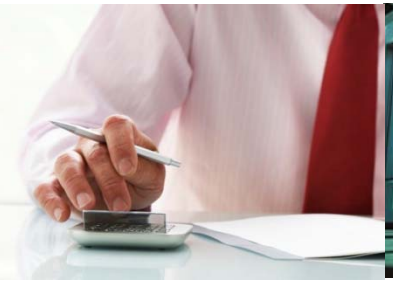
Assessing the Effectiveness of Your Risk Management Program

James B. Yard
Internal Audit and Risk Advisory Services

Schneider Downs & Co., Inc.
October 22, 2013

SCHNEIDER DOWNS

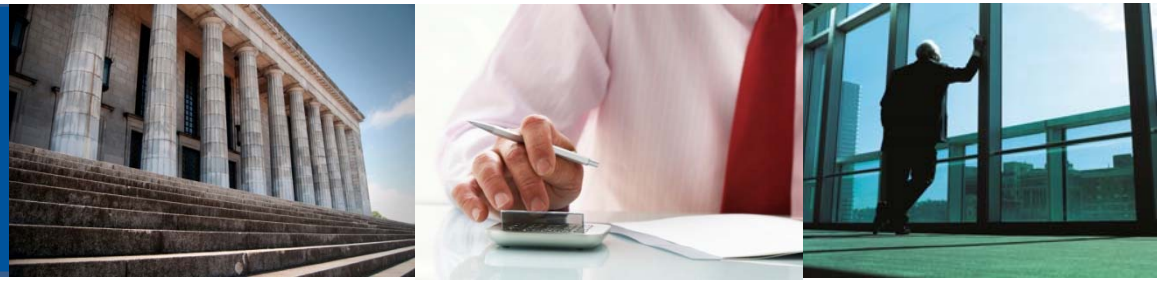
SCHNEIDER DOWNS



Learning Objectives

During our time together, we will explore:

- Evolution of risk management
- How are not-for-profits addressing risk management?
- How does an organization identify strategic risks in today's environment?
- How do we go about implementing and executing an effective risk management program?
- Best practices and pitfalls



Enterprise Risk Management (ERM) Overview

COSO – The Committee of Sponsoring Organizations of the Treadway Commission

The **COSO** "Enterprise Risk Management-Integrated Framework“ defines ERM as …

“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."

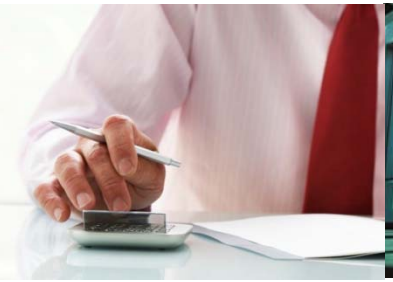
SCHNEIDER DOWNS

What is Enterprise Risk Management?

My definition - A discipline of understanding risk for the purpose of appropriately allocating an organizations resources on business activities that present high risk and exposure to the organizations strategic purpose and ability to prosper. ERM offers a framework for effectively managing uncertainty, responding to risk and harnessing opportunities as they arise.

By focusing on, dedicating resources to, and continuously monitoring these business activities - an organization continuously improves it's operations and value is derived.

SCHNEIDER DOWNS

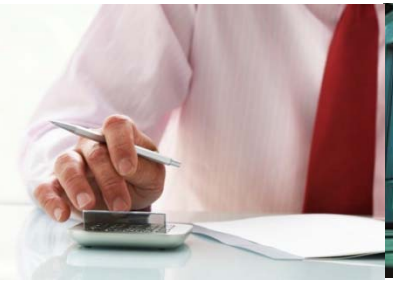


Evolution of Risk Management

Traditional risk management can be characterized by fragmented responsibility, rather than a holistic approach; a focus on discrete events; a perception of risk management being a product of transaction (insurance/hedge) or a reaction to events.

The move to today's ERM is strategic and focused. Today's ERM model allows organizations to integrate business managers with risk managers, increase non-financial risk awareness, and increase involvement from all areas of the organization - executive management, board members, and business managers.

SCHNEIDER DOWNS


Traditional vs. Leading Edge

Traditionally risk was viewed more from a financial risk perspective. The new standard is to look at risk throughout the enterprise.

Financial
Operational
Compliance

Strategic Initiatives
Competitive Advantages
Culture
Human Capital
Operational/Transaction
Interdependencies on other units
Financial Capture and Reporting
Technology
Compliance
Business Continuity
Legal/Regulatory
Reputation
Fraud
Waste and Mismanagement
Safety and Security

SCHNEIDER DOWNS

Board Members Should Be Asking

- Is there an established mechanism that addresses key risks across the organization and which elevates risk discussions to the strategic level?
- Has the organization conducted an in-depth, prioritized analysis of the top risks that can really make-or-break the organization?
- Do we understand the "big bets" we are taking as an organization?
- Is there a clear understanding of risks that management can measure and track?
- Do we have an established risk review process and get from management insightful risk reports?
- Do we have ownership, accountability and the right resources on risk matters?

Board Members Should be Asking

- Do our strategic planning, capital allocation, and financing activities consider risk factors?
- Is risk governance and risk-related committee structures at the board level defined?
- Is top management's compensation structured to ensure performance in light of risks taken?

Asking these tough questions enable directors to fulfill their fiduciary duties and ultimately help their organizations prosper.

Survey Results - What the Non-Profit Community Has to Say

Sent to over 600 Non-Profit Leaders

Responses rate of 12%

SCHNEIDER DOWNS

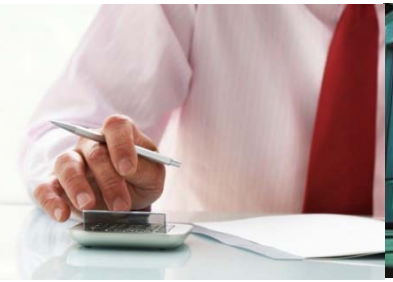
What is the size of your organization?

0-25 employees (20%)
26-50 employees (14%)
51-100 employees (11%)
101-500 employees (31%)
500+ employees (23%)

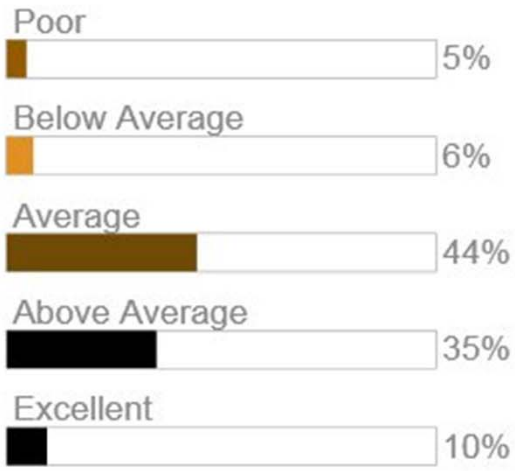
What is your organization's annual revenue?

Less than $2 million (12%)
$2-10 million (28%)
$10-25 million (19%)
$25-50 million (19%)
$50-100 million (11%)
Greater than $100 million (11%)

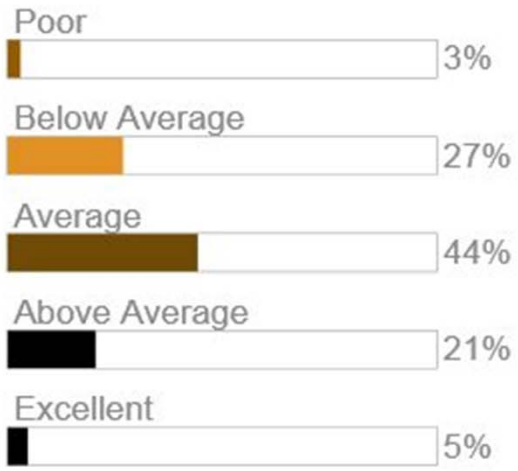
SCHNEIDER DOWNS



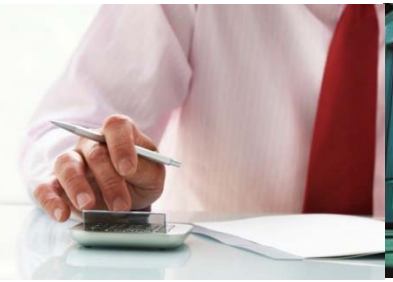
Identification and Consensus on Top Risks



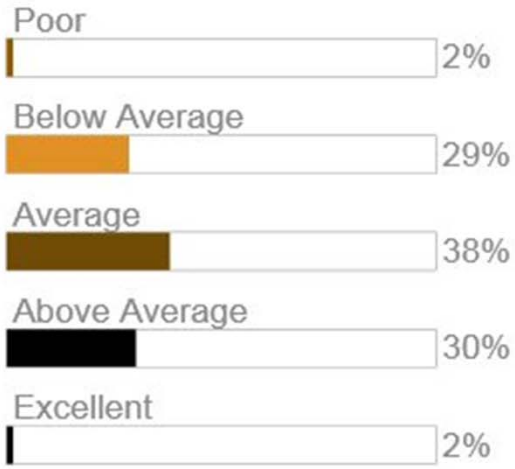
Education and Training on Risk Matters



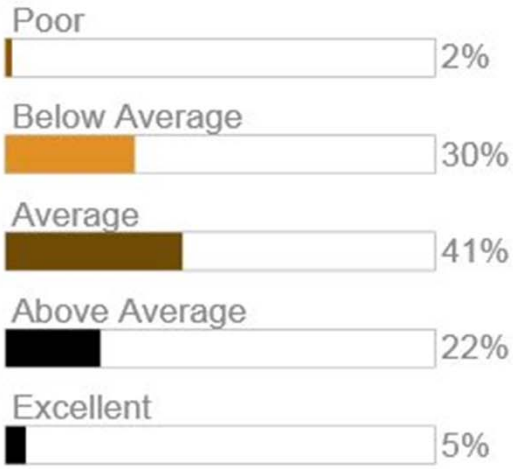
SCHNEIDER DOWNS



Linking Risk Management with Organizations Strategy and Decision Making

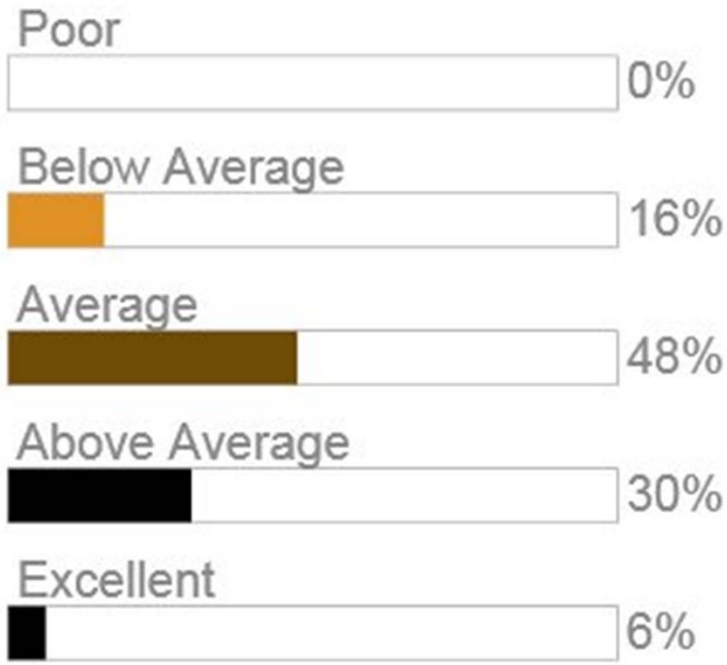


Ensuring Individuals Know Their Role in Managing Risk



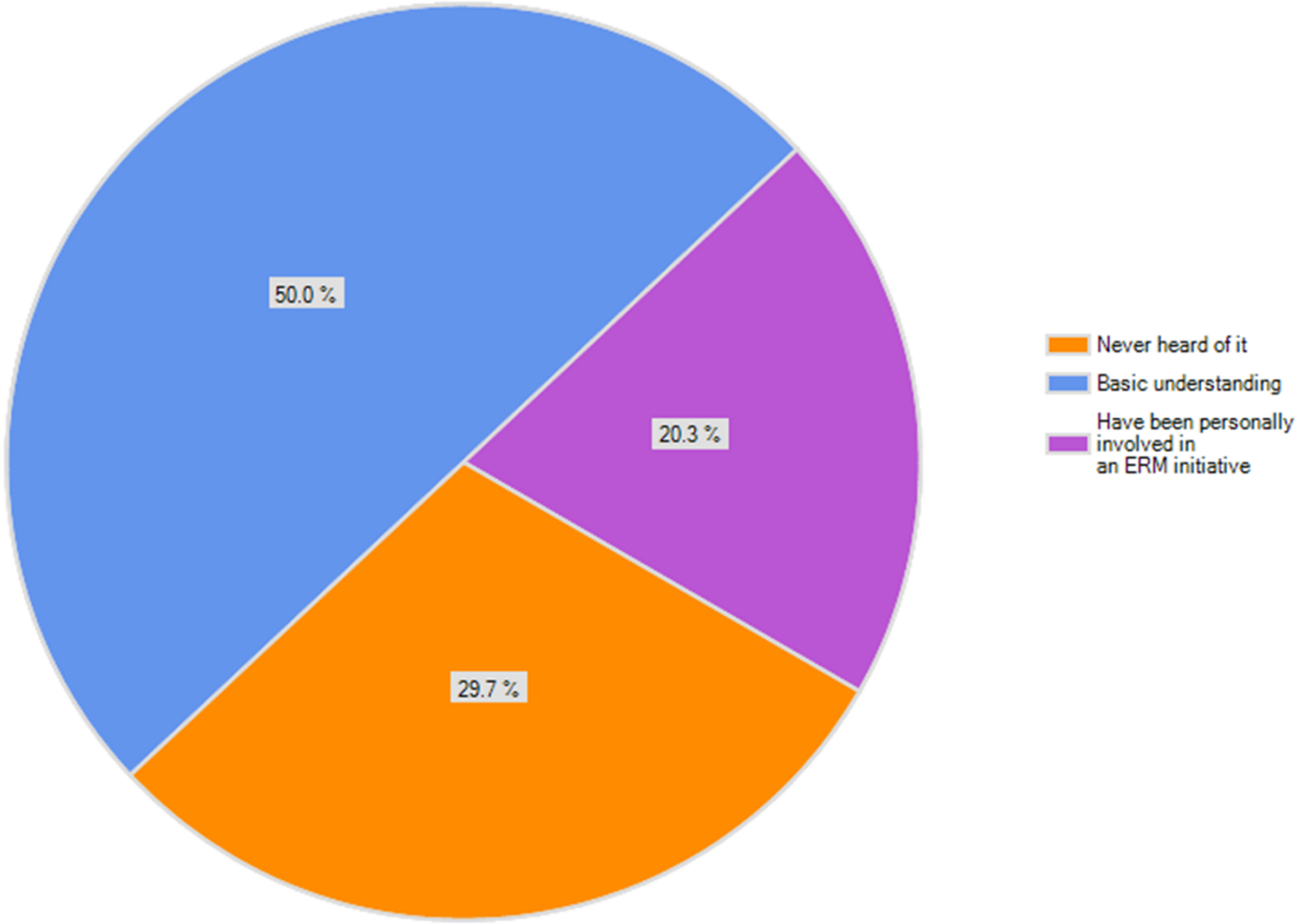
SCHNEIDER DOWNS

Anticipating and Managing Risks



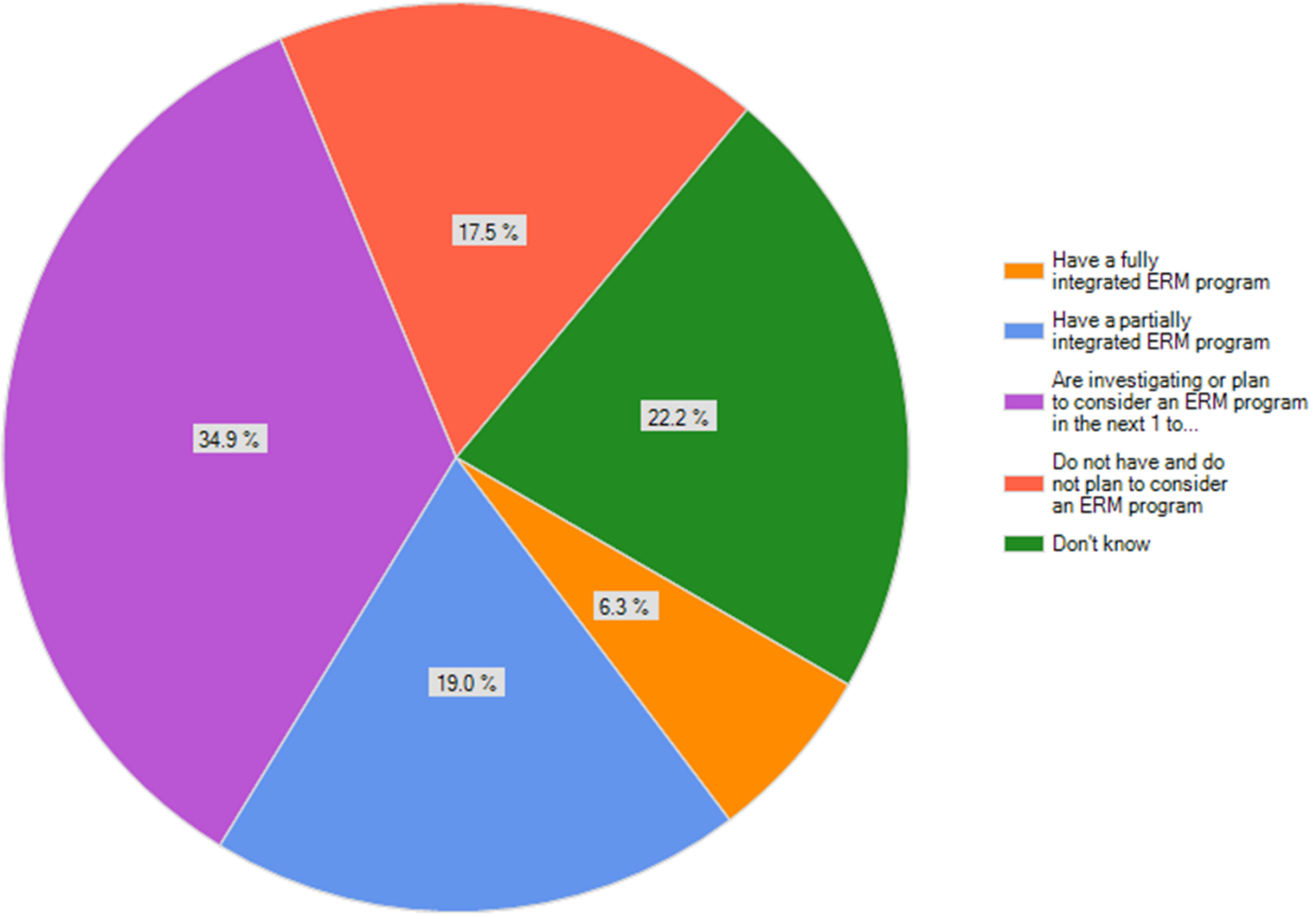
SCHNEIDER DOWNS

Please assess your individual knowledge of Enterprise Risk Management (ERM)



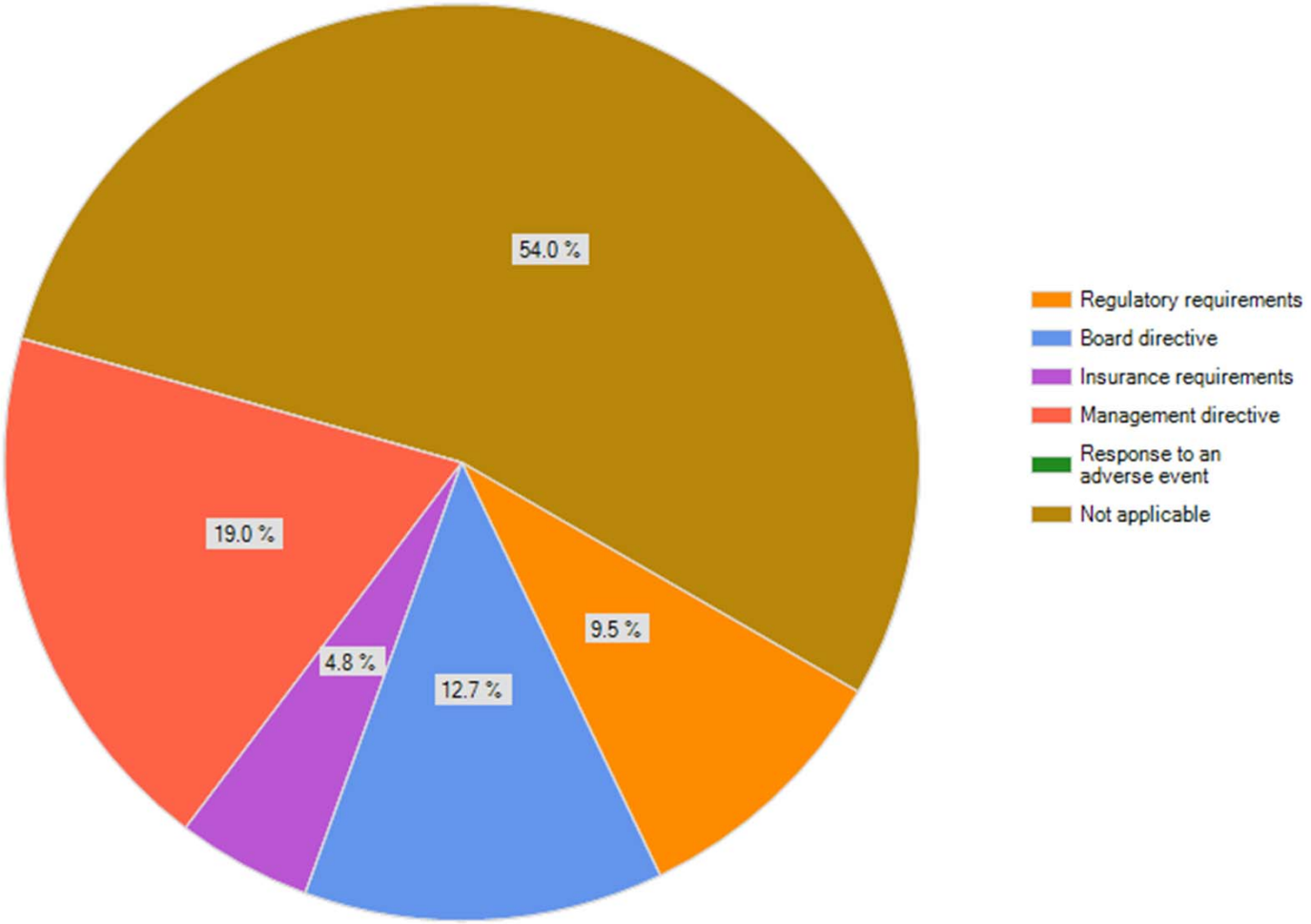
SCHNEIDER DOWNS

To what extent has your organization adopted or considered an ERM program?

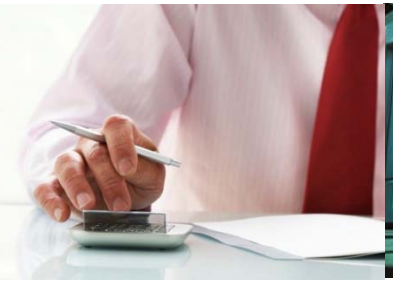


SCHNEIDER DOWNS

What was the primary motivator for adopting ERM in your organization?



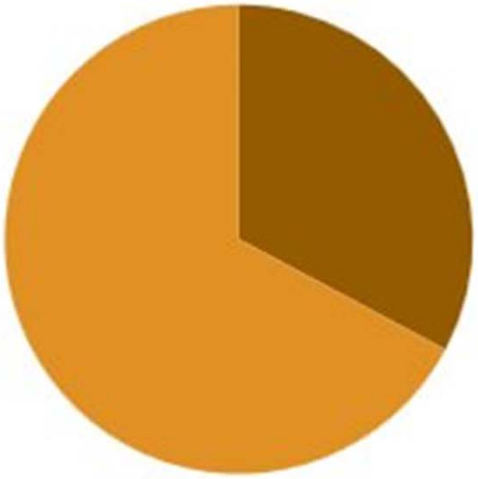
SCHNEIDER DOWNS



Outsourcing Risk Management Activities

- 7% of respondents surveyed outsource their risk management program
- An additional 9% are considering outsourcing within the next 1 to 5 years

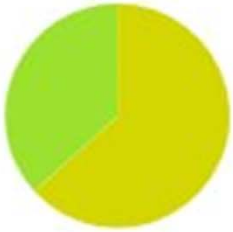
SCHNEIDER DOWNS



Does your organization have an employed individual dedicated to overseeing and identifying risk management?

If yes, how long has your organization had this position?

64.9% of respondents do not have this position
17.5% of respondents have had the position in place more than 5 years
10.5% have had the position 1-5 years
7% have had the position less than 1 year

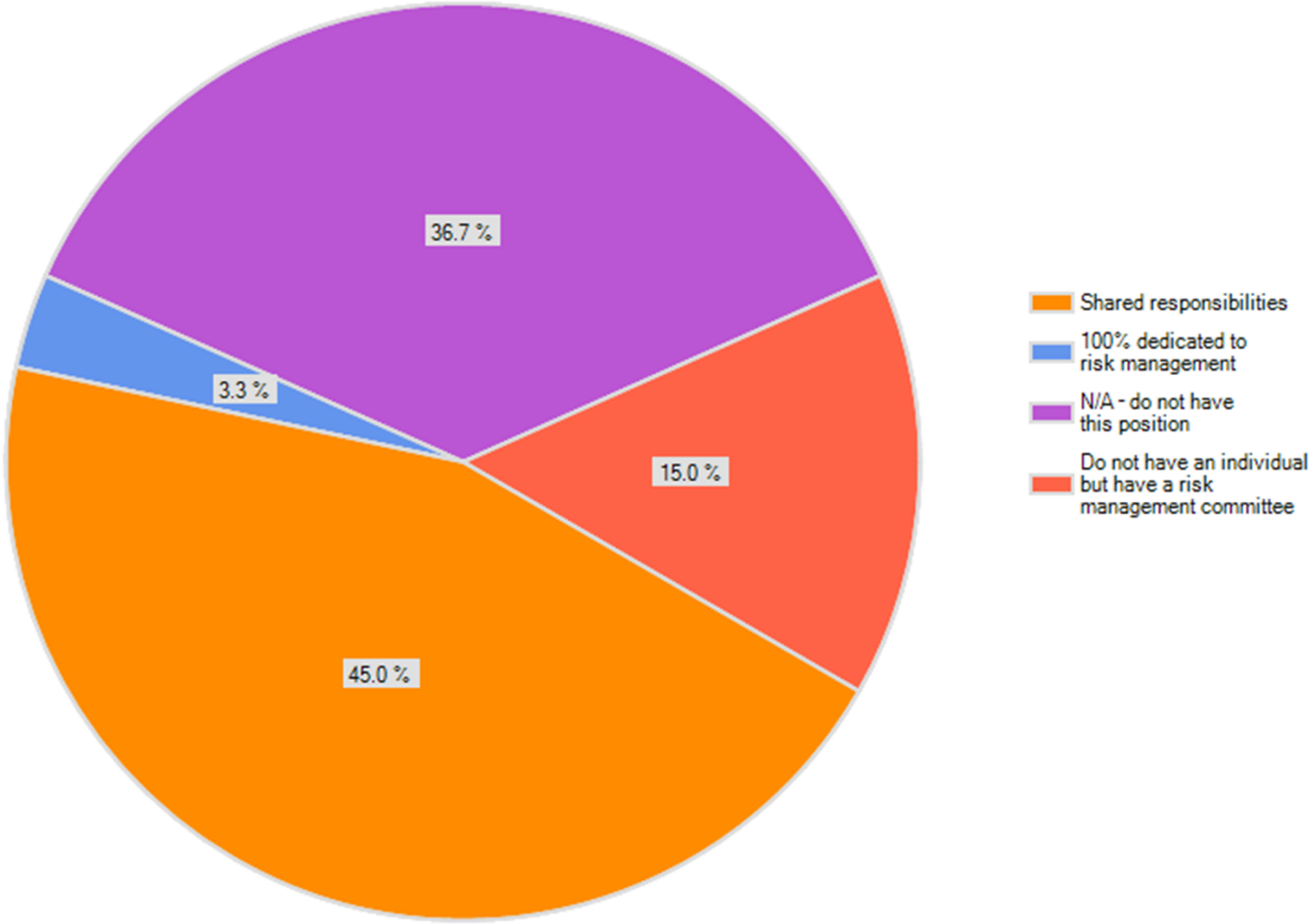


If no, are there plans to add a position?

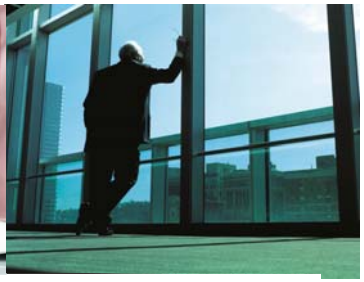
0% - yes
63.2% - no
36.8% - N/A, we have this position

SCHNEIDER DOWNS

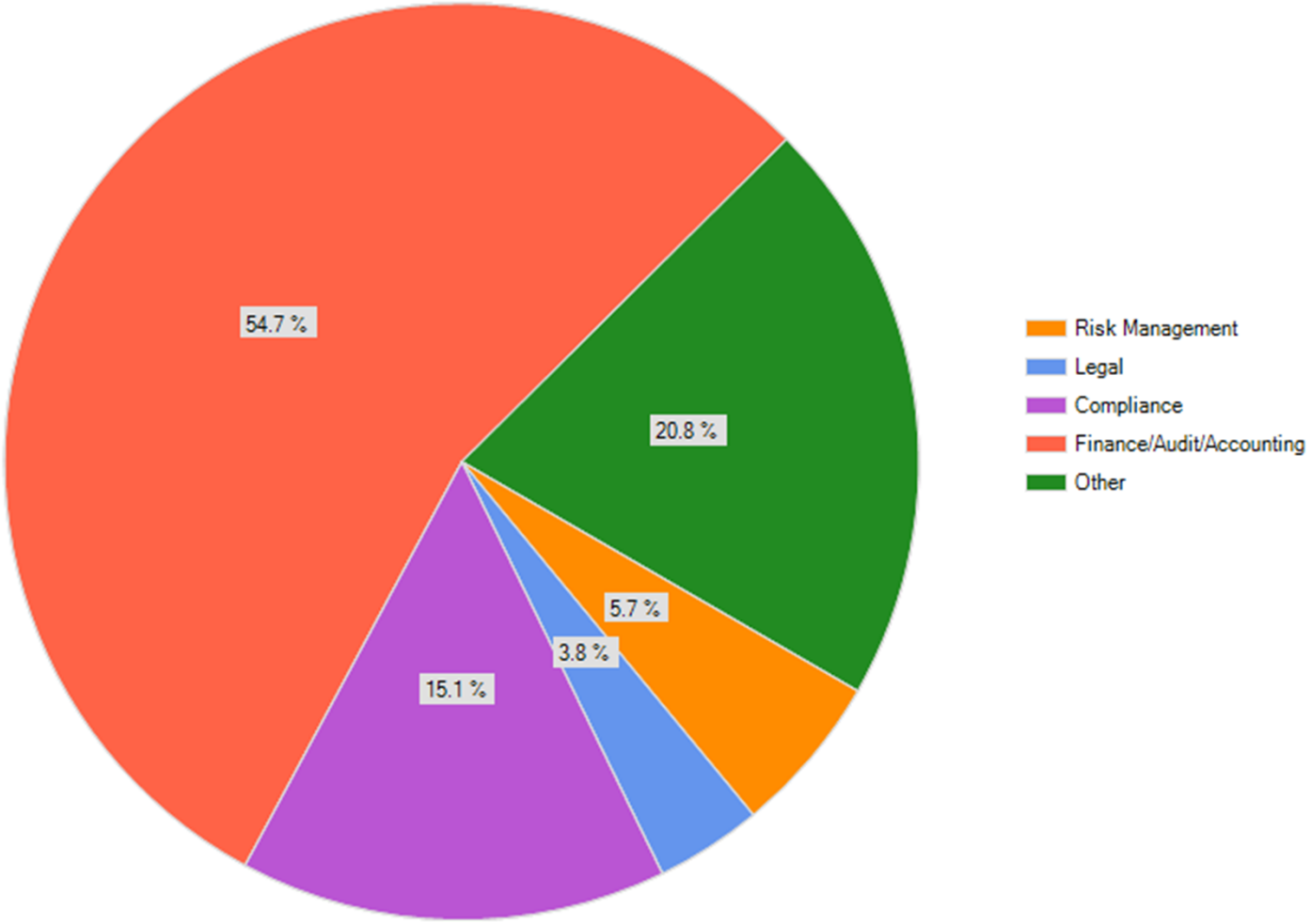
Does your risk management professional hold other responsibilities or are they 100% dedicated to risk management?



SCHNEIDER DOWNS



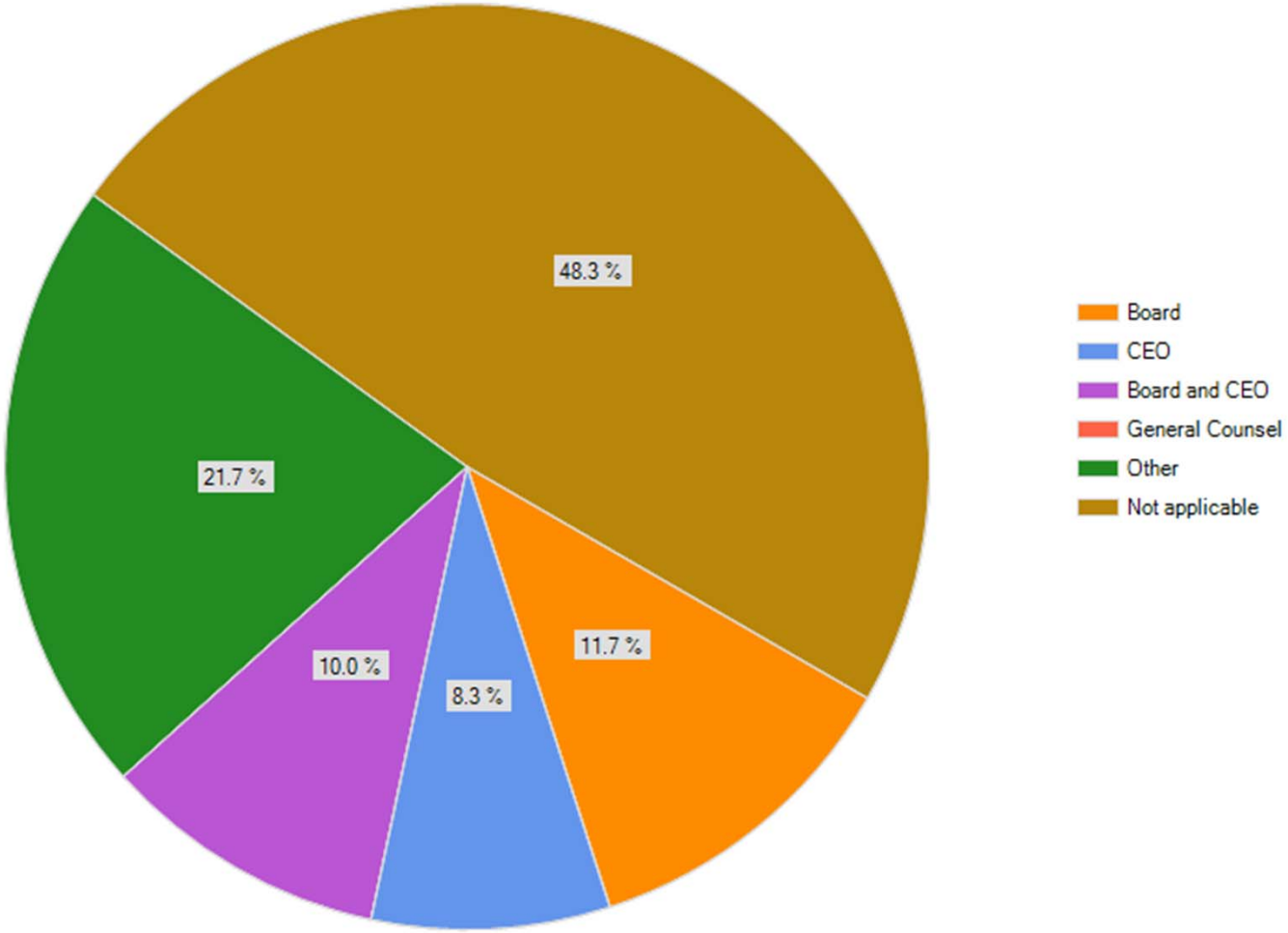
What department within your organization is primarily responsible for directing ERM?



SCHNEIDER DOWNS

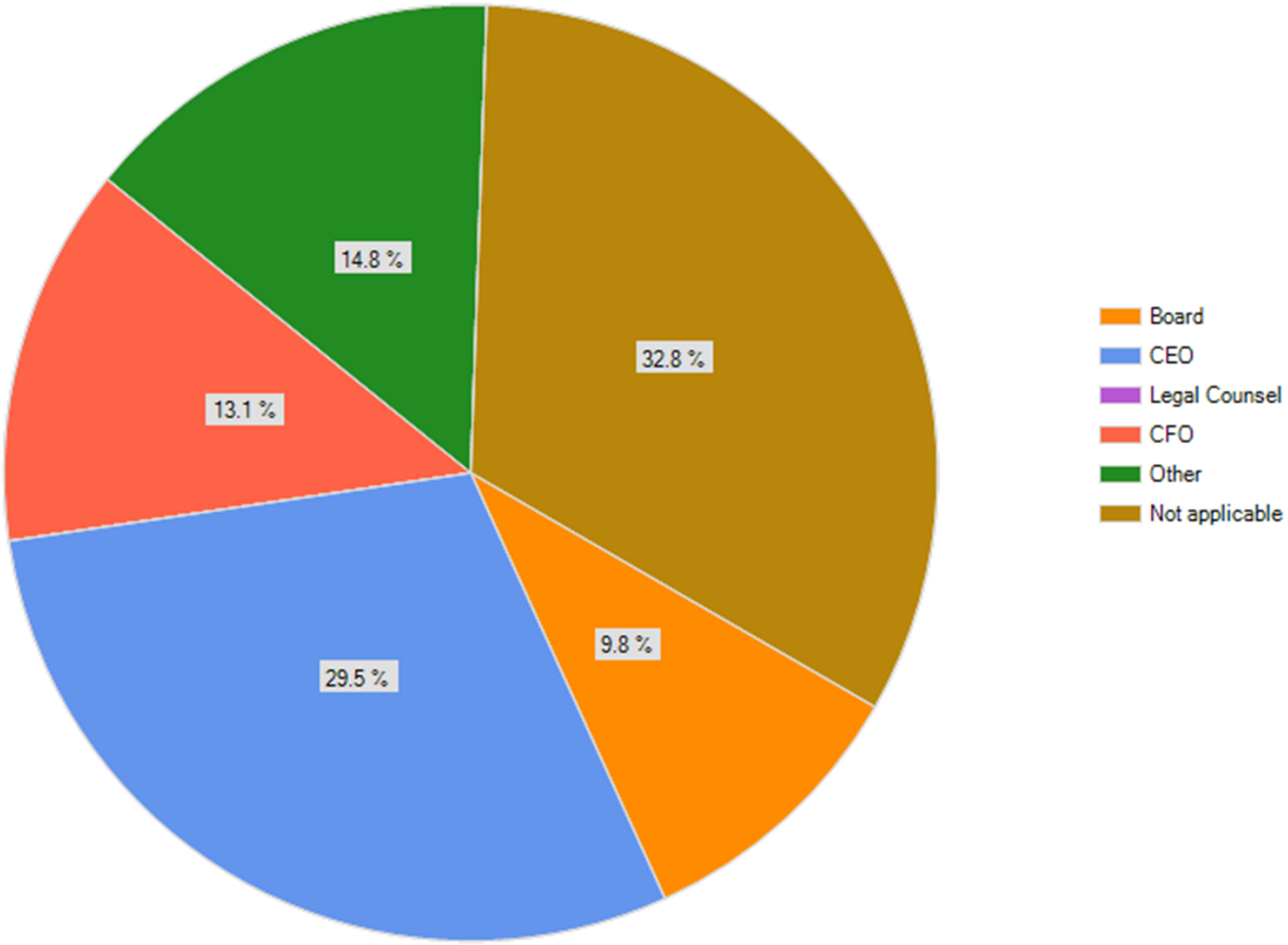


Who was the primary advocate for implementing ERM within your organization?



SCHNEIDER DOWNS

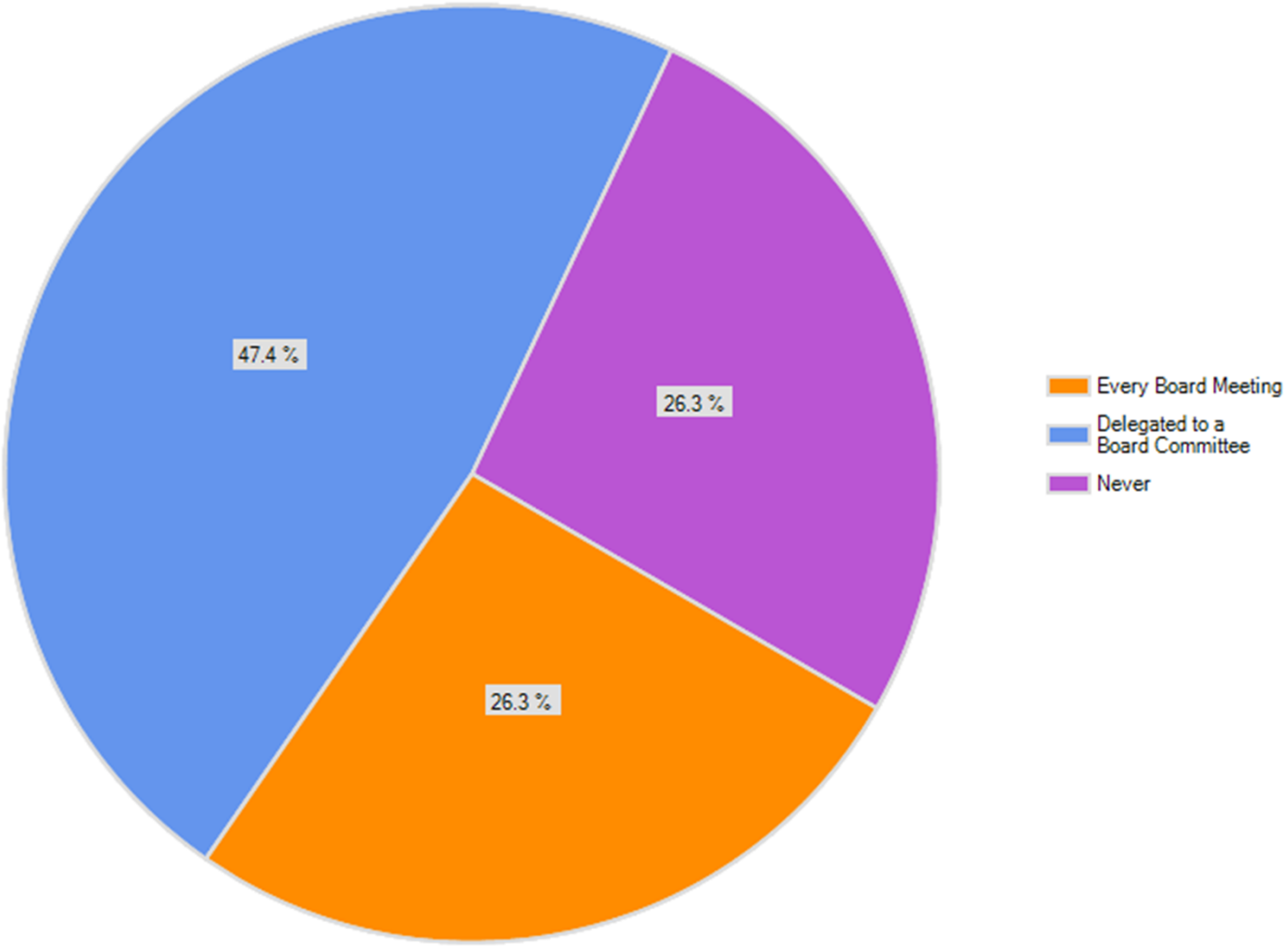
To whom does your risk management professional-administrative report?



SCHNEIDER DOWNS

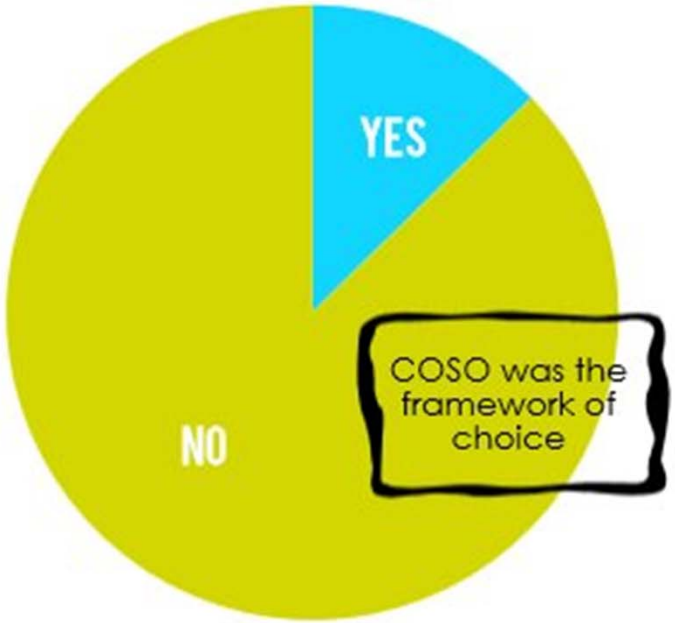


How often does your Board discuss the risks to your organization?



SCHNEIDER DOWNS

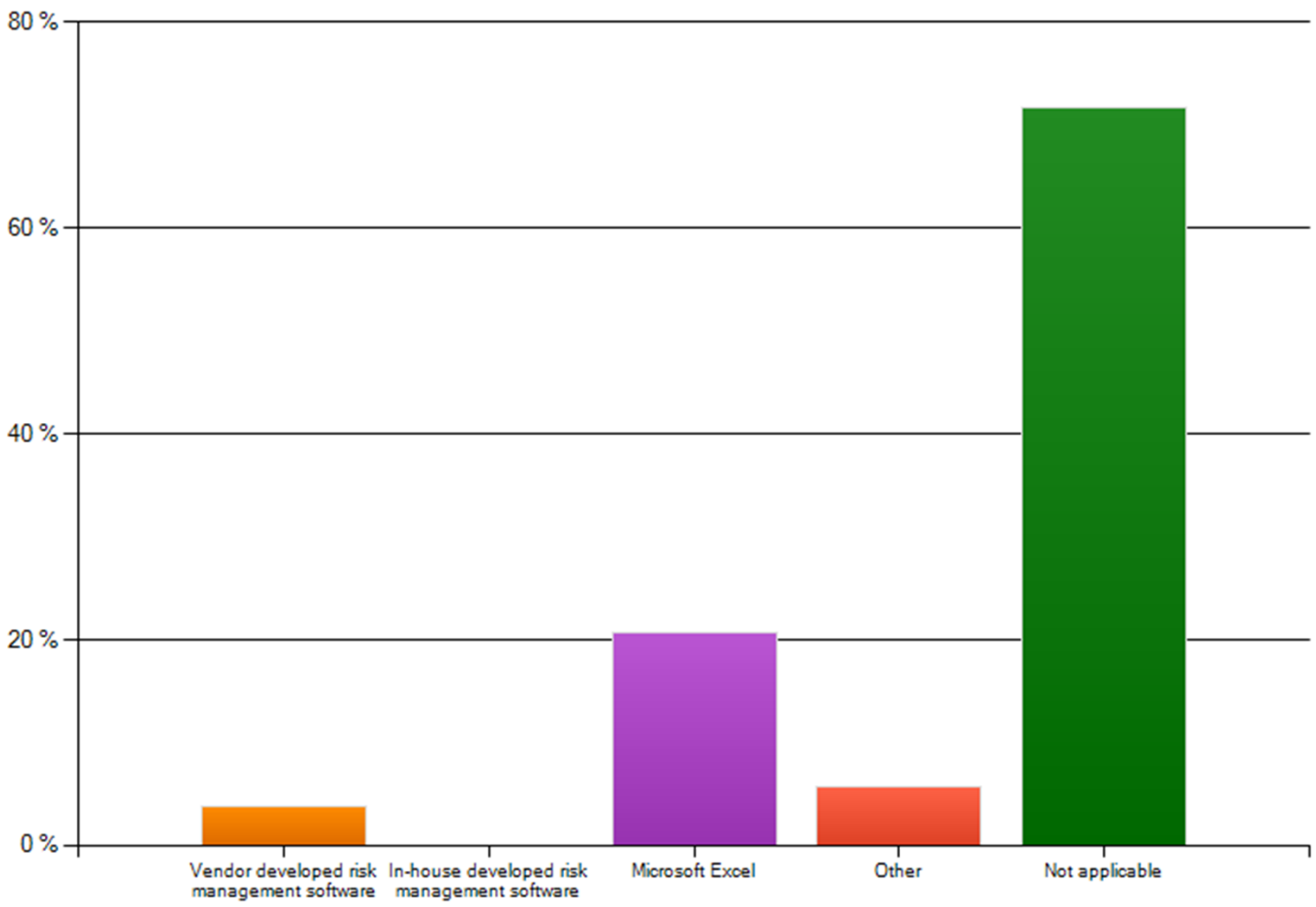
13% of respodents stated that their organizations have adopted a formal Enterprise Risk Management framework



9% of respondents answered that their framework was approved by the Board or a Board committee

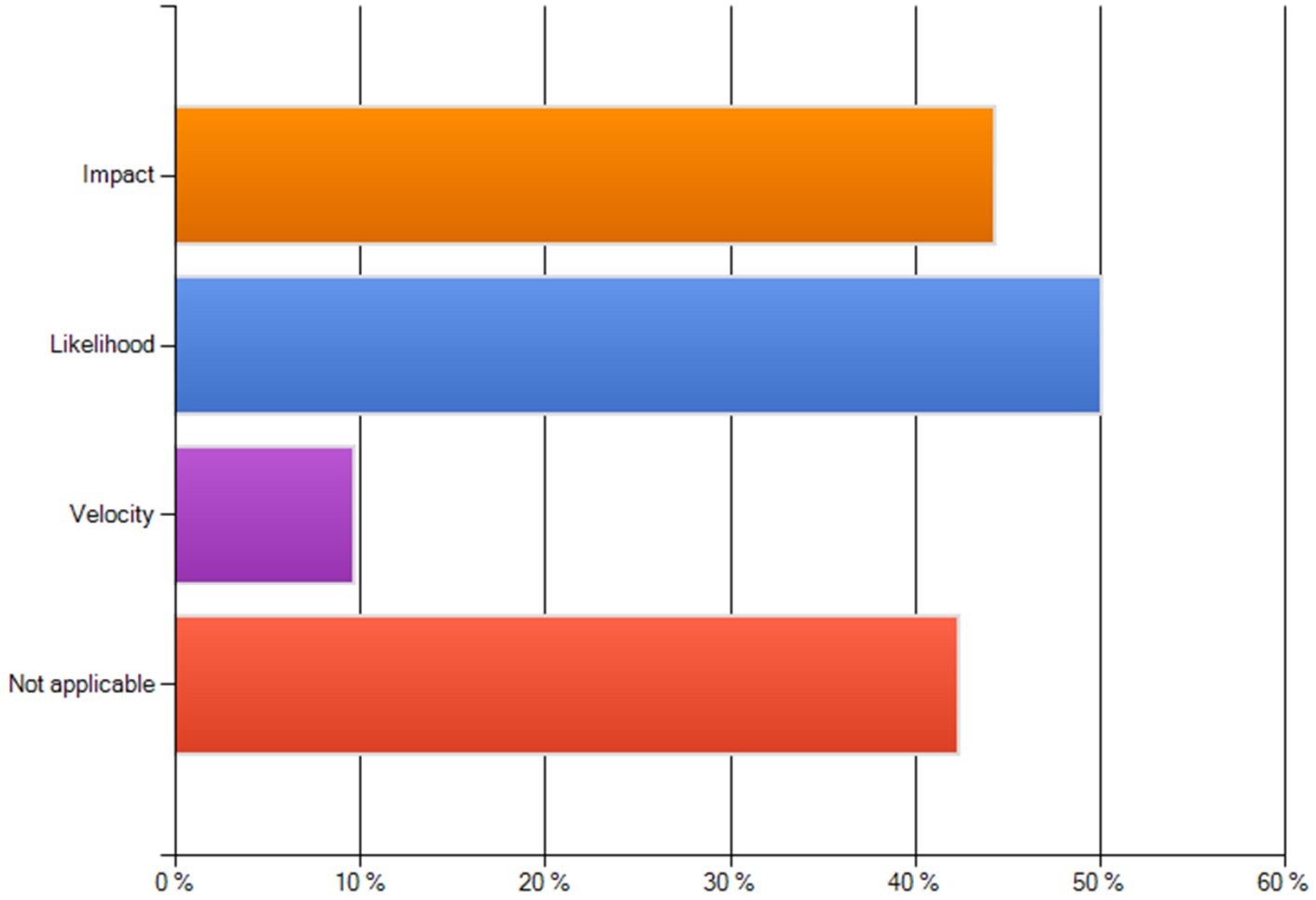
SCHNEIDER DOWNS

What software tools does your organization utilize to enable your risk management function?



SCHNEIDER DOWNS

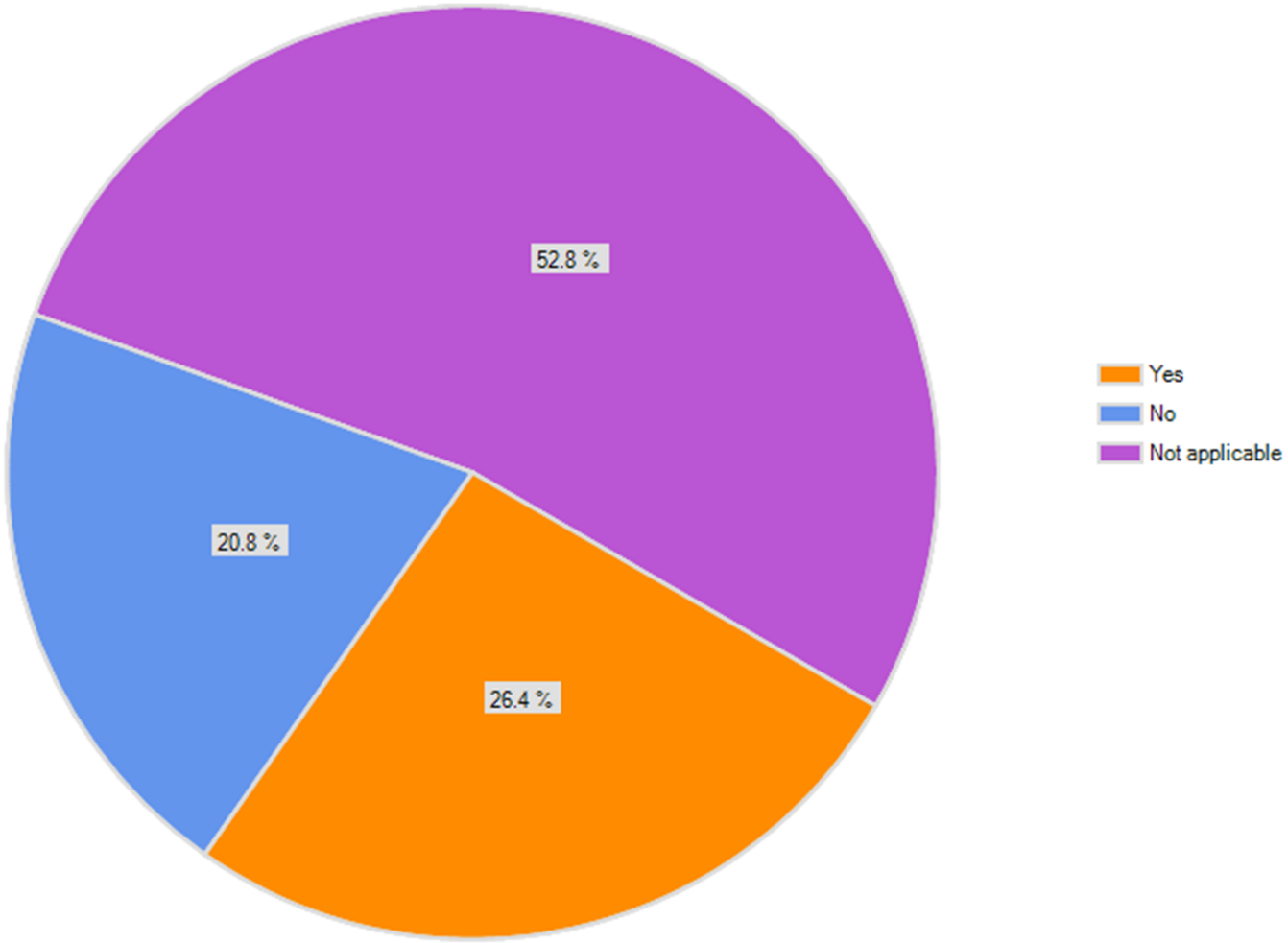
What criteria does your organization utilize for quantifying risk within your organization? Please select all that apply.



SCHNEIDER DOWNS



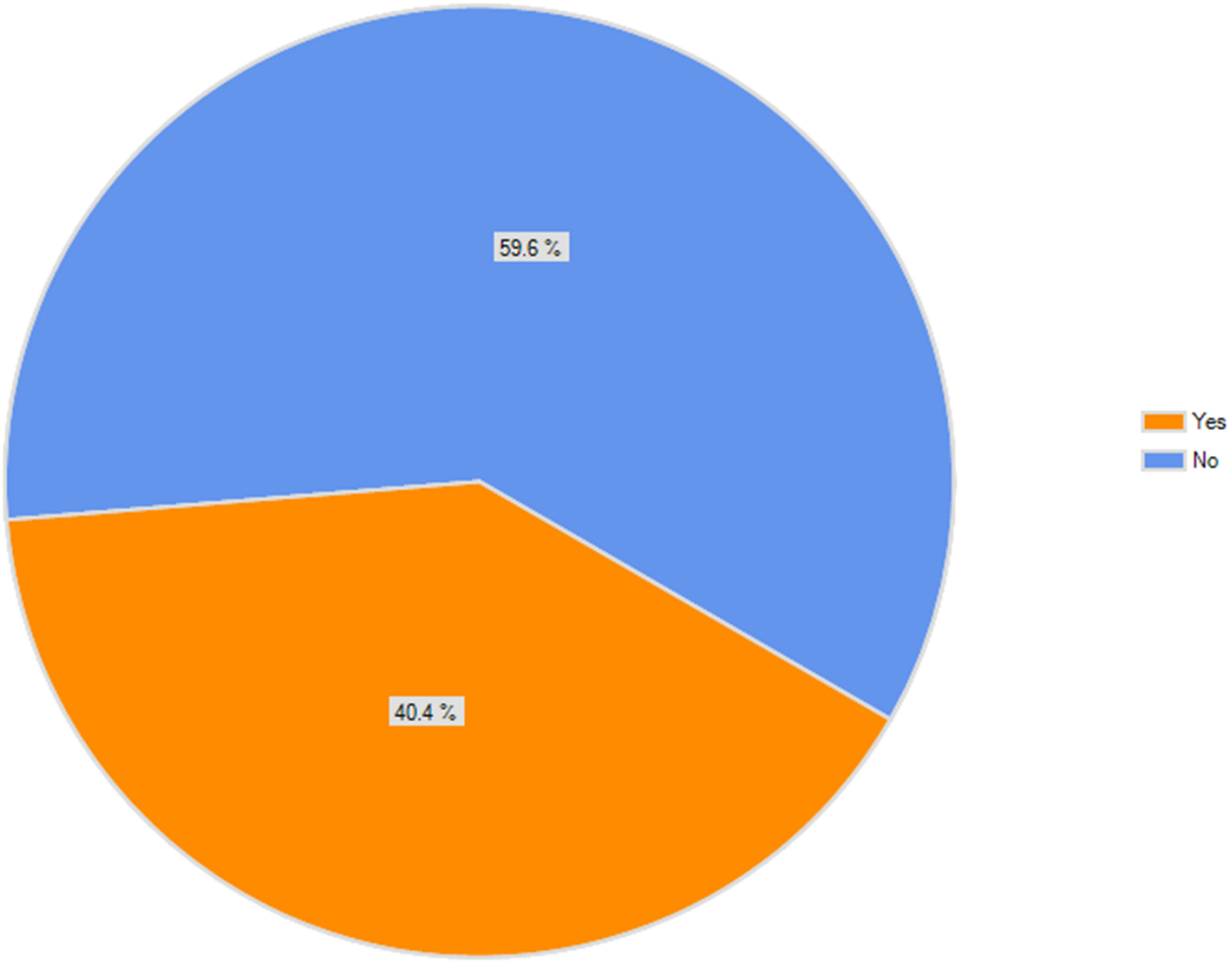
Does your organization utilize risk appetite to make informed decisions on risk matters?



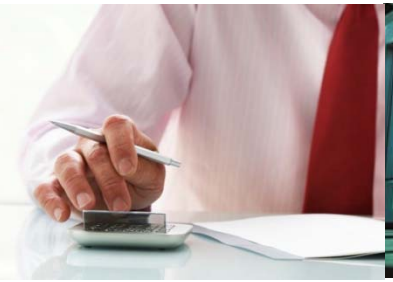
SCHNEIDER DOWNS



Is your organization satisfied with its risk management practices?



SCHNEIDER DOWNS



Implementation – It is really not that hard to do

1 Phase 1
Project governance

- Develop project plan
- Assign executive sponsor
- Define leadership team
- Approval of risk policy and framework

2 Phase 2
Conduct the initial enterprise-wide risk assessment & develop an action plan

- Define risk universe
- Develop and define ranking criteria
- Risk assessment advance communication sent to management

3 Phase 3
Inventory the existing risk management strategies and controls

- Conduct executive interviews – data gathering and documentation
- Evaluate management's responses on risk
- Perform gap analysis

4 Phase 4
Reporting and Sustainability

- Develop initial risk reporting
- Develop ongoing monitoring
- Final Plan to organization management
- Develop appropriate executive management & board communications

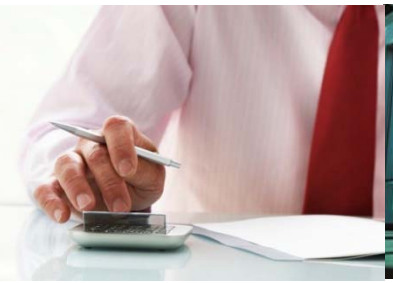
Key Outputs			
Project plan Policy Defining risk Defining reporting relationships and resource requirements	Risk workshop advance prep Ranking criteria Standard templates	Completed risk model Gap analysis	Risk reports

Risk Management Principles

Risk Management should:

- Be linked and embedded in your strategy
- Create and protect value
- Be part of all processes
- Be part of your decision making
- Be used to handle uncertainty
- Be systematic and timely
- Be based on the best data
- Be tailored to your environment
- Consider human factors
- Be transparent and inclusive
- Be responsive and iterative
- Support continuous improvement

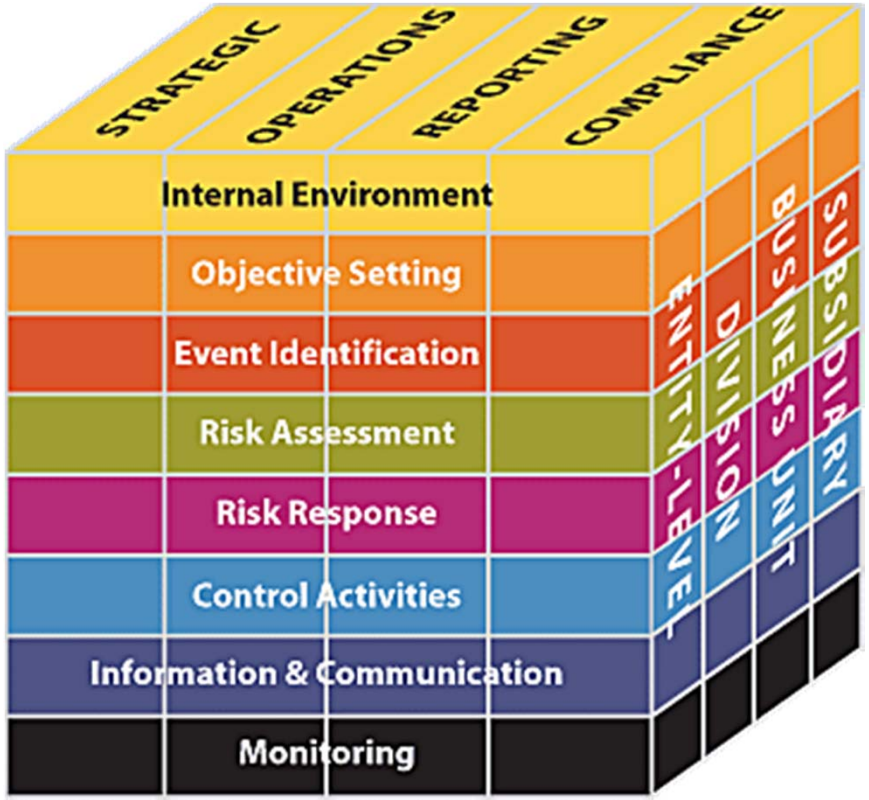
SCHNEIDER DOWNS


Choosing a Framework

Which Framework do you use?

- Anyone you want, however …
  - COSO ERM
  - AS/NZS 4360:2004
  - The Turnbull Guidance
  - ISO 31000-2009



My Take on ERM in Non-Profit World

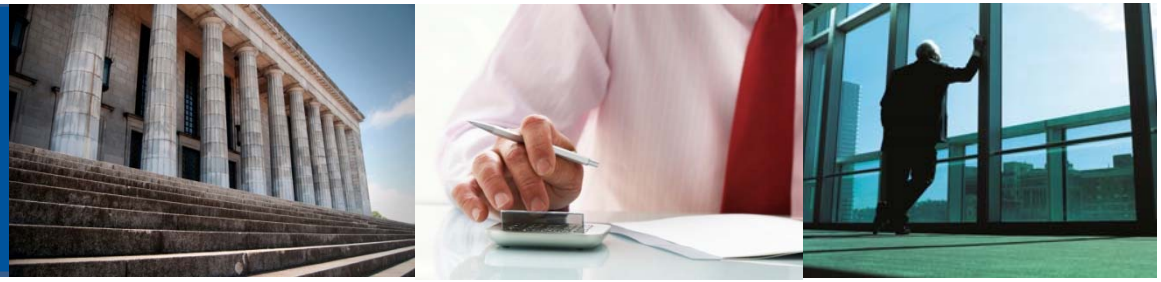
- Keep it focused, simple and easy to understand or it will fail
  - Commitment, involvement and consensus
  - Link it to your strategy
  - Looks outside your walls (industry and peer analysis)
  - Consider Black Swan events
  - Get to a top 10 or 20, but also evaluate scenarios where multiple risks could have substantial impact
  - Manage, monitor, and improve in areas where greatest value can be achieved
  - Manage progress and enforce accountability

- Often the most significant risks and opportunities for value reside in areas threatening your key/strategic business objectives:
  - Strategy
  - Competition
  - Reputation
  - Mission/Program Differentiation

SCHNEIDER DOWNS

Leading Practices

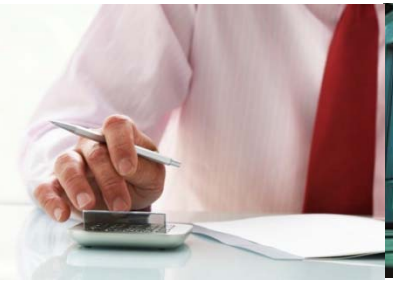
- Establish a risk management policy for your organization
- Communicate your risk management policy
- Fully engage your board of directors
- Involve risk management into strategic planning
- Integrate risk management into your business functions
- Assign risk ownership and accountability for risk management
- Communicate and ensure transparency
- Gather intelligence (benchmarking, trend analysis)
- Continuously monitor
- Evaluate scenarios (stress testing, disaster recovery)
- Allocate time and resources



What is the Value?

- More effective strategic and operational planning
- Planned risk-taking and the proactive management of risks
- Greater confidence in decision making and achieving operational and strategic objectives
- Greater stakeholder confidence
- Enhanced organizational resilience
- Dealing effectively with disruptions and losses, minimizing financial impact
- Avoid surprises through forward planning
- Regulatory compliance and director protection

SCHNEIDER DOWNS



Common Pitfalls

- Not linking strategic planning and risk management
- Not positioning ERM as a management practice
- Procedural approach (restrictive/limiting)
- Many failures explained by challenges of responding to an unanticipated event, Black Swan event, or combination of events
- Placing risk management oversight with the audit committee
- Diminishing transparency
- Lack of support at the executive level
- Not looking beyond impact and likelihood
- Lack of understanding on the “Big Bets” being taken
- Failure to assess industry and peer dynamics

SCHNEIDER DOWNS

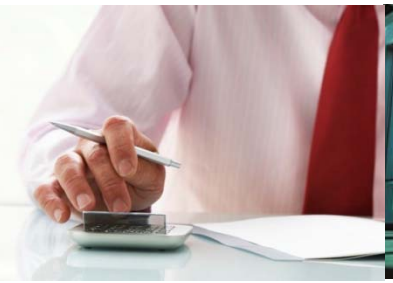
Key Takeaways

- Understand your organization's culture, strategies and objectives
- It is not that hard - keep it simple
- Involve your board and key business advisors
- Dedicate resources and train them
- Develop a common risk language
- It should improve your organization
- Continuously monitoring and reporting

SCHNEIDER DOWNS

"We've considered every potential risk except the risks of avoiding all risks."

SCHNEIDER DOWNS



James B. Yard

Internal Audit and Risk Advisory Services
CPA, CIA, CISA

Contact Information:

jyard@schneiderdowns.com
One PPG Place, Suite 1700
Pittsburgh, PA 15222
Phone: 412-697-5345