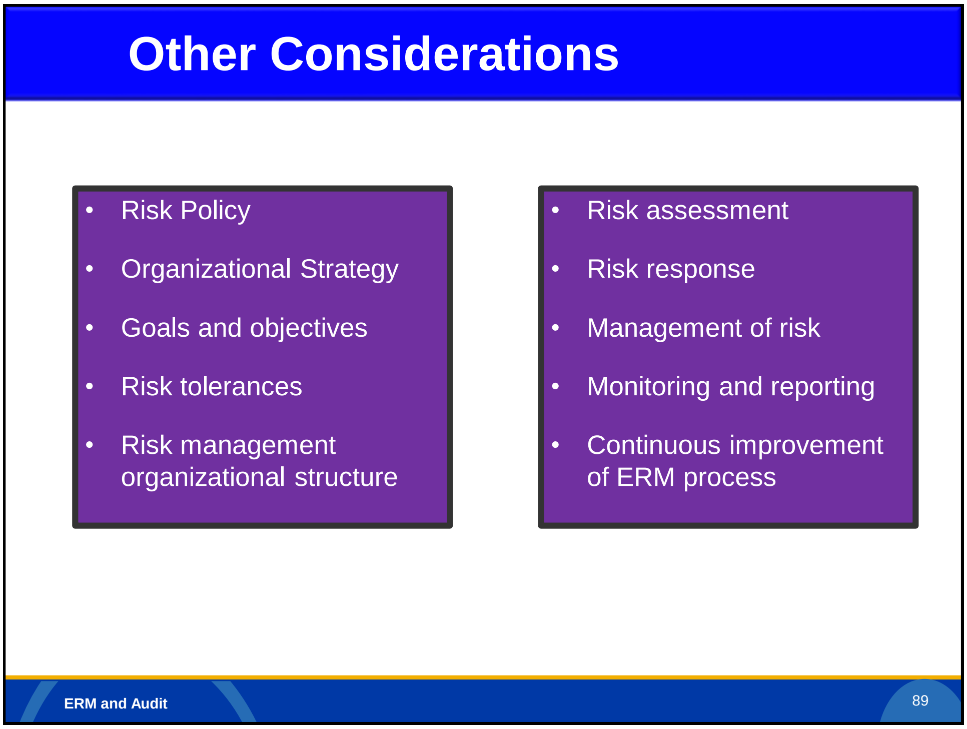
ERM and Audit 87



What to Look For

- Risk Management methods include the following:
  - Risks are identified and prioritized
  - Acceptable levels of risk are identified
  - Risk mitigation activities are adopted
  - Monitoring activities are conducted
  - Periodic reports are issued
- Review policies, procedures and periodic reports
- Interview responsible parties and assimilate information
- Assess reporting of monitoring activities
- Review actions taken and determine effectiveness of process

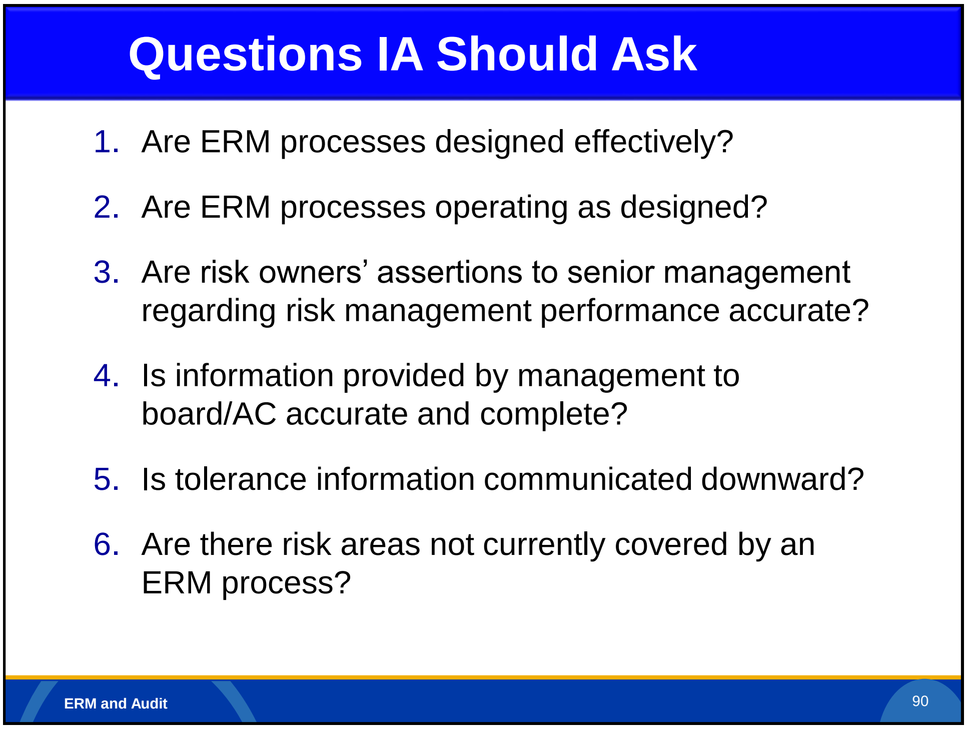
ERM and Audit 88



Other Considerations

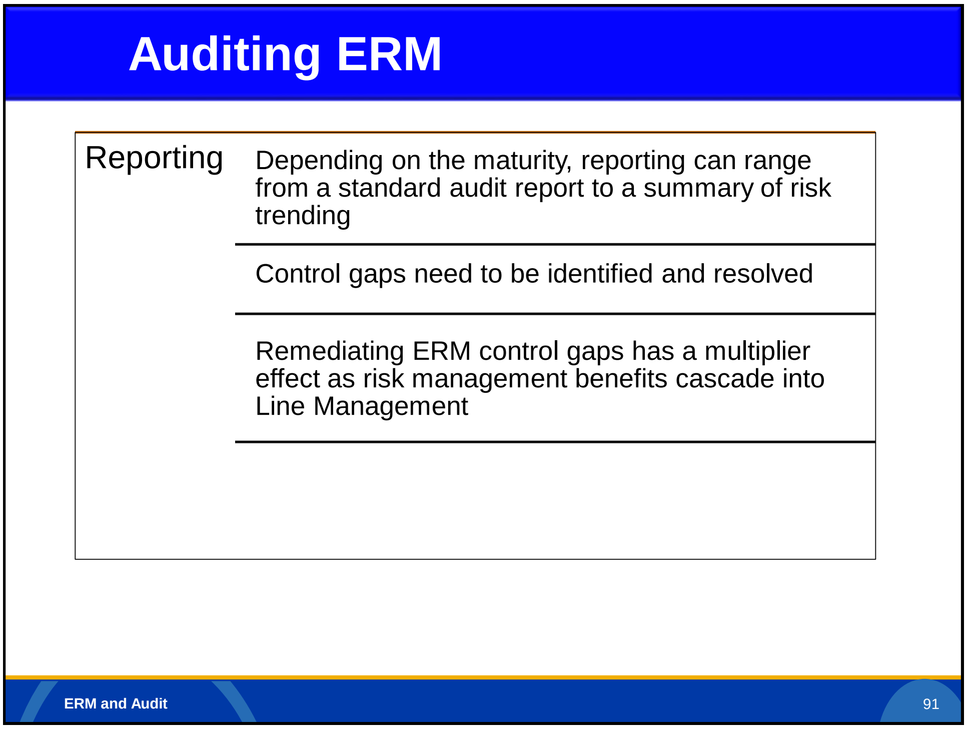
- Risk Policy
- Organizational Strategy
- Goals and objectives
- Risk tolerances
- Risk management organizational structure

- Risk assessment
- Risk response
- Management of risk
- Monitoring and reporting
- Continuous improvement of ERM process



Questions IA Should Ask

1. Are ERM processes designed effectively?
2. Are ERM processes operating as designed?
3. Are risk owners' assertions to senior management regarding risk management performance accurate?
4. Is information provided by management to board/AC accurate and complete?
5. Is tolerance information communicated downward?
6. Are there risk areas not currently covered by an ERM process?



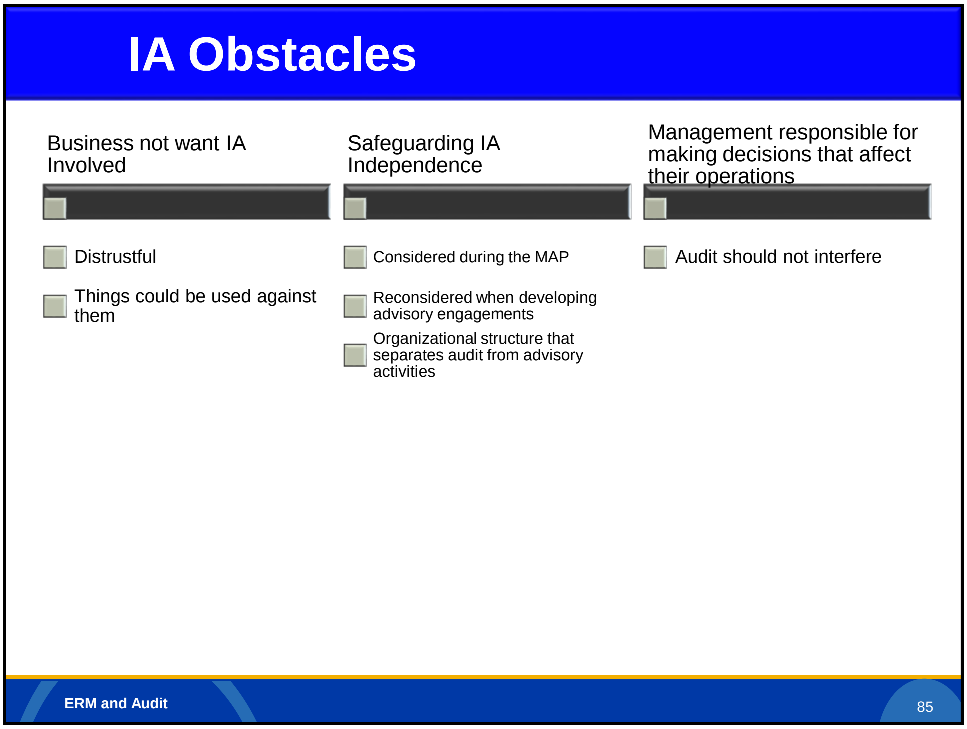
Auditing ERM

Reporting

- Depending on the maturity, reporting can range from a standard audit report to a summary of risk trending
- Control gaps need to be identified and resolved
- Remediating ERM control gaps has a multiplier effect as risk management benefits cascade into Line Management

ERM and Audit

91



IA Obstacles

Business not want IA Involved

- Distrustful
- Things could be used against them

Safeguarding IA Independence

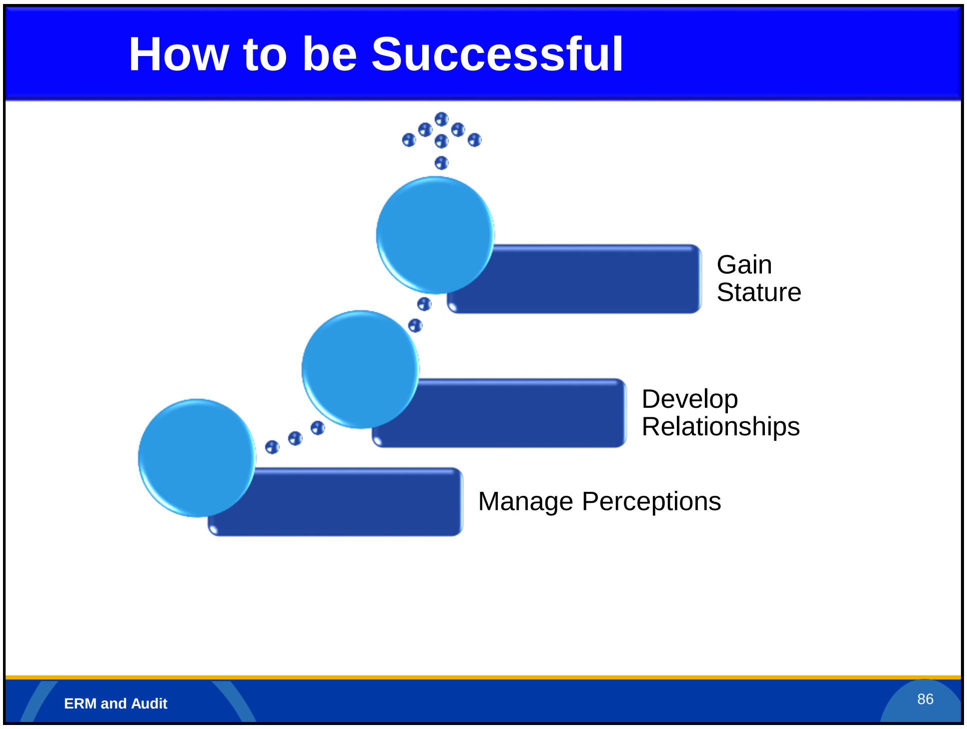
- Considered during the MAP
- Reconsidered when developing advisory engagements
- Organizational structure that separates audit from advisory activities

Management responsible for making decisions that affect their operations

- Audit should not interfere

ERM and Audit

85

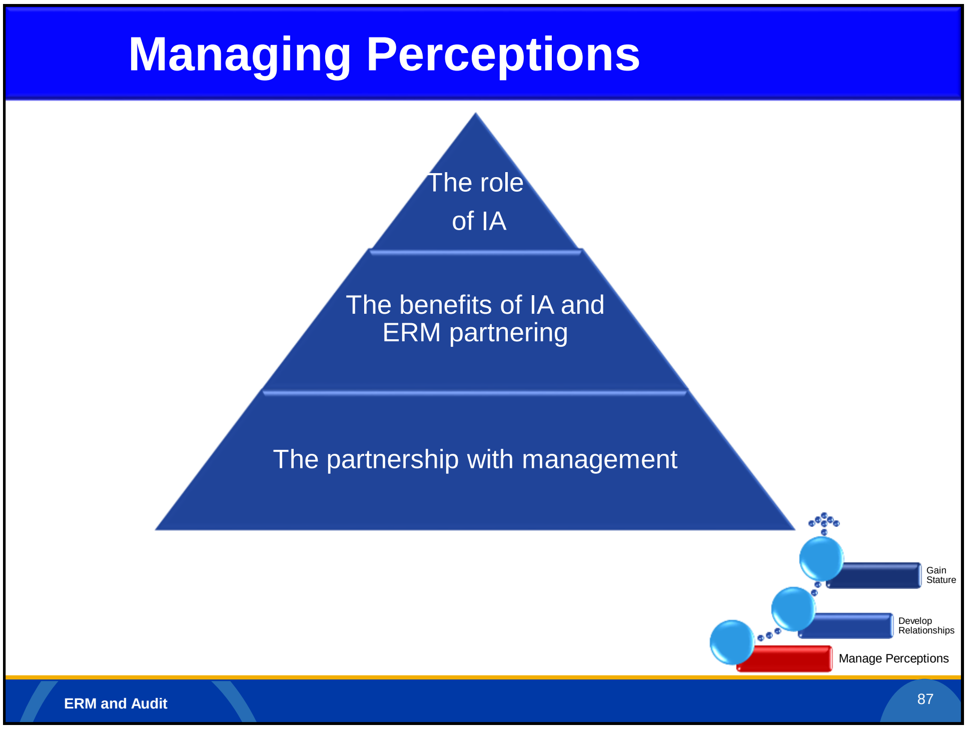


How to be Successful

Gain Stature

Develop Relationships

Manage Perceptions

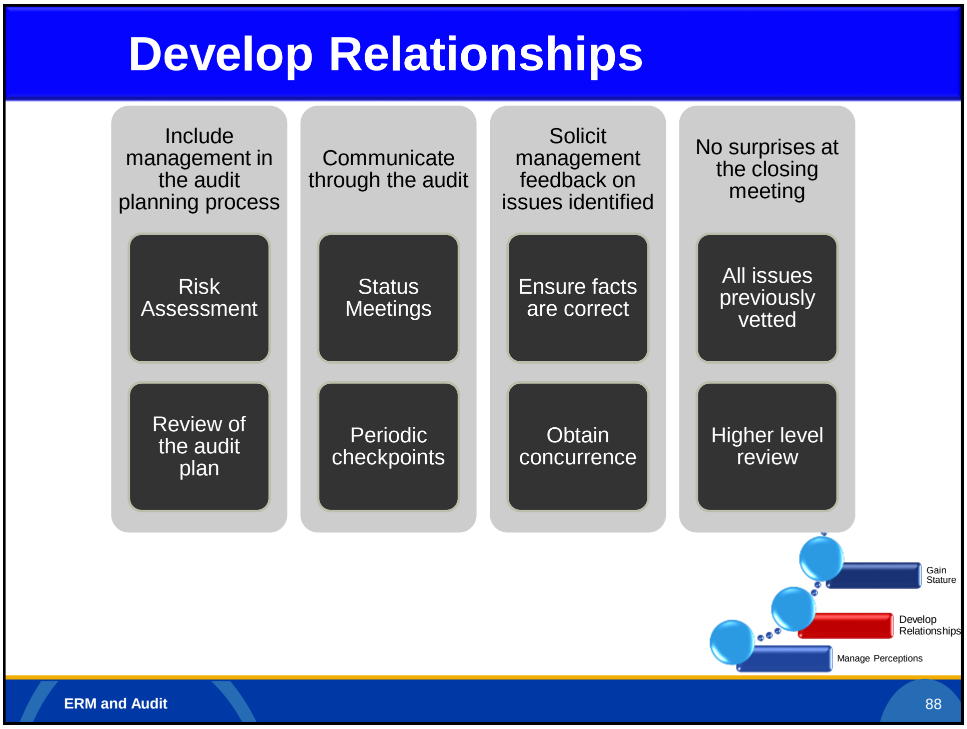


Managing Perceptions

The role of IA

The benefits of IA and ERM partnering

The partnership with management



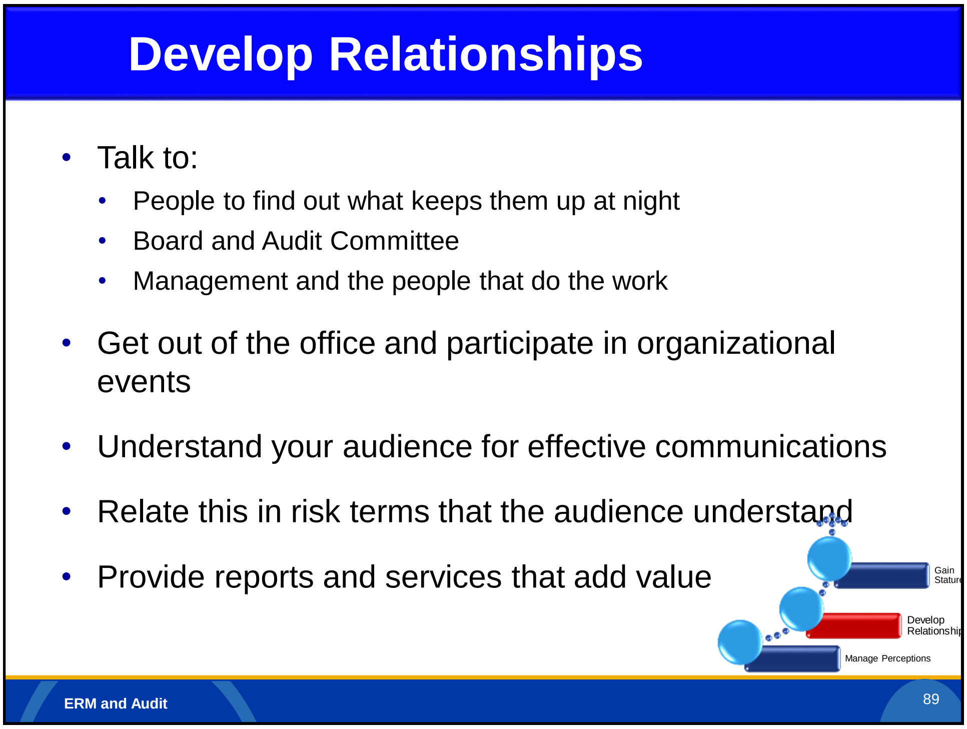
Develop Relationships

Include management in the audit planning process	Communicate through the audit	Solicit management feedback on issues identified	No surprises at the closing meeting
Risk Assessment	Status Meetings	Ensure facts are correct	All issues previously vetted
Review of the audit plan	Periodic checkpoints	Obtain concurrence	Higher level review

Gain Stature

Develop Relationships

Manage Perceptions



Develop Relationships

- Talk to:
  - People to find out what keeps them up at night
  - Board and Audit Committee
  - Management and the people that do the work
- Get out of the office and participate in organizational events
- Understand your audience for effective communications
- Relate this in risk terms that the audience understand
- Provide reports and services that add value

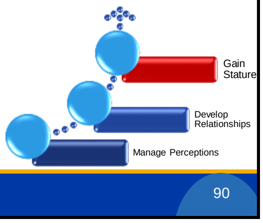
Gain Stature

Develop Relationships

Manage Perceptions

Gaining Stature

- Have an opinion
- Be proactive
- Be realistic with risk – don’t overplay your hand
- When you raise the alarm, they will listen

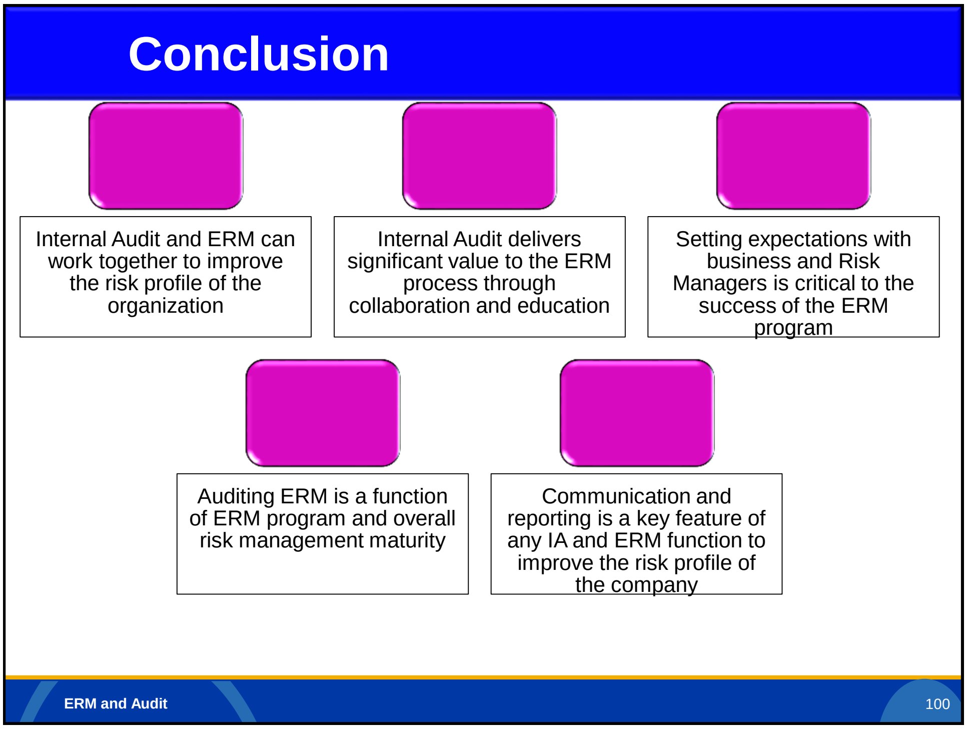


Spread the Message

- Educate and train audit committee and management on ERM
- Find ways to provide risk management advisory services – not audits
- Assess the risks of not having the right people and skills in your organization and mitigate as necessary

Agenda

- Definitions and Processes
- Risks
- Audit & ERM
- Key Strategies
- ➡ Conclusion



Conclusion

- Internal Audit and ERM can work together to improve the risk profile of the organization
- Internal Audit delivers significant value to the ERM process through collaboration and education
- Setting expectations with business and Risk Managers is critical to the success of the ERM program
- Auditing ERM is a function of ERM program and overall risk management maturity
- Communication and reporting is a key feature of any IA and ERM function to improve the risk profile of the company