

Keep Calm and Assess Your Risk with Enterprise Risk Management (ERM)

Wednesday, August 12, 2020



CPAs & ADVISORS

Melissa Musser,
CPA, CITP, CISA

*Principal, Risk & Advisory Services,
GRF CPAs & Advisors*

Alex McNeill,
PMP

*Enterprise Risk Manager,
Bridges to Prosperity*

Firm Background

Gelman, Rosenberg & Freedman CPAs is now GRF CPAs & Advisors



Personal
Service With
Powerful
Solutions

Since 1981

600+ nonprofits

accountingTODAY
BEST
ACCOUNTING
FIRMS
TO WORK FOR
2019

INSIDE
PUBLIC ACCOUNTING
TOP 200
FIRMS
2020

100²⁰¹⁹
accountingTODAY
REGIONAL LEADERS

- + Washington Business Journal's **Top 25 Accounting Firms in DC Metro**
- + Accounting Today's **Top Firms in the Capital Region for 2020 and 2020 Firm to Watch**

Housekeeping

CPE Credit/Technical Support

- **Important:** Three (3) CPE words will be provided during the presentation. Please write them down – **we will not provide them again via GoToWebinar or email (no exceptions).**
- Please complete the electronic survey that will appear automatically at the **end of the webinar.**
- Attendees seeking CPE for this presentation must complete the survey and **enter all three CPE words.** You cannot claim CPE unless we receive a completed evaluation with the correct words.
- This presentation will be recorded and made available to download at www.grfcpa.com/webinars.
- Technical questions about the survey can be addressed to Nathan McElveen at nmcelveen@grfcpa.com.

Housekeeping

Additional Information

Learning Objective To provide an overview of risk oversight and techniques to identify and combat risk within your organization	Instructional Delivery Methods Group Internet-based
Recommended CPE 1.0 CPE Credit	Recommended Fields of Study Accounting – Technical
Prerequisites None required	Advance Preparation None
Program Level Basic	Course Registration Requirements None
Refund Policy No fee is required to participate in this session.	Cancellation Policy In the event that the presentation is cancelled or rescheduled, participants will be contacted immediately with details.
Complaint Resolution Policy GRF CPAs & Advisors is committed to our participants' 100% satisfaction and will make every reasonable effort to resolve complaints as quickly as possible. Please contact kdavis@grfcpa.com with any concerns.	
Disclaimer This webinar is not intended as, and should not be taken as, financial, tax, accounting, legal, consulting or any other type of advice. Readers and users of this webinar information are advised not to act upon this information without seeking the service of a professional accountant.	

Firm Background

Today's Presenters



Melissa Musser, CPA, CITP, CISA

Principal, Risk & Advisory Services | mmusser@grfcpa.com

GRF CPAs & Advisors



Alex McNeill, PMP

Enterprise Risk Manager | alexmceill@bridgestoprosperty.org

Bridges to Prosperity

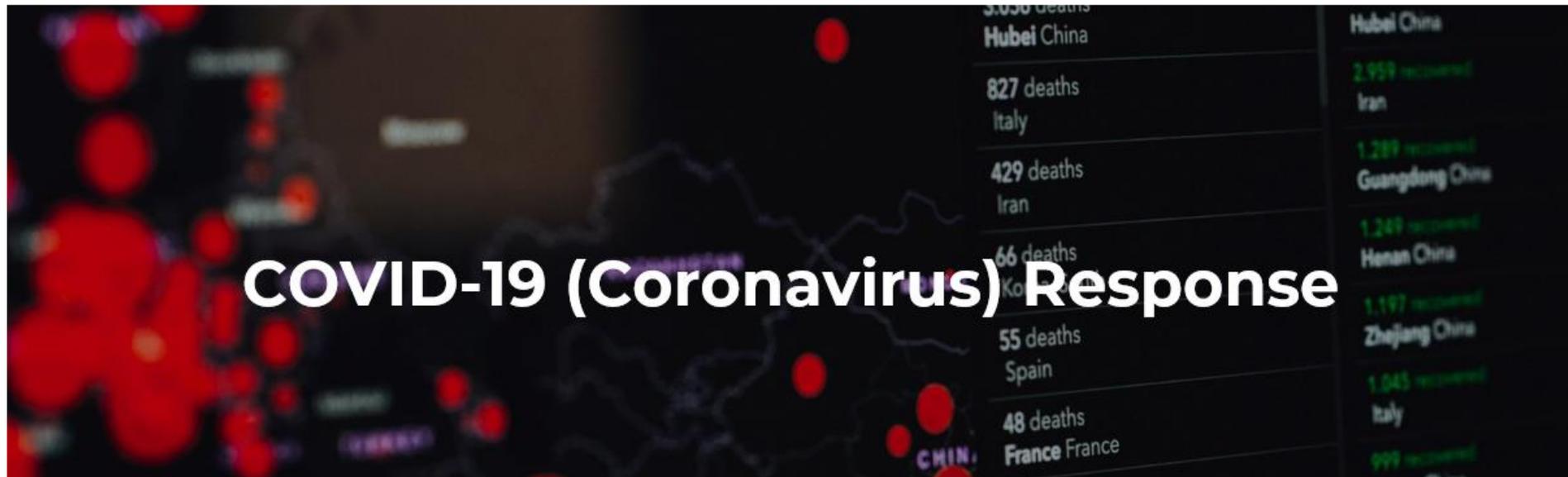
Firm Background

GRF's COVID-19 Response Resource Page



SEARCH 🔍

About ▾ Services ▾ Specialties ▾ Careers ▾ Contact ▾ Resources ▾



<https://www.grfcpa.com/resources/covid-19-coronavirus-response/>



Firm Background

Annual Partnership with NC State

- GRF formed a strategic partnership with North Carolina State (NC State) University's [Poole College of Management's Enterprise Risk Management \(ERM\) Initiative](#)
- Powerful insights and tailored ERM consulting to tax-exempt organizations including public charities, private foundations, associations, international NGOs and colleges and universities
- The partnership complements the growth of the firm's [Risk & Advisory Services](#) practice as it focuses on providing comprehensive business management solutions to nonprofit clients.



**2019 ERM in Nonprofits 2-Day Workshop
NC State, Raleigh**

Agenda

Topics to be Discussed

- Firm Background
- Understanding the Need for Better Risk Oversight
- Techniques for Identifying Risk & Top Forecasted Risks
- Techniques for Assessing & Communicating Risk
- Developing Next Steps

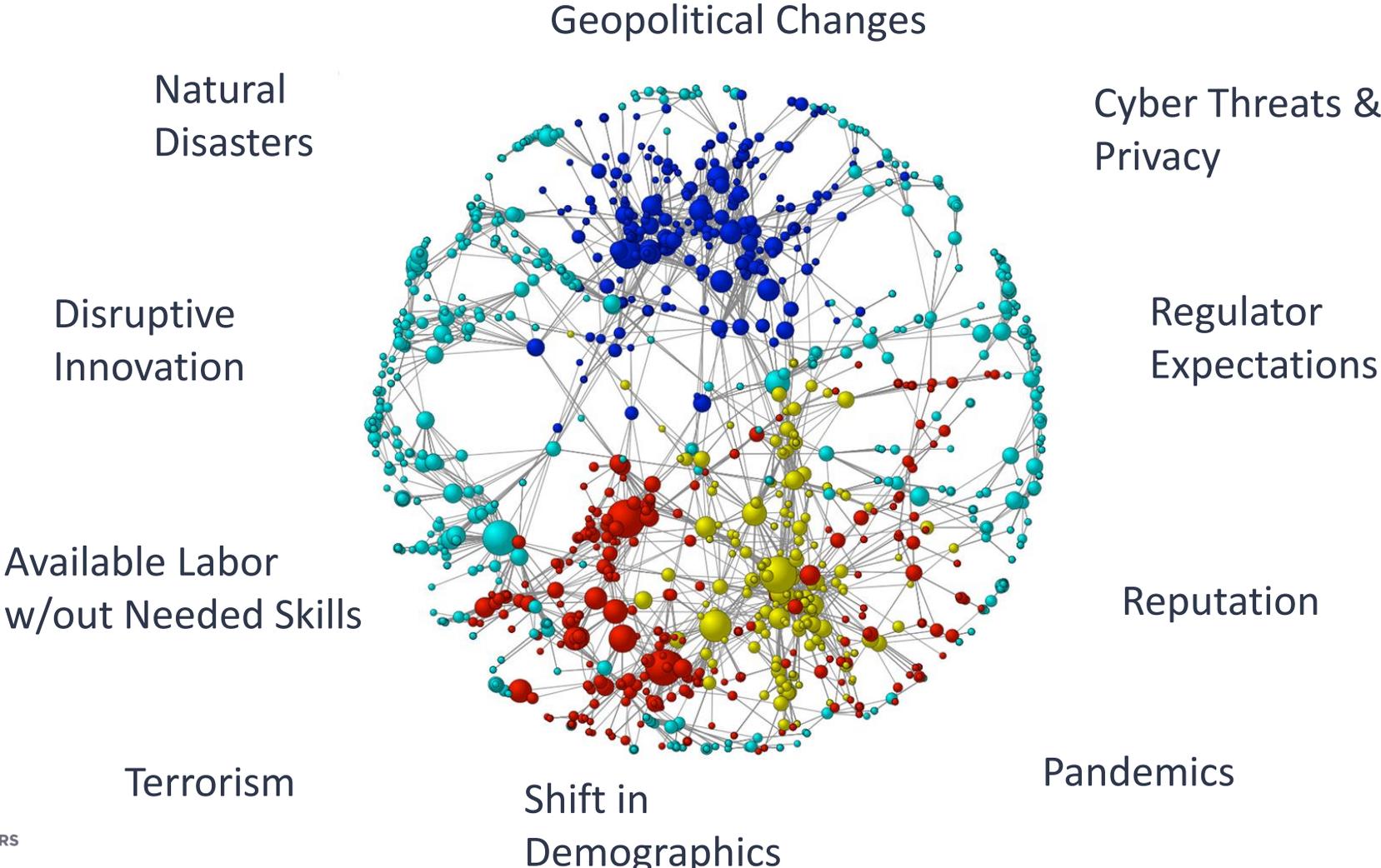
Understanding the Need for Better Risk Oversight



CPAs & ADVISORS

Understanding the Need for Better Risk Oversight

Growing Uncertainty



Understanding the Need for Better Risk Oversight

Early Examples



Understanding the Need for Better Risk Oversight

Traditional Approach to Risk Management



“Silo” or “Stove-Pipe” Risk Management

Understanding the Need for Better Risk Oversight

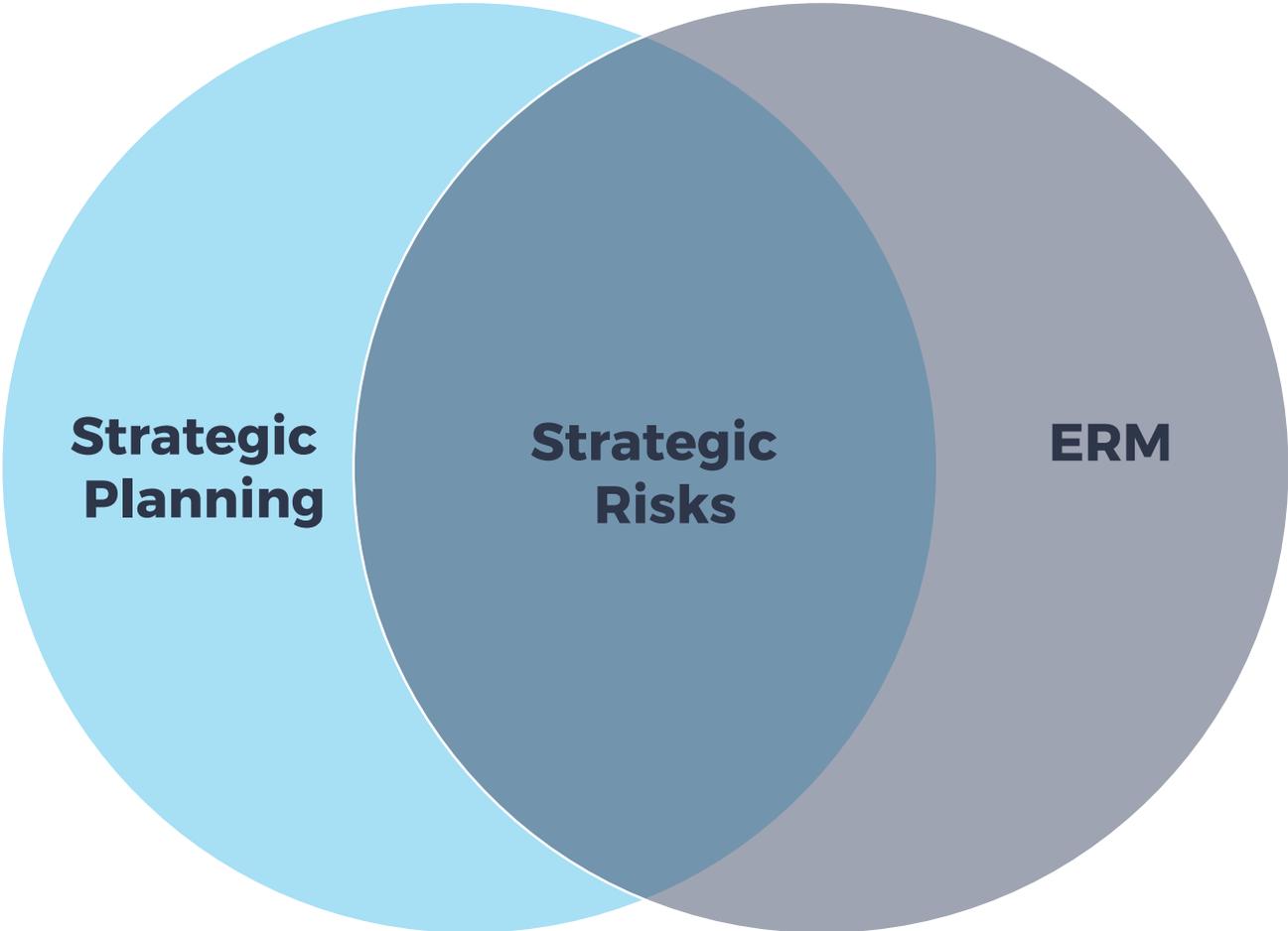
Traditional vs. Enterprise Risk Management

Traditional Risk Management	Enterprise Risk Management
Insurable	Not necessarily covered by insurance
One-dimensional assessment (potential impact)	Multi-dimensional assessment
Manages risks one-by-one	Analyzes material risks and how they relate
Occurs within one business unit (siloed)	Spans the entire organization (holistic)
Reactive and sporadic	Proactive and continuous
Considers only downside (loss)	Considers both upside and downside
Focuses solely on loss prevention	Focuses on business goals, adding value and more
Disjointed activities	Embedded in culture and mindset

<http://erminsightsbycarol.com/traditional-risk-management-erm-differences/>

Understanding the Need for Better Risk Oversight

Intersection of Risk and Strategy



Understanding the Need for Better Risk Oversight

ERM Frameworks



Understanding the Need for Better Risk Oversight

State of Risk Oversight

Enterprise Risk Management Survey

Data was collected through an online survey instrument electronically sent to members of the AICPA's Business and Industry group who serve in Chief Financial Officer or equivalent senior executive positions.

- 142 large organizations (those with revenues greater than \$1 billion)
- 126 publicly-traded companies
- 119 financial services entities
- **107 not-for-profit organizations**



<https://www.aicpa.org/content/dam/aicpa/interestareas/businessindustryandgovernment/resources/erm/downloadabledocuments/aicpa-erm-research-study-2019.pdf>

Polling Question #1

Do you have some form of ERM implemented at your organization?

- A. *Not at this time*
- B. *Considering*
- C. *Yes or Partially implemented*
- D. *Unsure*

Understanding the Need for Better Risk Oversight

Why is ERM on the Rise?

Percentage of Respondents Selecting “Mostly” or “Extensively”						
Factors “Mostly” or “Extensively” Leading to Increased Senior Executive Focus on Risk Management Activities	Full Sample	Largest Organizations (Revenues > \$1B)	Public Companies	Not-for-Profit Organizations 2017	Not-for-Profit Organizations 2018	Not-for-Profit Organizations 2019
Regular Demands	31%	34%	44%	22%	24%	17%
Unanticipated risk events affecting organization	32%	36%	40%	37%	37%	32%
Emerging best practice expectations	38%	33%	37%	41%	53%	41%
Emerging corporate governance	29%	32%	37%	20%	24%	19%
Board of Director requests	32%	43%	44%	25%	25%	39%

<https://www.aicpa.org/content/dam/aicpa/interestareas/businessindustryandgovernment/resources/erm/downloadabledocuments/aicpa-erm-research-study-2019.pdf>



Understanding the Need for Better Risk Oversight

Current State of ERM

Percentage of Respondents				
Description of the State of ERM Currently in Place	Full Sample	Not-for-Profit Organizations 2017	Not-for-Profit Organizations 2018	Not-for-Profit Organizations 2019
No enterprise-wide management process in place	12%	17%	9%	7%
Currently investigating concept of enterprise-wide risk management, but have made no decisions yet	9%	11%	13%	8%
No formal enterprise-wide risk management process in place, but have plans to implement one	8%	9%	11%	12%
Partial enterprise-wide risk management process in place (i.e., some, but not all, risk areas addressed)	40%	44%	40%	48%
Complete formal enterprise-wide risk management process in place	31%	19%	27%	25%

<https://www.aicpa.org/content/dam/aicpa/interestareas/businessindustryandgovernment/resources/erm/downloadabledocuments/aicpa-erm-research-study-2019.pdf>

Understanding the Need for Better Risk Oversight

Who is Responsible for Risk Oversight?

Percentage of Respondents					
If Board delegates formal responsibility of risk oversight to a subcommittee, which committee is responsible?	Full Sample	Largest Organizations (Revenues > \$1B)	Public Companies	Financial Services	Not-for-Profit Organizations
Audit Committee	48%	56%	47%	38%	64%
Risk Committee	27%	19%	34%	44%	12%
Executive Committee	10%	11%	9%	7%	5%

<https://www.aicpa.org/content/dam/aicpa/interestareas/businessindustryandgovernment/resources/erm/downloadabledocuments/aicpa-erm-research-study-2019.pdf>

Understanding the Need for Better Risk Oversight

Who Does the Chief Risk Representative Report to?

Percentage of Respondents					
To Whom Does the CRO Formally Report?	Full Sample	Largest Organizations (Revenues > \$1B)	Public Companies	Financial Services	Not-for-Profit Organizations
Board of Directors or Committee of the Board	20%	11%	26%	24%	12%
Chief Executive Officer or President	48%	42%	43%	53%	44%
Chief Financial Officer	18%	29%	19%	14%	23%

<https://www.aicpa.org/content/dam/aicpa/interestareas/businessindustryandgovernment/resources/erm/downloadabledocuments/aicpa-erm-research-study-2019.pdf>



Polling Question #2

Where does risk oversight sit at the board level?

- A. *Board of directors*
- B. *Audit committee*
- C. *Finance committee*
- D. *Other risk committee*
- E. *Unsure*

Techniques for Identifying Risk & Top Forecasted Risks



CPAs & ADVISORS

Techniques for Identifying Risk/Top Forecasted Risks

Organizations Often Start by Asking . . .

- *What keeps you awake at night?*

-or-

- *Given your functional area, please identify risks within your area (e.g.):*

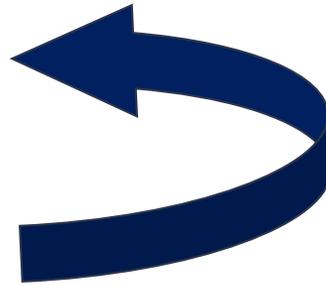
- IT Risks
- Compliance
- Supply Chain
- Legal Risks
- Liquidity
- Staffing/Human Resources

Source: NC State ERM Initiative

Techniques for Identifying Risk/Top Forecasted Risks

Focus Tends to be on the “Known Risks”

- *Known, Knowns*
- *Unknown, but Knowable*
- *Unknown, Unknowable*



Source: NC State ERM Initiative

Techniques for Identifying Risk/Top Forecasted Risks

Discussion

- How does your organization ensure that the focus is not simply on “known” or everyday risks?
- What has (or hasn’t) worked in moving the conversation beyond “everyday risks?”



Source: NC State ERM Initiative

Techniques for Identifying Risk/Top Forecasted Risks

Questions to Consider: Risk To Strategy

Think about factors that might prevent a critical aspect of the strategy from going right.

- Key technologies, key people, key processes that might not go as planned
- Internal obstacles?
- External obstacles?

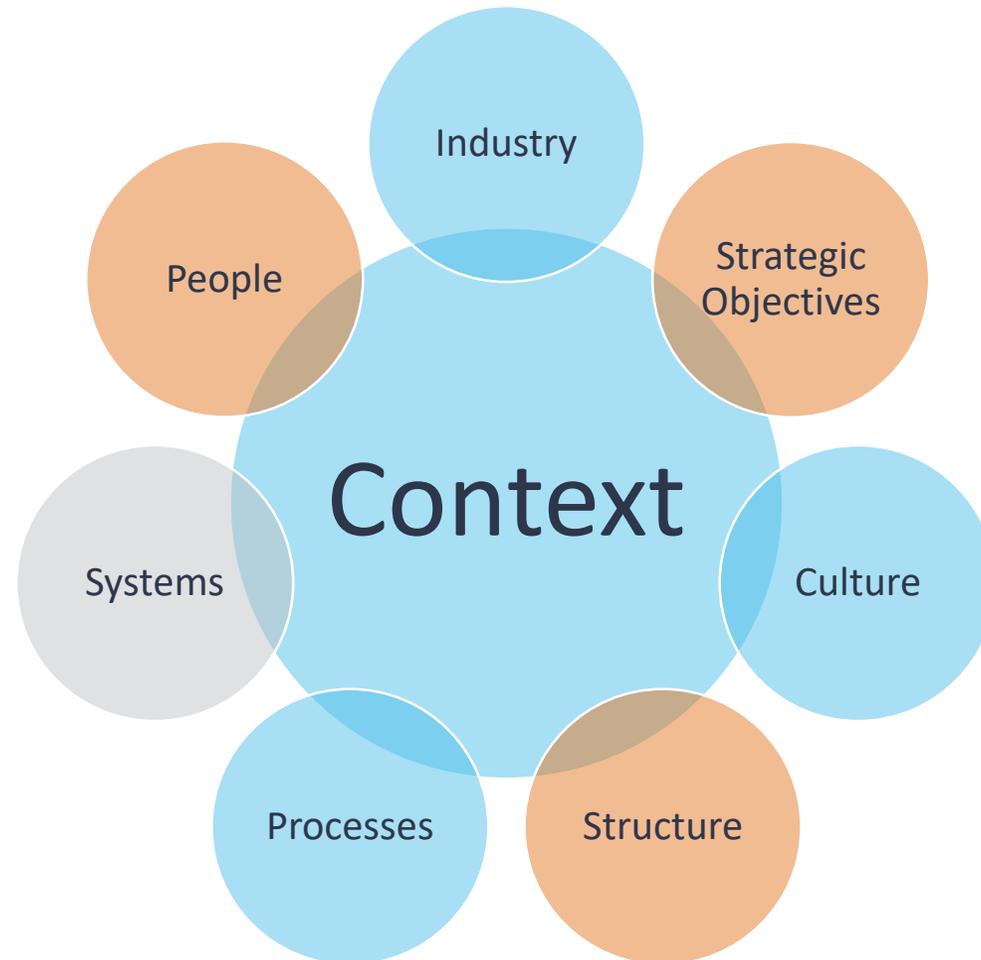
Focus on the key assumptions and consider the following:

- How sound is the assumption?
- How likely are underlying factors supporting the assumption to change and how fast might changes occur?
- What is the process we are using to monitor/update the assumption?

Source: NC State ERM Initiative

Techniques for Identifying Risk/Top Forecasted Risks

Understand the Organizational Context



Techniques for Identifying Risk/Top Forecasted Risks

Key Risk Identification Techniques



Techniques for Identifying Risk/Top Forecasted Risks

Risk Universe

Categories

Management and
Operational Risk

Financial and
Fraud Risk

External,
Collaboration and
Reputation Risk

Legal and
Compliance Risk

Personnel and
Volunteer Risk

IT Risk

Strategic and
Governance Risk

Third-Party
Vendor Risk

Environmental,
Health and
Human Safety

Polling Question #3

What does your organization see as a top risk for 2021?

- A. *Strategy transformation / Business continuity / Disaster recovery*
- B. *Cyber threats / Privacy / Information security management / Digital transformation*
- C. *Finance / Fraud / Corruption*
- D. *Culture / HR / Talent management*
- E. *Other*

Techniques for Identifying Risk/Top Forecasted Risks

Top Forecasted Risks

**Strategy/
Transformation**

**Cyber Threats/Privacy
and Information
Security Management**

**Culture/HR/Talent
Management**

Fraud/Corruption

**Environmental,
Social, and
Governance (ESG)**

**Business Continuity/
Disaster Recovery/
Third Party Risk**

Source: NC State ERM Initiative

Techniques for Assessing & Communicating Risks



CPAs & ADVISORS

Techniques for Assessing & Communicating Risk

Risk Assessment Considerations

- Need guidance for consistency across organization
- Keep it simple; understandable
- Create a common scale for different types of impacts

Techniques for Assessing & Communicating Risk

Likelihood Scale Example

	RARE	UNLIKELY	POSSIBLE	LIKELY	ALMOST CERTAIN
Description	The event may occur only in exceptional circumstances	This event could occur at some time	The event should occur at some time	The event will probably occur in most circumstances	The event is expected to occur in most circumstances
Frequency	Less than once in 10 years	Will occur once every 5 to 10 years	Will occur once every 1 to 5 years	Will occur once every year	Will occur more than once a year

Techniques for Assessing & Communicating Risk

Impact Scale Example

	INSIGNIFICANT	MINOR	MODERATE	MAJOR	CATASTROPHIC
Injury	No injuries	Employee loss time injury	A single event involving serious injury and/or multiple employee lost time injury	A single event involving death and/ or multiple injuries as a direct result of ORG negligence and/or single employee death or multiple injuries	Two or more events involving death and/or multiple injuries as a direct result of ORG negligence and/or multiple employee deaths
Financial	Loss of assets or revenue less 4%	Loss of assets or revenue of 5% to 9%	Loss of assets or revenue of 10% to 24%	Loss of assets or revenue of 25% to 49%	Loss of assets or revenue exceeding 50%
Media / Reputation	Local newspaper headline (not front page)	Local television/ newspaper headlines (front page)	State television/ newspaper headlines	In-country television/ newspaper headlines	Global television/ newspaper headlines
Compliance		Regulatory Inquiry	Regulatory Investigation	Government Investigation	Global Agency Investigation
Operational	Minor service disruption	Business interruption over 12 hours	Total service cessation for a period of 1 to 2 days and subsequent interruption over several days	Total service cessation for a period of 2 to 3 days and subsequent interruption over several weeks	Total service cessation for more than 1 week

Techniques for Assessing & Communicating Risk

Types of Risk Impact



Techniques for Assessing & Communicating Risk

Example Likelihood and Impact Matrix

Impact	Likelihood				
	Rare - 1	Unlikely - 2	Possible - 3	Likely - 4	Certain - 5
Catastrophic - 5	Moderate - 5	Moderate - 10	High - 15	Critical - 20	Critical - 25
Major - 4	Low - 4	Moderate - 8	Moderate - 12	High - 16	Critical - 20
Moderate - 3	Low - 3	Moderate - 6	Moderate - 9	Moderate - 12	High - 15
Minor - 2	Very low - 2	Low - 4	Moderate - 6	Moderate - 8	Moderate - 10
Insignificant - 1	Very low - 1	Very low - 2	Low - 3	Low - 4	Moderate - 5

Techniques for Assessing & Communicating Risk

Determine Risk Response



Techniques for Assessing & Communicating Risk

Risk Register Tracking Technique

RISK ID#	Title	Impact Description	Status	Strategic Objective	Risk Category	Impact 1=Low, 5= Hi	Likelihood 1=Low, 5=Hi	Risk Owner	Owner	Risk Response	Risk Response Summary	Date Closed	Closed Reason
----------	-------	--------------------	--------	---------------------	---------------	---------------------	------------------------	------------	-------	---------------	-----------------------	-------------	---------------

RISK ID#	Title	Impact Description	Status	Strategic Objective	Risk Category	Impact 1=Low, 5= Hi	Likelihood 1=Low, 5=Hi	Risk Owner	RISK ID#	Title	Impact Description	Status	Strategic Objective	Risk Category
RISK ID#	Title	Impact Description	Status	Strategic Objective	Risk Category	Impact 1=Low, 5= Hi	Likelihood 1=Low, 5=Hi	Risk Owner	RISK ID#	Title	Impact Description	Status	Strategic Objective	Risk Category
RISK ID#	Title	Impact Description	Status	Strategic Objective	Risk Category	Impact 1=Low, 5= Hi	Likelihood 1=Low, 5=Hi	Risk Owner	RISK ID#	Title	Impact Description	Status	Strategic Objective	Risk Category
RISK ID#	Title	Impact Description	Status	Strategic Objective	Risk Category	Impact 1=Low, 5= Hi	Likelihood 1=Low, 5=Hi	Risk Owner	RISK ID#	Title	Impact Description	Status	Strategic Objective	Risk Category

Techniques for Assessing & Communicating Risk

Monitor and Report

Management Handling Plans

RISK STATEMENT		DATES		
Cause		Status	Open	
Risk		Opened		
Impact		Approved		
Management effectiveness score		Closed		
RISK CLASSIFICATION		HANDLING PLAN		
Executive Owner		Description of Task	Owner	Status
Risk Manager				
Handling Approach	Mitigate			
INHERENT RISK RATING	CURRENT	TARGET		
Impact Rating (1-5)				
Likelihood Rating (1-5)				
Risk Score				
INTERRELATED TOP ENTERPRISE RISKS				

Independent Assurance



Techniques for Assessing & Communicating Risk

Monitor and Report

KPI vs. KRI

KPI - Effectiveness
Act as an decision making tool by providing key dimensions of performance
Provide a backward looking view on past data to identify lessons learned
Signal to management areas where there is a hindrance of the achievement of goals

VS

KRI – Risk Exposure
Act as an input to a risk owner’s risk assessment, thus making the assessment more reliable and informative
Alert management of trends that may adversely affect the achievement of goals or may forecast the likelihood of a risk occurrence
Signal to management if corrective action needs to be taken based on KRI performance

KPI is a **backward** looking indicator, and a **KRI** is a **forward** looking indicator. KPI tracks how well you did, and a KRI attempts to predict where you are going.

Practical Implementation



CPAs & ADVISORS

Practical Implementation of the ERM Framework

Understanding the Need for Better Risk Oversight

- Bridges to Prosperity (B2P): International NGO that engages governments around the world to build footbridges to improve rural infrastructure = High Risk Environment
- As the organization prepared to scale its operations, the need for improved risk oversight was identified by the BoD and Senior Leadership
- The creation of an ERM framework began in August, 2019 and we began working with GRF in February, 2020.
- Often “Risk” may be seen as adding bureaucracy or “slowing things down” however...

Practical Implementation of the ERM Framework

Understanding the Need for Better Risk Oversight

Q: Why does a car have brakes?

A: To stop?

NO! A car has brakes so you can go FAST. Imagine if you had a car without brakes – and you knew it.

How fast would you go?

Quote: John Reed, Former Citigroup CEO

Practical Implementation of the ERM Framework

Techniques for Identifying Risk/Top Forecasted Risks



ERM Framework

Next Steps – COVID-19 Response

- Finished our first org-wide risk assessment in February, 2020
- We did not have “Global Pandemic” on that list but we did have Ebola
 - Similar mitigation strategies and our team were prepared to implement additional measures
- Examples of other mitigations identified in the assessment
 - Create a more diverse revenue portfolio
 - Re-examine international travel protocols
- Other “softer” changes
 - Noticed a change in the way our teams were talking about risk

ERM Framework

Next Steps – Supporting Strategic Growth and Creating Resilience

- Second time round with the risk assessment – the environment has shifted slightly...
- Established our risk council, committee, engagement from BoD and departments within the organization
- Integrating our ERM framework into strategic decision making so that it is not seen as add-on rather, the way in which we achieve our objectives
 - Creates business resilience and continuity
 - Generates confidence within our teams and among our larger stakeholder groups

ERM Framework

Key Take Aways

- What I would have loved to know before starting this process:
 - ERM is iterative – you will not get it right the first time (or even the second)
 - Art not a Science!
 - There are so many ways to do this and everyone has their own opinion:
 - Use best practice: ISO31000, COSO
 - Do your research but get support from a reliable source
 - Be open to learn and update the process as you create and implement – don't let perfection be then enemy of done.
- ERM drives and supports strategy and organizational growth
- Having brakes allows you to move fast **AND** to be safe, informed, responsible and compliant at the same time

Developing Next Steps



CPAs & ADVISORS

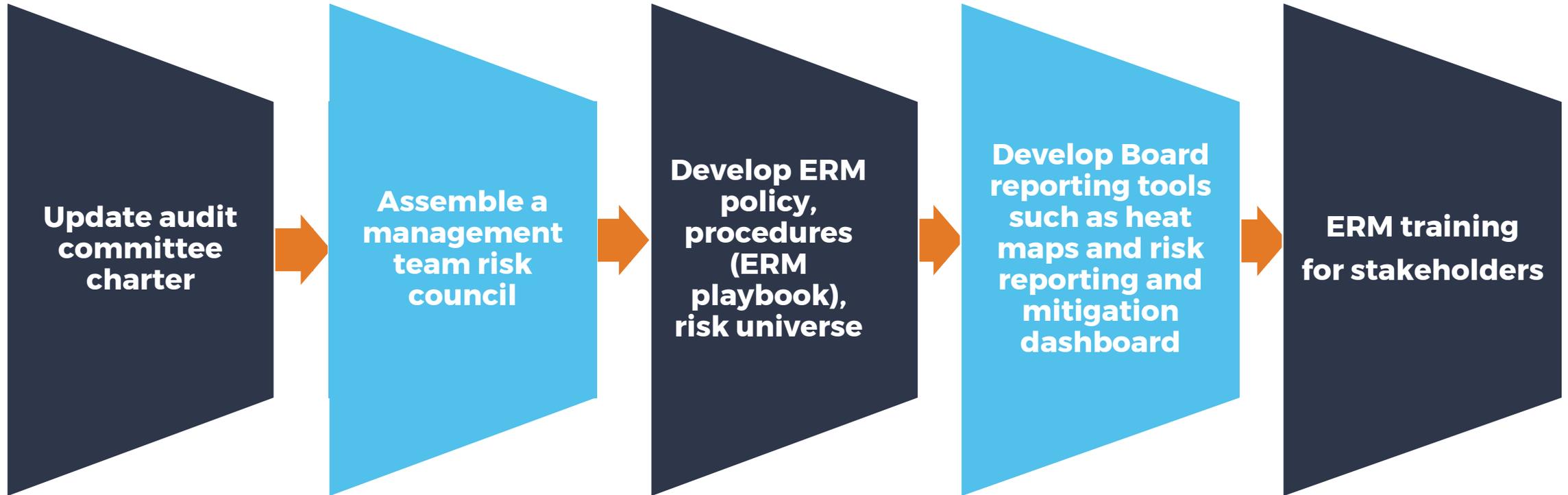
Developing Next Steps

Benefits of Enterprise Risk Management



Developing Next Steps

Critical Success Factors



Developing Next Steps

Developing Procedures

- Develop and document procedures for conducting risk assessments and develop templates and tools to facilitate and standardize the process
- The procedures generally contain the following information:

Who is responsible for initiating and conducting risk assessments

Who will participate

What steps will be followed

How disagreements will be handled and resolved

What approvals will be needed

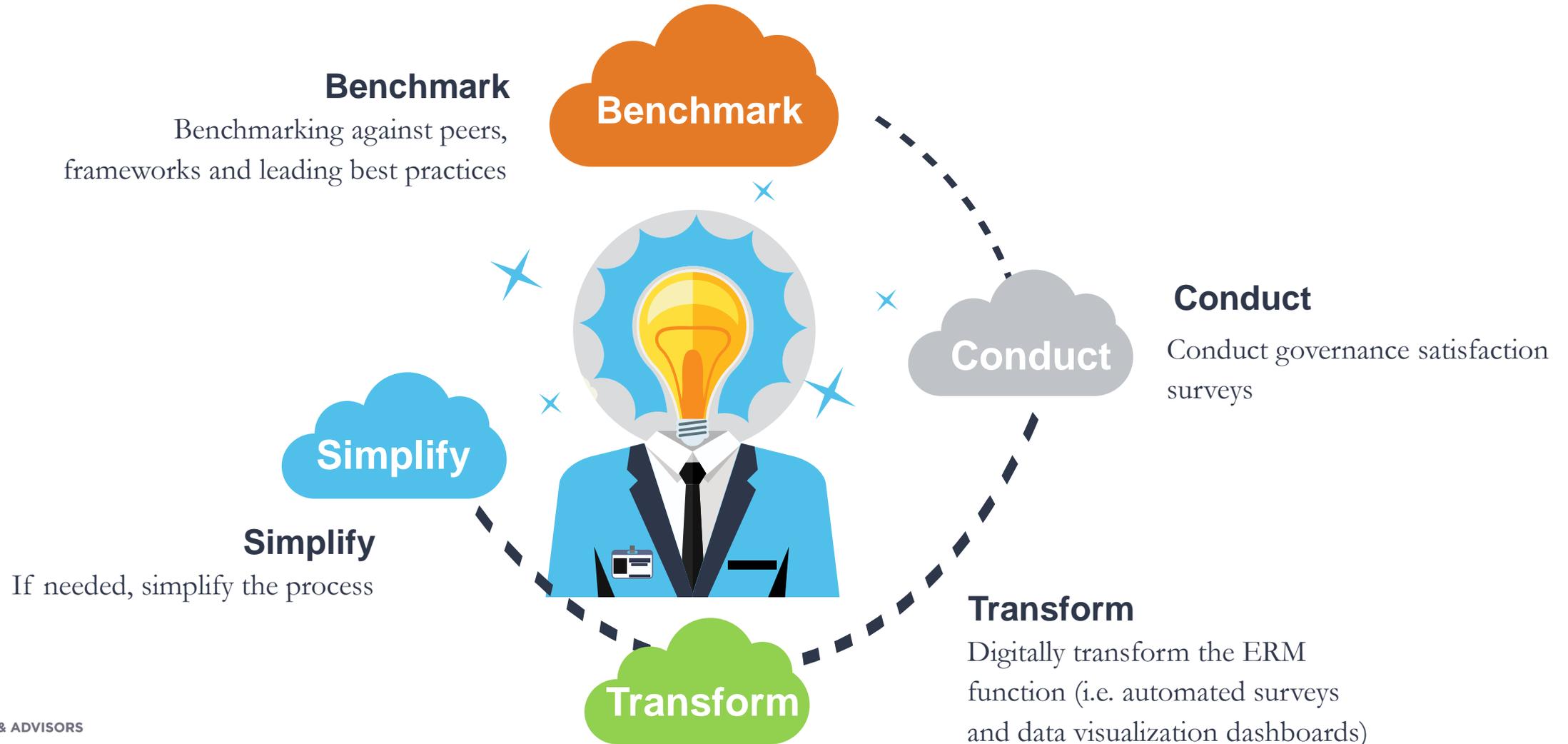
How assessments will be documented

How documentation will be maintained

To whom reports will to be provided

Developing Next Steps

ERM Maturity



Developing Next Steps

Questions to Ask

Do we know our key risks?

Do we have effective risk reporting for executive management and the Board?

Are we accepting the right level of risk?

Do we know if our risks are being properly managed?

Do we have a comprehensive risk framework in place?

Are we focused on the risks that matter?

Do we have duplicative or overlapping risk functions?

Are we leveraging automated controls versus manual controls?

Do we have the right mix of skills at the right cost?

Have we optimized the use of technology to manage risk?

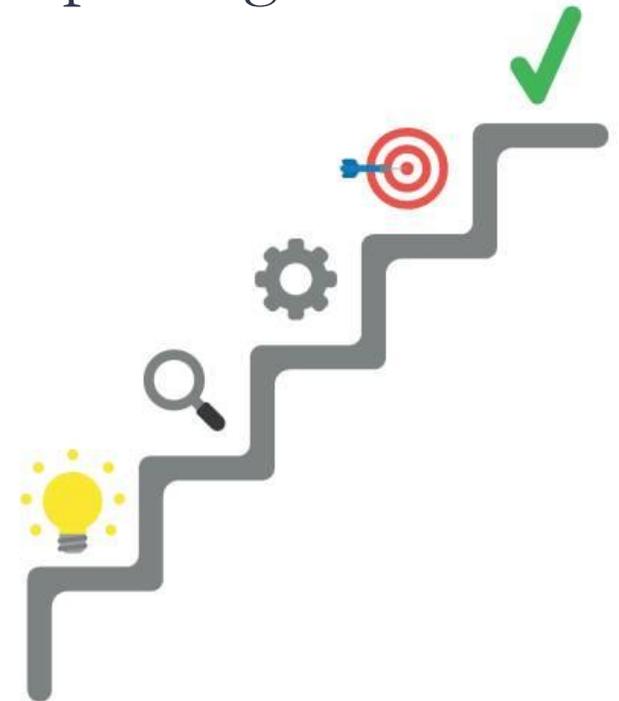
Are the risks we take aligned to our business strategies and objectives?

Is risk management slowing us down or helping us go faster?

Developing Next Steps

Questions to Ask

- Get the conversation started ... What keeps the Board up at night?
- Attend specialized training
- Obtain senior management approval and involvement
- Designate committees or individuals to champion
- Develop procedures
- Involve business and technical experts
- Formalize risk reporting to the board



Questions

Thank you!



CPAs & ADVISORS



Bethesda | New York

877-437-4771 | www.grfcpa.com



Melissa Musser, CPA, CITP, CISA

Principal

mmusser@grfcpa.com



Alex McNeill, PMP

Enterprise Risk Manager

alexmceill@bridgestoprosperty.org

Disclaimer

This webinar is not intended as, and should not be taken as, financial, tax, accounting, legal, consulting or any other type of advice. While we use reasonable efforts to furnish accurate and up-to-date information, we do not warrant that any information contained in or made available in this presentation is accurate, complete, reliable, current or error-free. We assume no liability or responsibility for any errors or omissions in the content of this presentation.

The use of the information provided in this presentation does not establish any contractual or other form of client engagement between GRF CPAs & Advisors and the reader or user. Any U.S. federal tax advice contained in this presentation is not intended to be used for the purpose of avoiding penalties under U.S. federal tax law. Readers and users of this presentation information are advised not to act upon this information without seeking the service of a professional accountant.