Crowe

Smart decisions. Lasting value.™

Sustainable ERM in the Public Sector Part One

Presented by Bill Dykstra

August 9, 2018

Housekeeping

- Please note that all of today’s audio is being broadcast to your computer speaker
- Please submit questions through the Q&A function on your screen. Questions will be addressed at the end of the presentation.
- To download a copy of the presentation or access the resources connected to this session, please visit the resources icon at the bottom of your console

Click the resource icon below to download slides

CPE Details

CPE Credit

- Login individually to the session
- Minimum of 60 minutes on the session
- Successfully complete 3 of the 4 polling questions

NO CPE Credit

- Fail to successfully complete 3 of the 4 polling questions
- Viewing a recording of this session (CPE is only awarded for live sessions)

Upon completion of this program you will receive a post event evaluation

Your feedback is important

- CPE certificate of completion
- E-mailed within two weeks of upon successfully passing this program

Crowe

Smart decisions. Lasting value.™

Sustainable ERM in the Public Sector Part One

Presented by Bill Dykstra

July 27, 2018

Introduction

Bill Dykstra
CRMA, CIA

Mr. Dykstra specializes in enterprise risk management in Crowe's Public Sector Risk unit. He has an internal audit background with 16 years of experience serving public and not-for-profit organizations. During his career, Bill has managed a wide-variety of initiatives which included developing a tailored ERM framework for a not-for-profit organization.

Since joining Crowe in May 2016, Bill has focused on promoting ERM in government, not-for-profit, and higher education organizations. This has included leading several enterprise risk assessment workshops at colleges and universities. It has also involved developing ERM training materials for a not-for-profit professional organization, supporting an initiative to create a new professional certification for ERM professionals in the federal government.

Bill is also a frequent presenter on the topic of ERM at various professional association and internal training events.

Learning Objectives

At the end of this webinar, you should be able to:

- Understand the key components and activities needed to implement ERM according to COSO and the federal Office of Management and Budget (OMG Circular A-123) guidelines.
- Obtain examples and templates to use to validate and communicate that these foundational components are in place.
- Obtain tools for building cost-effective and efficient ERM practices, not only for compliance purposes, but to add value to the agency and its strategic pursuits.

Agenda

- Enterprise Risk Management Basics
- The ERM Implementation Process
  - Establish a Charter
  - Establish the Structure
  - Establish Context
  - Identify Risks
  - Create the Risk Profile
  - Analyze and Evaluate
  - Develop Alternatives
  - Respond to Risks
- Conclusion

Polling Question #1

- How would you rate the maturity level of your organization’s ERM program?
  - Level 1: Nascent. Lacks formal process, communication or monitoring. Risks are addressed ad hoc.
  - Level 2: Emerging. Roles/responsibilities defined; governance established; risk assessment process in place.
  - Level 3: Integrated. Endorsed by leadership; policies/procedures defined; risks are shared across silos.
  - Level 4: Predictive. Program recognized organization-wide; comprehensive policies/procedures in place; risks are identified and assessed qualitatively
  - Level 5: Advanced. Risk discussion embedded in strategic planning; thresholds are established to trigger warning when risks exceed threshold; learning from past events incorporated into future preparation.

Enterprise Risk Management Basics

What is Enterprise Risk Management?

- Various definitions
  - “It is the culture, capabilities, and practices that organizations integrate with strategy-setting and apply when they carry out that strategy, with a purpose of managing risk in creating, preserving, and realizing value. “

    (Enterprise Risk Management Integrating with Strategy and Performance, COSO, 2017)

  - “Coordinated activities to direct and control an organization with regard to *risk.”*

    (ISO 31000, International Standards Organization, 2018)

Enterprise Risk Management Basics

- ERM provides an enterprise-wide, strategically-aligned portfolio view of organizational challenges that provides improved insight about how to more effectively prioritize and manage risks to mission delivery.
- Effective ERM helps agencies implement strategies to ensure effective use of resources, enable an optimized approach to the identification and remediation of compliance issues, and promote reliable reporting and monitoring across business units.
- An ERM framework allows agencies to increase risk awareness and transparency, improve risk management strategies, and align risks to each agency’s risk appetite and risk thresholds.
  - Risk Appetite is the articulation of the amount of risk an organization is willing to accept in pursuit of strategic objectives.
  - Risk Tolerance is the acceptable level of variance in performance relative to the achievement of objectives.

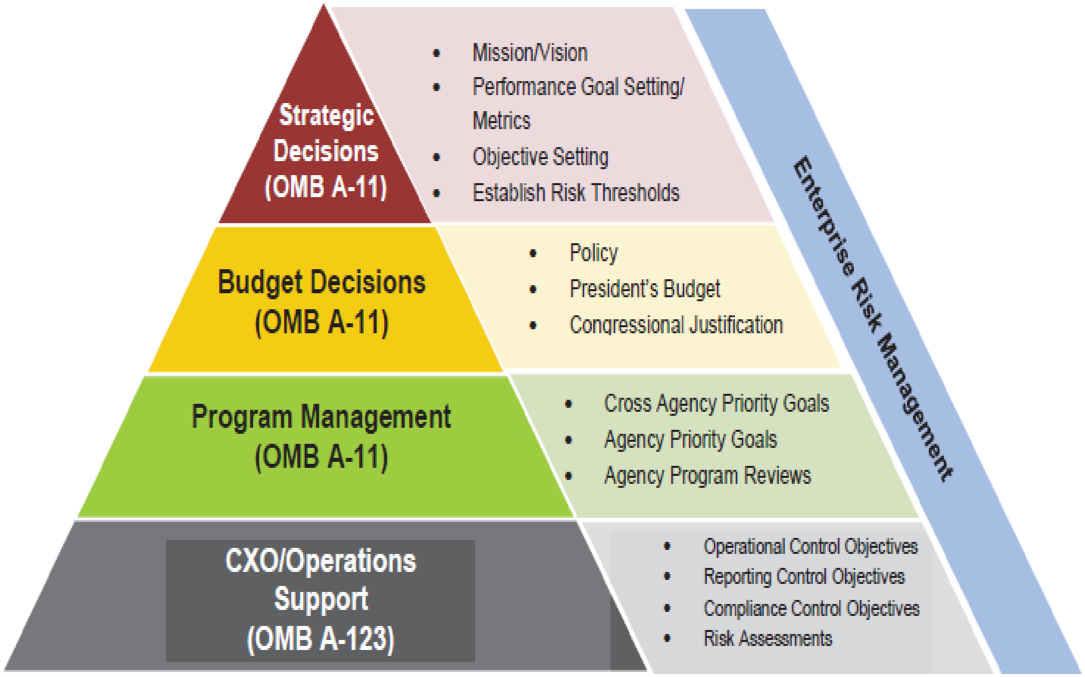
Commonly Used Frameworks

- Not a requirement
- Helpful guide to
  - Educate management and the board
  - Establish shared terminology
  - Establish a starting point for a tailored approach
  - Identify avoid pitfalls to implementation
  - Establish the RM process based on best practices

- Most widely recognized and accepted frameworks
  - COSO
  - ISO 31000

OMB Circular A-123

- This circular provides guidance to Federal managers on improving the accountability and effectiveness of Federal programs and operations by establishing, assessing, correcting, and reporting on internal control.
- A-123 encourages agencies to establish a governance structure, including a Risk Management Council or Committee; require the development of “Risk Profiles” to identify major risks arising from mission and mission-support operations; and analyze those risks in relation to achievement of strategic objectives.


Strategic Decisions (OMB A-11)
• Mission/Vision
• Performance Goal Setting/ Metrics
• Objective Setting
• Establish Risk Thresholds
Budget Decisions (OMB A-11)
• Policy
• President's Budget
• Congressional Justification
Program Management (OMB A-11)
• Cross Agency Priority Goals
• Agency Priority Goals
• Agency Program Reviews
CXO/Operations Support (OMB A-123)
• Operational Control Objectives
• Reporting Control Objectives
• Compliance Control Objectives
• Risk Assessments
Enterprise Risk Management

Polling Question #2

Which framework has your organization used in developing its ERM program?

1. COSO – ERM
2. ISO – 31000
3. OMB A-123 or “the Playbook”
4. Something else or multiple sources
5. I don’t know

The ERM Implementation Process

Establish a Charter

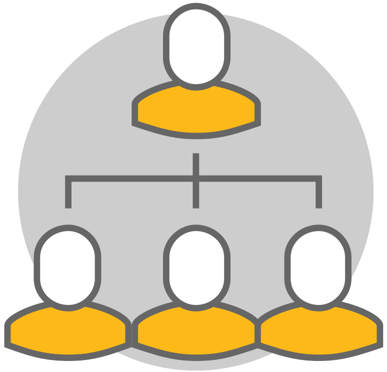
- An ERM Charter is an effective means to
  - Formally document expected outcomes and goals for the program
  - Identify key individuals and governance structures and their roles
  - Communicate those roles and responsibilities to the key stakeholders and throughout the organization
- A Board-approved charter will help establish
  - The importance of ERM within the organization
  - Accountability for those involved
  - A reporting channel through which to report progress and modify direction

Establish a Charter (continued)

- Charters should be tailored to fit the organization’s needs and culture.
- Basic components should include:
  - Purpose of ERM
  - Scope
  - Roles and Functional Activities
  - Levels of Authority, Staffing, and Reporting Channels
  - Risk Management Approach
    - Frameworks, Rules or Regulations

Establish the Structure

- Risk Management Committee
  - Typically composed of executive leadership
  - May report to the Board or Board committee
  - Should also have a charter to specify the committee’s
    - Purpose and Objectives
    - Structure and Members (e.g. CRO, CFO, COO, etc.)
    - Authority
    - Roles and Responsibilities
    - Key Functional and Reporting Activities



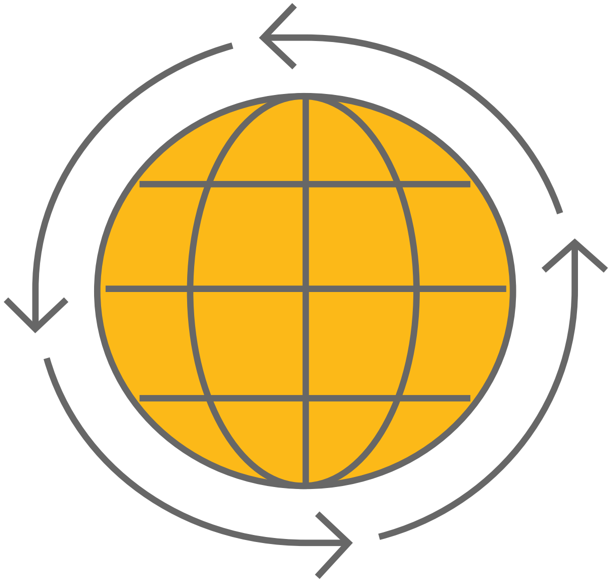
Polling Question #3

Does your organization have a formal ERM Charter or Risk Management Committee charter?

1. ERM Charter
2. Risk Management Committee Charter
3. Both
4. Neither

Establish Context

- Effective risk management needs to give full consideration to the context in which the organization functions and to the risk aspects of partner organizations.
- The risk context includes all factors that affect the ability of an agency to achieve its stated mission and program objectives, both internal and external.
- Factors may include but is not limited to Congress, the economy, the agency's capacity, legal and compliance structures, dependency on partner organizations and taxpayers.
- Understanding and defining the context will inform and shape successive stages of ERM implementation



Establish Context (continued)

- Key Steps in Defining Context When Applying Risk Management Principles

Risk Tolerance and Risk Appetite	Having a current and accurate perspective on an organization and decision makers' risk tolerance and risk appetite will help shape the assessments and the development of actionable risk management alternatives.
Scope & Criticality of the Decisions	Understand the decision or range of decisions that have to be made and the range of options available to leaders. Also consider the breadth and depth of the decision's impact. The risk analysis and effort should be commensurate to that criticality.
Establish Goals & Objectives	Ensure that the goals and objectives for business function or unit are clear in order to ensure identified risks are relevant to those expected outcomes.
Decision Timeframe	Consider the timeframe in which a decision must be made, socialized and executed including time available for conducting formal analysis and decision review.

Establish Context (continued)

- Key Steps in Defining Context When Applying Risk Management Principles

Resource and Risk Management Capabilities	Identify the staffing, budget, skill sets/expertise, and other resources available for successful project completion including risk analysis and risk management efforts. Resources applied should be commensurate with the complexity of the issues involved and the magnitude of the decision.
Availability and Quality of Information	Consider the availability and quality of information that exists within the Agency or that can be accessed as needed, based on the design of the risk analysis approach, the time available for analysis and other factors. In engaging with decision makers at the outset of a risk based analysis cycle, it is important to convey anticipated data limitations, including expected levels of data availability.
Decision Makers and Stakeholders	Organizational leaders must be engaged at the beginning of a risk management/analysis process so the approach and presentation of results are tailored to their preferences and the analysis is responsive to the breadth of issues upon which they're seeking guidance.
Policies and Standards	Ensure risk management efforts utilize, complement and take into account any risk management policies, standards or requirements the Agency already has in place. The Enterprise Risk Management program is designed to leverage and complement these and other existing processes to identify monitor and mitigate risk.

Identify Risks

- Agencies should use a structured and systematic approach to recognize potential risks and should strive to address all key risks significant to the achievement of organizational objectives.
- After major risks are determined, agencies should examine them and decide which are the most significant risks to the agencies:
  - Prioritize the risks based on likelihood and impact
  - Risk velocity is also something to consider. For example: a disinvestment in a joint venture would take a long time for the risk to come to fruition, but, a systems failure causes harm immediately, and therefore has a much higher risk velocity.

Create the Risk Profile

- How do we identify risks in practice?
  - Agencies can use either a “top down” approach, “bottom up” approach, or both.
  - Interviews and surveys with managers/ subject matter experts
    - These are the people who are closest to operations and are most knowledgeable about the risks faced.
  - As yourself the question: What events could happen that would affect my program areas or objectives?
  - Establishing a **risk profile** is a useful way to summarize all risks and help determine what the most significant risks to the agency are. Below is an example of a risk profile template:

Risk Description	Risk Event	Primary Impact	Threat or Opportunity	Likelihood	Impact Category	Order of Priority	Response Type	Response Strategy

Create the Risk Profile - Case Example

- Federal Agency A has a Risk Management Council (RMC) which consists of an agency leadership (e.g. CFO, General Council, CRO, COO, CIO).
- This multi-disciplinary team provides an organization-wide perspective on both risk identification as well as prioritization. This is how they identify risks:

The Core Team is able to pull together themes that cross business unit/functional area boundaries and use their respective points of view to prioritize these themes into entity level risks based on a strategic, organization-wide perspective. In this way, the RMC serves as a critical transition point from the “silo” perspective of the individual units to the more organization-wide, portfolio view to present to the chief executive and the board.

Risk Profile - Example

- Let’s pretend we are part of the Risk Management Council (RMC) at a government agency, and we are at risk of a data privacy breach.
- How would this risk fit into our risk profile?

Risk Description	Risk Event	Primary Impact	Threat or Opportunity	Likelihood	Impact Category	Order of Priority	Response Type	Response Strategy
Personal identifiable information about our employees or the public has been lost, misused, or stolen.	Data Privacy Breach							

We will continue to fill out this risk profile as we follow the ERM Implementation steps.

Analyze and Evaluate

- Once managers identify and categorize risks, agencies should consider root causes, sources, and likelihood of the risk occurring, as well as potential positive or negative outcomes, and then prioritize the resulting identified risks.
- Assessments of the likelihood and impact of risk events help agencies monitor whether risk remains within acceptable levels and support efficient allocation of resources to addressing the highest priority risks.
- When analyzing risk, it is important to consider the risk that is integral to what an agency does, for example:

A Federal Credit program is designed to meet specific social and public policy goals by providing financial assistance to borrowers who may be too risky to obtain private sector credit under reasonable terms from lenders. Some of these borrowers present great risk to the agency, but the program's *specific objective* was to help those who could not get a reasonable loan otherwise, and it believes that the potential social and reputational benefits are considered to outweigh the risks.

Analyze and Evaluate (continued)

- Using a Likelihood Scale like the one below can help prioritize risks by assigning number values to each risk based on the probability that the risk event will occur.

Likelihood	Definition
1- Remote	Risk event rarely to occur within the next 12 months
2 - Low	Risk event not likely to occur within the next 12 months
3 - Possible	Risk event may occur within the next 12 months
4 - Probable	Risk event will likely occur within the next 12 months
5 – Almost Certain	Risk event will almost certainly occur within the next 12 months

Analyze and Evaluate (continued)

- Using an Impact Scale like the one below can help prioritize risks by assigning number values to each risk based the impact to the organization if the risk event were to occur.

Impact	Definition
1- Nominal	Risk event will have almost no adverse effect on mission or organizational goals
2 - Slight	Risk event will temporarily effect mission or organizational goals
3 - Moderate	Risk event will require unanticipated time and resources to remediate effects on mission or organizational goals
4 - Significant	Risk event will prevent achievement of organizational goals
5 – Catastrophic	Risk event will preclude the organization from fulfilling its mission

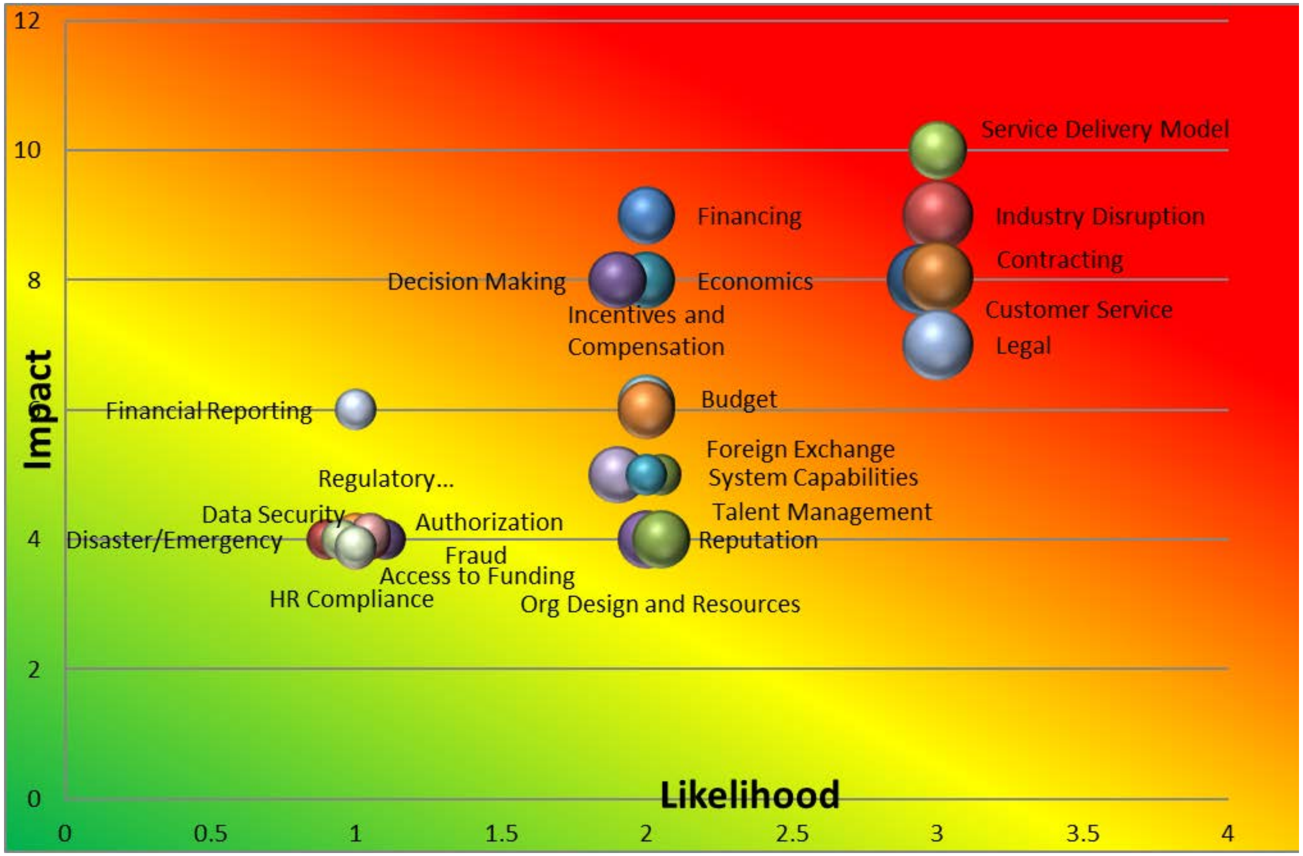
Analyze and Evaluate – Risk Profile Example

- Using the same risk of a data privacy breach, as before, populate the primary impact, threat or opportunity and likelihood columns.

Risk Description	Risk Event	Primary Impact	Threat or Opportunity	Likelihood	Risk Impact Category	Order of Priority	Response Type	Response Strategy
Personal identifiable information about our employees or the public has been lost, misused, or stolen.	Data Privacy Breach	4 – Significant	Threat	4 - Probable				

Analyze and Evaluate (continued)

- Here is an example of a heat map that helps evaluate risk based on the assessed likelihood and impact of the risk event.



Analyze and Evaluate – Risk Profile Example

- Using the same risk of a data privacy breach as before, populate the risk impact category and order of priority columns. Order of priority should be determined by where this risk lands on your heat map based on its impact and likelihood.

Risk Description	Risk Event	Primary Impact	Threat or Opportunity	Likelihood	Risk Impact Category	Order of Priority	Response Type	Response Strategy
Personal identifiable information about our employees or the public has been lost, misused, or stolen.	Data Privacy Breach	4 – Significant	Threat	4 - Probable	Financial, Cyber Information Security, Compliance, Legal, Reputational	High Priority		

- Risk Impact Category includes the following risk categories:
  - Compliance, Credit Program, Cyber Information Security, Financial, Legal, Legislative, Operational, Political, Reporting, Reputational, Strategic
  - Often times, each risk will cover several categories

Respond to Risks

- The agency leadership must decide how to allocate scarce resources, such as budget resources, analytical capabilities, and management attention, to address them.
- While the Risk Officer can help to facilitate the process, managing risk is the responsibility of the unit heads where the risk resides.
- Once risks are prioritized and risk responses are determined, milestones for carrying out the risk management process should be documented.

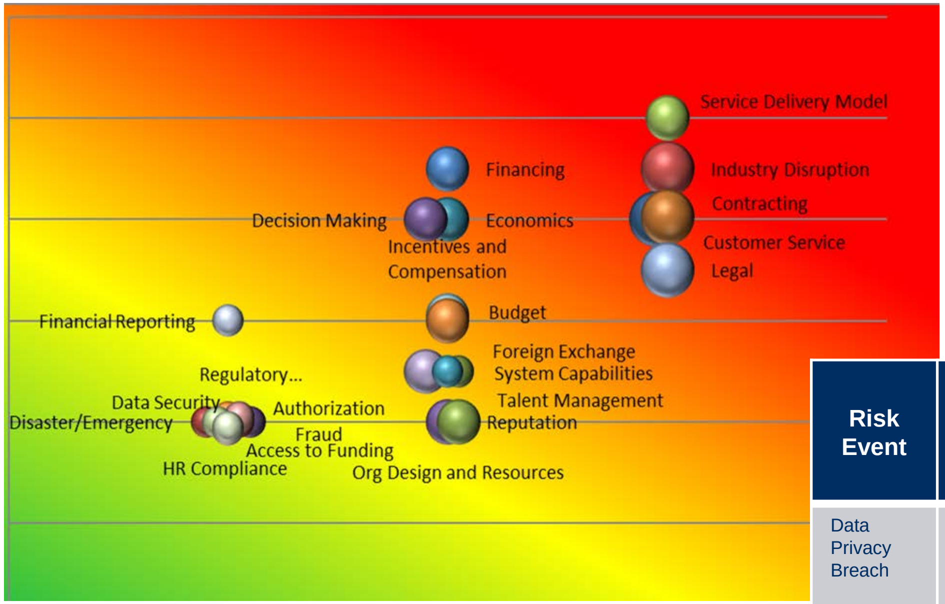
Respond to Risks – Risk Profile Example

- Using the same risk of a data privacy breach as before, populate the risk impact category and order of priority columns. Order of priority should be determined by where this risk lands on your heat map based on its impact and likelihood.

Risk Description	Risk Event	Primary Impact	Threat or Opportunity	Likelihood	Risk Impact Category	Order of Priority	Response Strategy Type	Response Strategy
Personal identifiable information about our employees or the public has been lost, misused, or stolen.	Data Privacy Breach	4 – Significant	Threat	4 - Probable	Financial, Cyber Information Security, Compliance, Legal, Reputational	High Priority	Reduction	Obtain the infrastructure , personnel, training, and technology to reduce impact and likelihood to a level three or lower

Risk Response Types: Acceptance, Avoidance, Reduction, Sharing

Summarize for the Board



Risk Event	Impact	Likelihood	Risk Categories	Priority	Response Type
Data Privacy Breach	4 – Significant	4 - Probable	Cyber,, Reputational	High	Reduction
Service Delivery	4 – Significant	4 - Probable	Financial Reputational	High	Reduction
Industry Disruption	4 – Moderate	3 – Possible	Financial Reputational	High	Sharing

Polling Question #4

At which level in your organization are frequent updates on the ERM program, entity-level risks, and managements’ response provided?

1. Board or board committee level
2. Executive management level
3. Other
4. No one
5. I don’t know

Conclusion

- ERM should be inclusive of and supported by leadership (i.e. tone at the top)
- Key participants should have a diverse and high-level view of the organization
- ERM purpose, authority, structures, activities should be formally defined
  - Establish a Charter
  - Identify Risks and Create Risk Profile
  - Summarize top risks for leadership and the Board
  - Create an iterative, repeatable process

Thank You

Bill Dykstra

Crowe, LLP

Bill.Dykstra@crowe.com

The information in this document is not – and is not intended to be – audit, tax, accounting, advisory, risk, performance, consulting, business, financial, investment, legal, or other professional advice. Some firm services may not be available to attest clients. The information is general in nature, based on existing authorities, and is subject to change. The information is not a substitute for professional advice or services, and you should consult a qualified professional adviser before taking any action based on the information. Crowe is not responsible for any loss incurred by any person who relies on the information discussed in this document. Visit www.crowe.com/disclosure for more information about Crowe LLP, its subsidiaries, and Crowe Global. © 2018 Crowe LLP.