Sustainable ERM in the Public Sector: Part Two

Presented by Bill Dykstra

September 20, 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 (OMB 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

- Part One – Recap
- Building Sustainable Risk Management Practices
  - Embed into the Culture
  - Build upon Existing Practices and Processes
  - Building Maturity
  - Administration
- Templates and Practical Applications
- Q&A

Polling Question #1

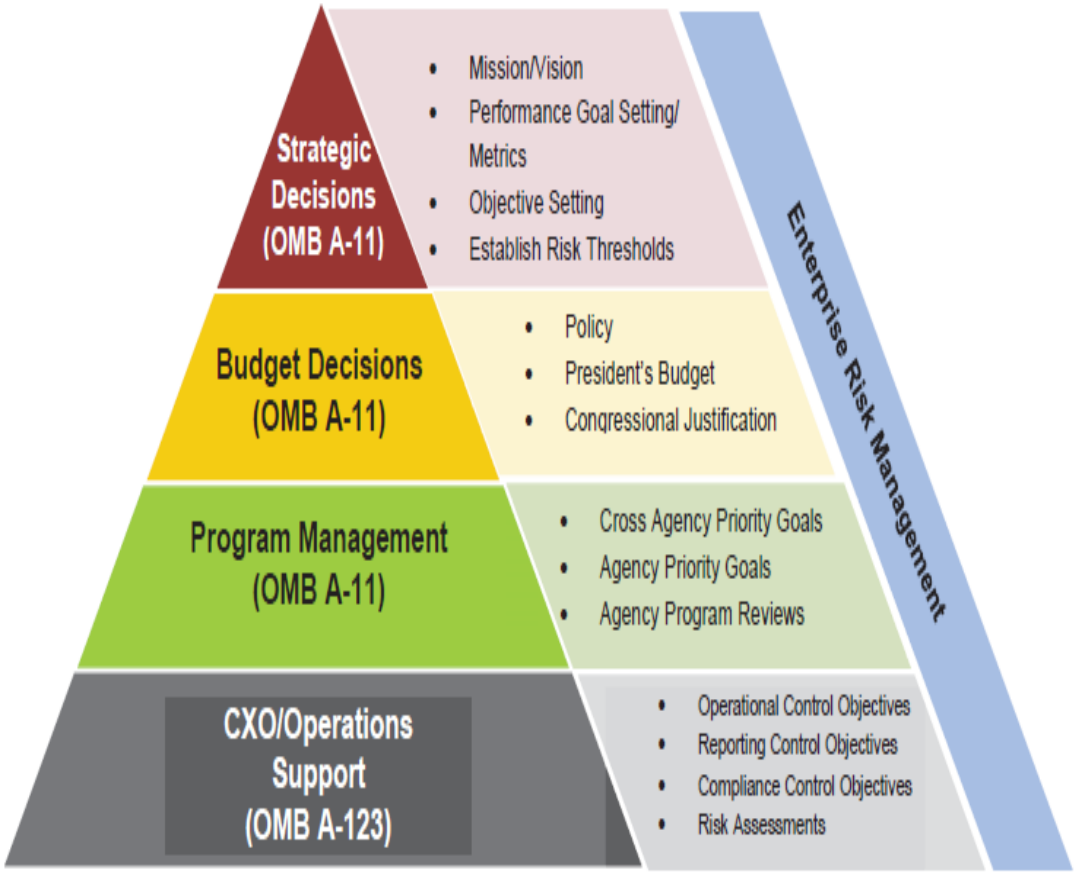
How would you rate your organization's willingness to enhance the maturity of its ERM?

1. Opposed – leadership has recently expressed that it is not willing to move the ERM program toward a more mature model at this time.
2. Reluctant – it would take a very strong business case to move this forward, but leadership is not expressly opposed to it.
3. Uncertain - leadership is either unaware of the value of a more mature ERM model or is trying to decide on the best allocation of its resources on various major initiatives.
4. In Favor – leadership has expressed interest and willingness in advancing the ERM program but no tangible plans have yet been made.
5. Eager – leadership has given, or indicated that it will give the "green light" to advancing the ERM program to the next level.

Enterprise Risk Management Part One - Recap

Part One - Recap

- 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.
- 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



Part One – Recap (continued)

- 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.

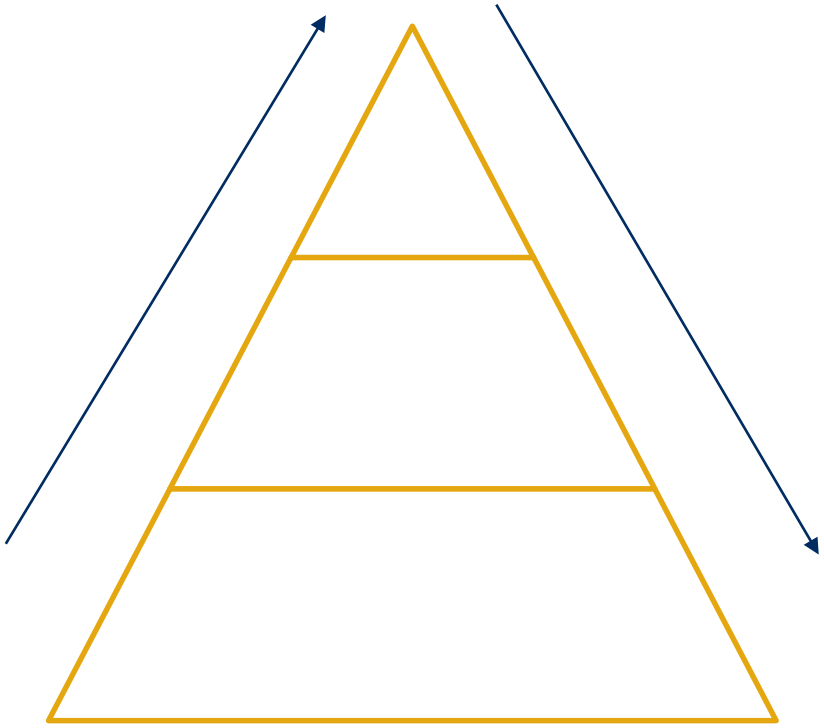
- Most widely recognized and accepted frameworks
    - COSO
    - ISO 31000

Part One – Recap (continued)

- 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

Embedding ERM into the Culture

- Building strong communication flow is critical.
  - Top-down
  - Bottom-up
- Employees at all levels have tools necessary to:
  - Evaluate risks
  - Act on risks
  - Share recommendations
  - Seek input



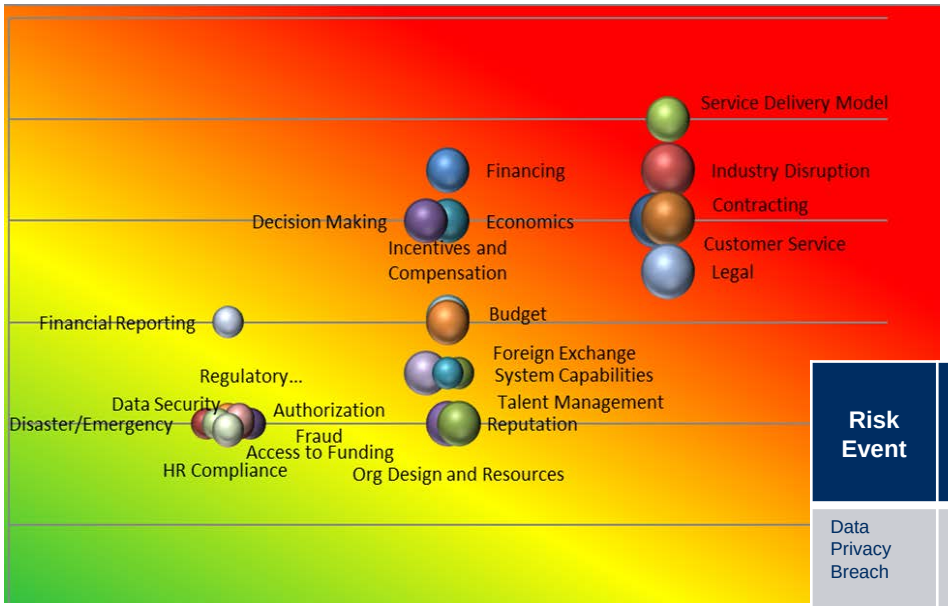
Respond to Risks – Risk Profile Example (from Part 1)

- 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



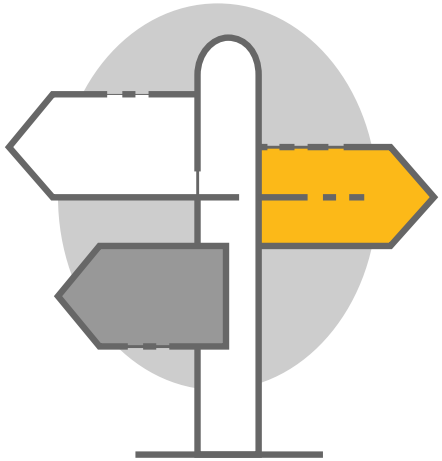
Risk Event	Impact	Likelihood	Risk Categories	Priority	Response Type
Data Privacy Breach	4 – Significant	4 - Probable	Cyber,, Reputational	High	Reduction
Service Delivery	4 – Significant	4 - Probable	Financial Reputational	High	Reduction
Industry Disruption	4 – Moderate	3 – Possible	Financial Reputational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

Building Sustainable Risk Management Practices

Strategic and Tactical Decisions Tied To Risk Appetite

Clearly defined risk appetite statements provide guidance in the decision-making process for long and short-term goals

- Integrated across the organization
- Forward looking, learning from past, integrating current best practices
- Allows agencies to make risk-informed decisions in regards to
    - Resources
    - Controls
    - Organizational consequences or impacts
    - Reduce surprises and unexpected losses



Strategy and Performance

- Consideration of risks is key when focusing on strategy and performance.
  - ERM provides the potential for a fully integrated, prioritized, and forward-looking view of risk to drive strategy and business decisions, eliminating organizational barriers
  - Transparency supports informed decision making in all levels of the organization
  - ERM allows for clear roles and responsibilities: defining expectations and ownership of roles
  - Risk response strategies help identify actions/priorities to be included in performance plans for individuals and the organization

Risk Owners and Responses

- Risk ownership is key to establishing a repeatable, sustainable ERM cycle
- Selecting a **Risk Owner** is a delicate mix of the right level of authority and the appropriate level of subject matter expertise (it will be different in every org)
- The **Response** should be maintained and implement by the Owner
- The Response should be aligned with the **Risk Appetite**
- The RMC should monitor implementation and success.

Risk Response Example

Using our previous example of a data privacy breach scenario, the Risk Owner will update the action plan to execute the previously established Risk Response In this case, the response was, “Reduction”.

Risk Title: Data Privacy Breach				Risk Manager: CISO	
Treatment Plan Summary: Reduction					
Treatment Plan Status: In Progress					Trend: ⬆
Task No:	**Task Description**	**Owner**	**Est.**	**Actual**	**Notes/Status**
1	Formally established security policies and procedures	IT Security Administration	12/31/2018	TBD	On Schedule
2	Mandatory data privacy requirements training for all employees	IT Security Administration	3/31/2019	TBD	On Schedule
3	Random “mock-phishing” attempts to test employees’ ability to identify and properly respond to social engineering schemes	IT Security Administration	6/30/2019	TBD	Requirements in Draft
Contingency Plan: Hire third party to develop P&P, conduct employee training, and execute random, mock phishing attempts.					Trigger: Funding, Conflicting Priorites
Treatment Alternatives Considered: In development					

Monitor Residual Risks – Extended Risk Profile

- Now we can use the residual risk assessment to evaluate the response's effectiveness, ensure it is within the organization's risk appetite and tolerances, and monitor going forward.

Risk Event	Primary Impact	Likelihood	Inherent Risk Rating	Response Strategy Type	Response Strategy	Primary Impact	Likelihood	Residual Risk Rating
Data Privacy Breach	4 – Significant	4 - Probable	High	Reduction	Strategy 1 Strategy 2 Strategy 3	4 – Significant	3 - Possible	Medium

Polling Question #2

Does your organization maintain a risk profile of some type (regardless of its format or title) which includes an assessment of both inherent and residual risk?

1. No, we do not maintain a risk profile
2. We maintain an informal risk profile but it is not actively managed and monitored.
3. We maintain an risk profile that is updated and reviewed periodically but it does not include both an inherent and residual risk profile.
4. We maintain a comprehensive risk profile with both inherent and residual risk ratings which is actively managed and monitored for residual risk levels that exceed risk appetite or established tolerances.
5. I don’t know, or my organization does not fit into any of the above.

Polling Question #3

Has your organization identified risk owners who maintain risk responses and detailed action plans as discussed above?

1. No, we have not formally established risk owners as discussed above.
2. We have informally identified individuals who periodically address how certain risks to the organization are being addressed; however this is done on more of an ad hoc basis than the process described above.
3. We have formally identified risk owners but they do not maintain formal risk responses/action plans as described above.
4. We have formally identified risk owners who maintain the risk response/action plan, inform the risk profile, and provide frequent updates to leadership and the board on the progress of those plans
5. I don’t know, or my organization does not fit into any of the above.

Leverage the Strategic Planning Cycle

Strategic Planning

- Risk must align to the goals/objectives of the organization
- Organizational goals/objectives have already been set
- Use goals to build tolerable risk levels

Example:

If the purpose of a program is to inject capital into an under-served market during a recession in which private lenders are “de-risking”, or cutting back on lending to high-risk borrowers, the government may determine a higher risk of default is acceptable at that point in order to fulfill that market need. In this case, the government would have a higher risk appetite than in more expansive times.

Leverage the Budget Cycle

Budget Cycle

- Employ ERM to evaluate program areas with consideration of staffing and budget resources
- Ability to focus limited resources
- Strengthen efficiency
- Utilize project funding oversight
- Overall budget formulation
- Capital Investment Planning

Are you adequately funding your Risk Responses?

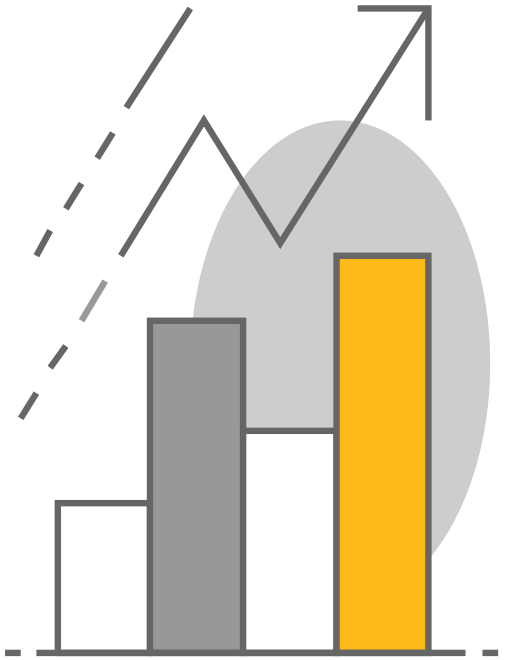
Leverage the Way Decisions are Made

- Decision-making methodologies currently in practice:
  - How are decisions made?
  - Are risks considered?
  - How can ERM enhance the decision-making process?

- Effective ERM improves decision making through a structured understanding of opportunities and threats
- Integrating ERM into management's day to day decision-making helps to
  - Focus goals
  - Align resources
  - Monitor progress
  - Ensure compliance with applicable laws, regulations and controls

Leverage Existing Reporting Requirements

- Reporting (monthly or quarterly – based upon organization needs)
  - Do goals continue to be aligned with organization's mission?
  - Ability to measure goals – both strategic and tactical
  - Using KPI and KRI to communicate changes since the last reporting period to leadership, general public
  - Adjust objectives and risks if necessary



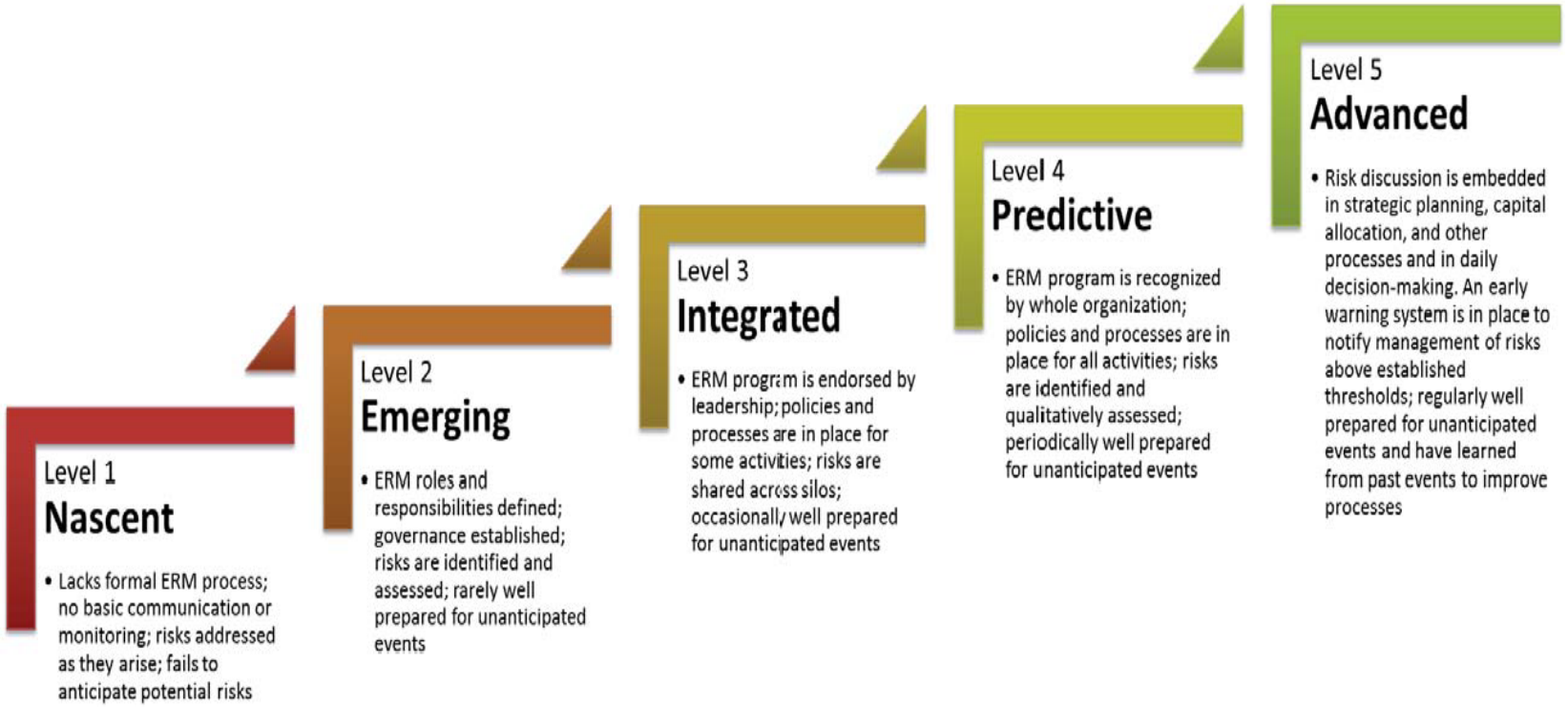
Polling Question #4

Which of the existing processes does your organization’s ERM program leverage to provide value without expanding bureaucracy?

1. Strategic Planning
2. Budget Cycle
3. Board or Committee meetings
4. Reporting (Financial or Operational)
5. Other
6. None

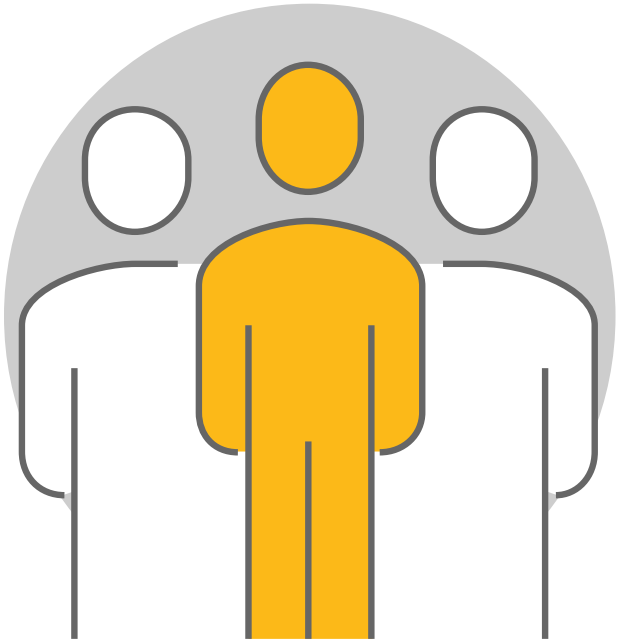
Maturity of the ERM Implementation

Every organization has its own level of organizational and process maturity. Not all levels within the organization and processes need to be at a level five.



Administration

- To be effective, the ERM program needs an appropriate team with experience and an understanding of risk management
- Size of ERM team needs to reflect organizations ERM needs/desires
- ERM team needs to collaborate and share information and knowledge
- Organization must provide continuous training, tools and resources for sustained ERM growth



Pitfalls

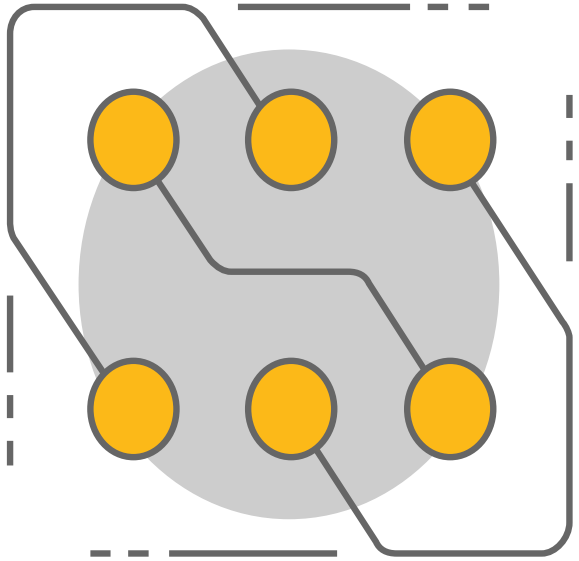
- Cultural Challenges - Lack of incentive to embrace risk management
- Lack of resources, authority, support to execute
- Too much too soon
- Not considering the need to periodically assess and adjust
- Lack of effective communication/reporting on progress

Manual Processes

- So who is going to maintain this?
  - Most effective at maturity levels 1 and 2
  - Considerations:
    - Cost
    - Risk of error and omission of data
    - Key stakeholders
    - Volume of information
    - Reporting requirements

ERM Software Solutions

- Most appropriate at Levels 3-5
  - Consider risk vs reward
  - Value added efficiencies gained
  - Constraints include:
    - organization's size, complexity, available resources, desired maturity level



ERM Software Solutions (continued)

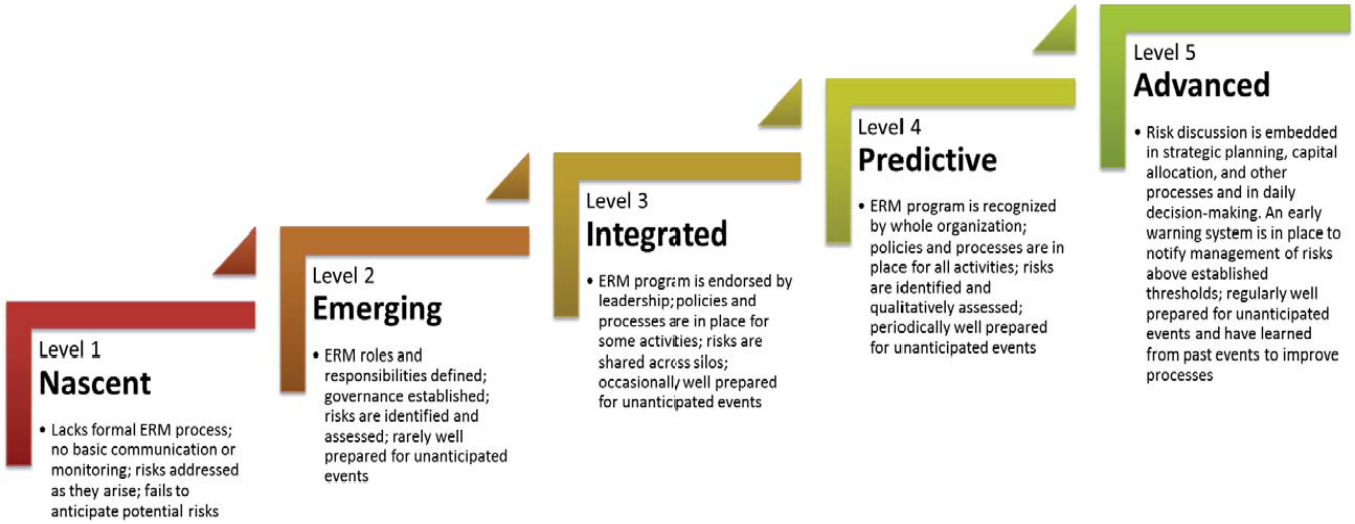
- GRC platforms are often used to help administer ERM programs more efficiently and effectively
- Examples include Metricstream, Nasdaq B-Wise, Service Now GRC, IBM Open Pages, SAP GRC, and RSM Archer

Benefits	Limitations
Integrates standards and information across the organization.	It will not replace governance, risk, and compliance functions or controls (It will enhance and supplement, but does not replace).
Increases collaboration and awareness	It will not eliminate the need for risk and compliance professionals (the system is a tool intended to help support those individuals)
Uses dashboards and enhanced reporting to provide greater visibility and insight	It will not solve underlying, existing data quality and integrity problems (these platforms can only be as good as the data an organization puts into it)
Formalizes workflows, improves efficiency and enforces standard processes	
Reduces manual efforts and allows humans to focus on analysis and actions	
Improves strategic decision making	
Documents risk and compliance activities and easily demonstrates the same for auditors and regulators	

Polling Question #5

Which level of the maturity model, do you believe would be the best fit for your organization's needs over the next 3-5 years?

1. Nascent
2. Emerging
3. Integrated
4. Predictive
5. Advanced



Thank You

Bill Dykstra

Crowe, LLP

Bill.Dykstra@crowe.com