Atlanta Chapter Meeting

How to Build an Effective Enterprise Risk Management program (ERM)

APRIL 24 | 10AM-10AM ET

BT

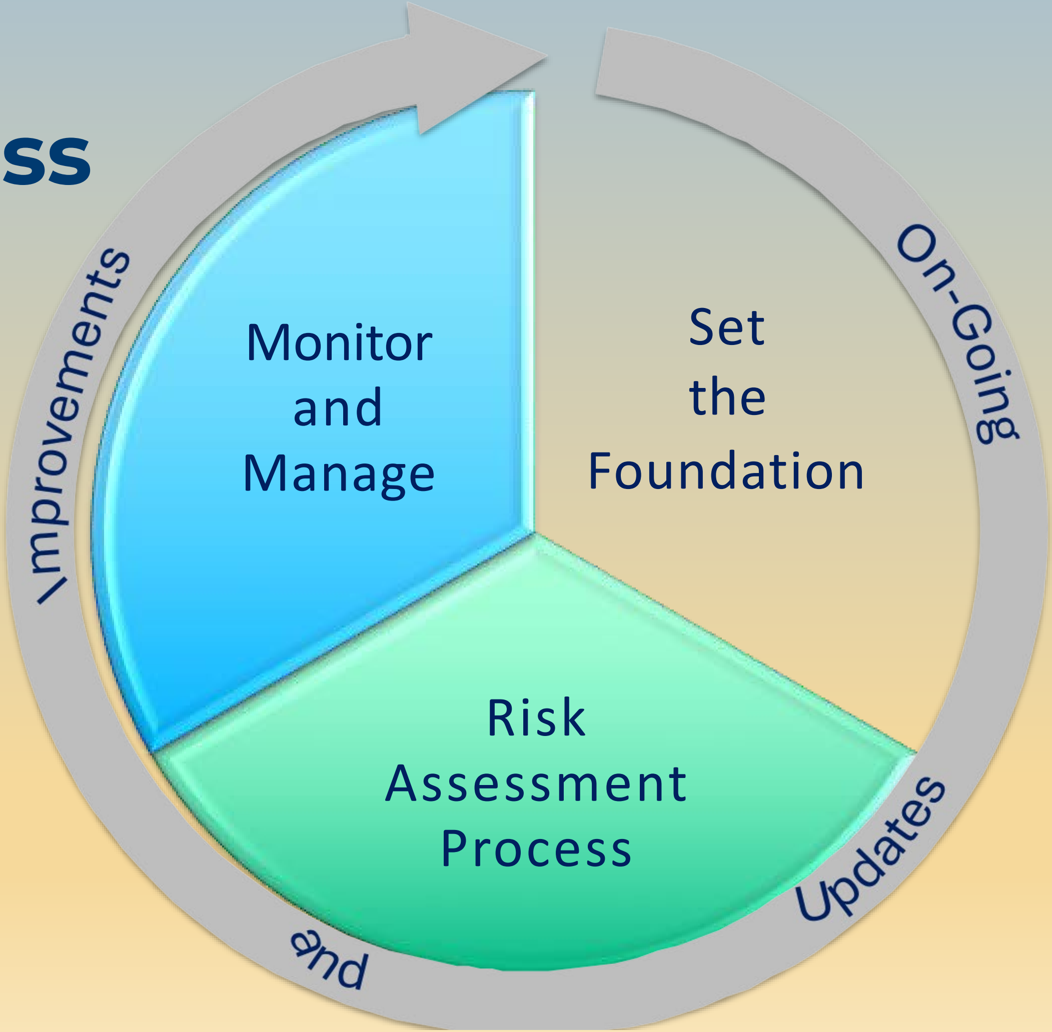
The Institute of Internal Auditors

Durran Dunn, CPA, CIA
Partner at Bennett Thrasher

Learning Objectives

- Designing an ERM program that fits your organization's specific needs and culture.
- Apply practical techniques for risk identification and assessment.
- Integrate ERM into daily business operations rather than an annual compliance exercise.

ERM Process



Set the Foundation

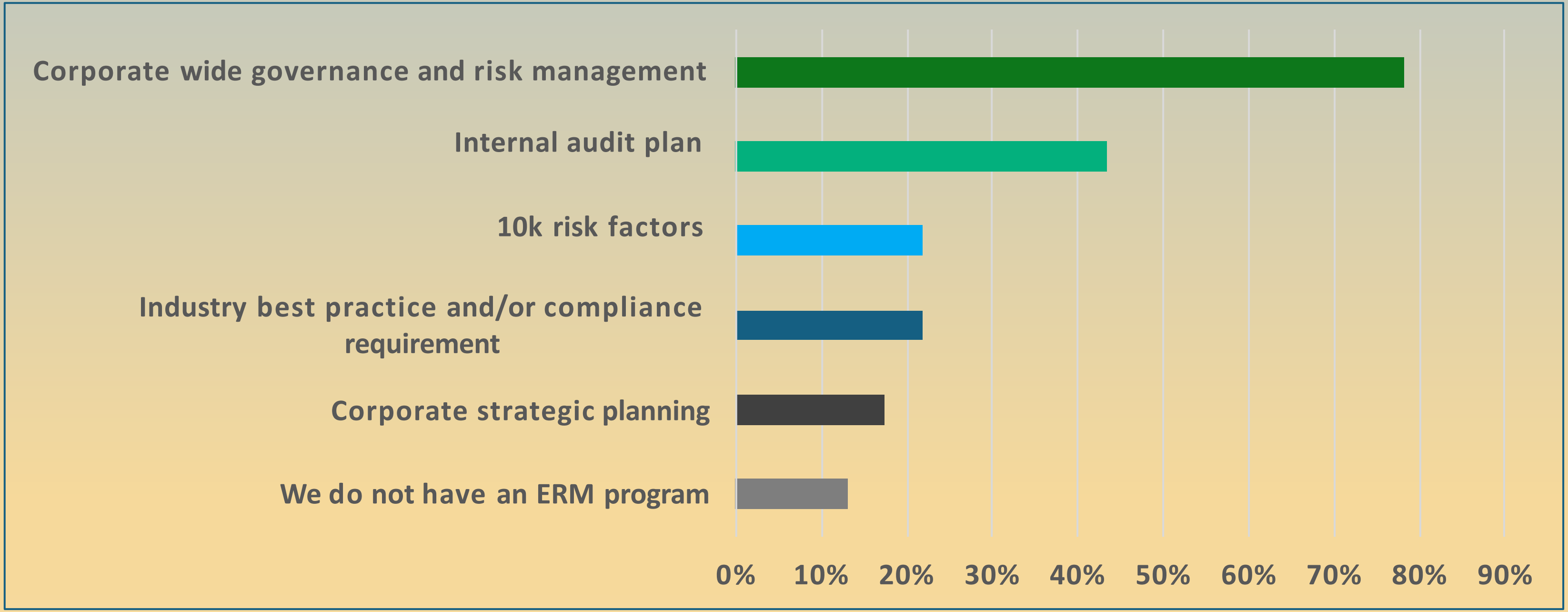
Risk Assessment Process

Monitor and Manage

Setting the Foundation

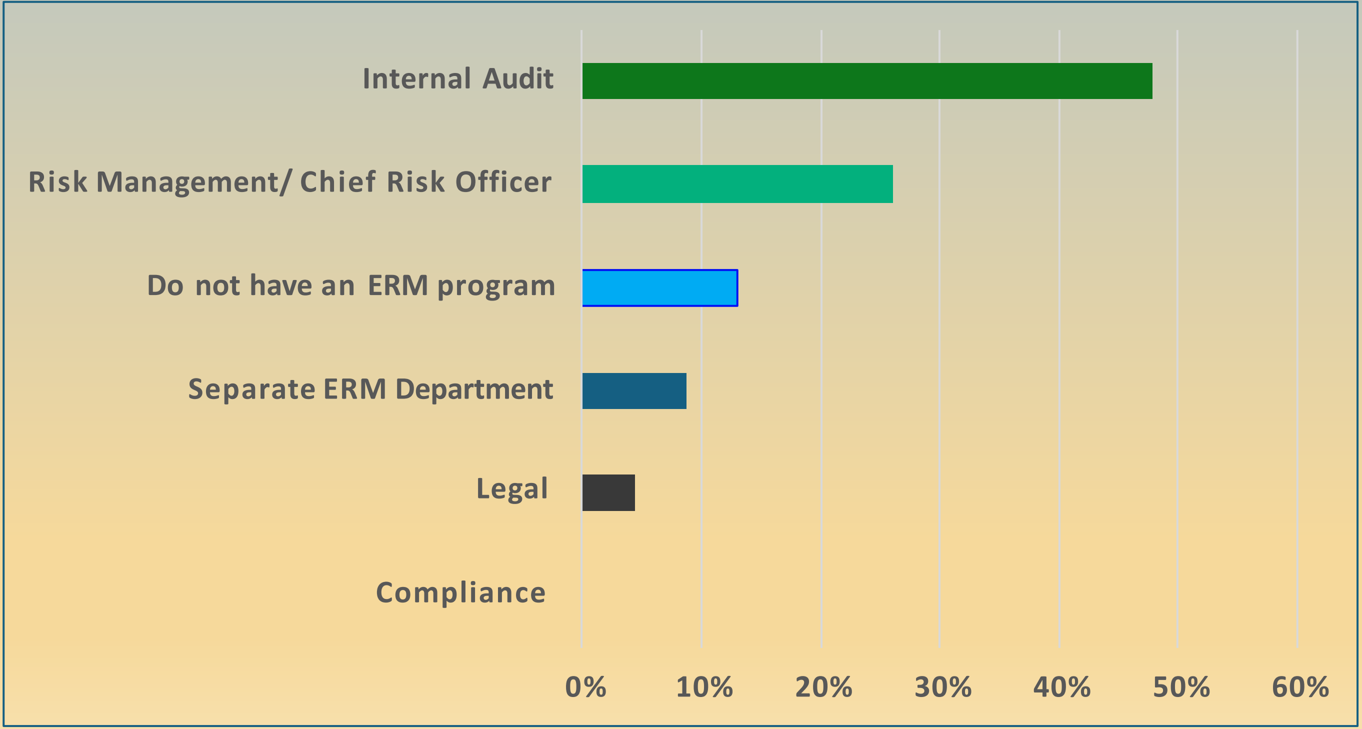
- Executive Leadership and Board Support
- ERM Program Objectives/Purpose
- ERM Program Ownership
- Building the Program

ERM Purpose – Benchmarking Data



**Insights gathered from polling internal audit departments nationwide for benchmarking purposes.*

ERM Ownership – Benchmarking Data



**Insights gathered from polling internal audit departments nationwide for benchmarking purposes.*

Building the Program

Setting the Foundation

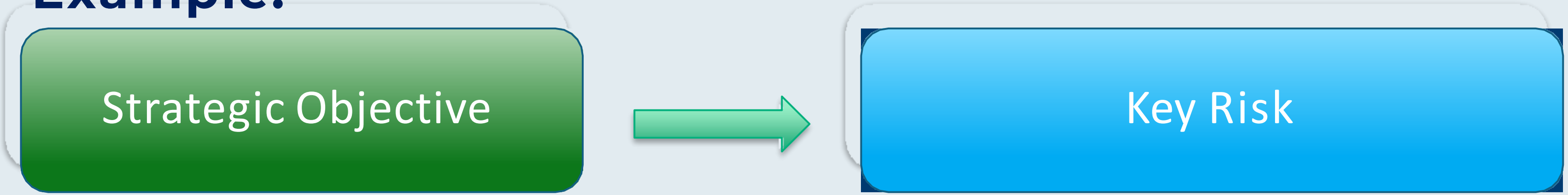
- Framework
- Charter & Policies
- Risk Appetite and Risk Tolerance

Risk Assessment Process

- Linking Strategic Objectives & Risk
- Risk Identification
- Risk Scoring
- Risk Assessment Methods

Linking Strategic Objectives & Risks

Example:



Strategic Objective

Key Risk

Innovation in Healthcare: Advancing knowledge and research to discover innovative solutions for pain management and breakthrough cures.

If critical research funding, resources, or partnerships are not secured or maintained, the organization may be unable to advance knowledge and discover innovative solutions for pain management and breakthrough cures.

Risk Identification Techniques

Format

- Individual interviews
- Group session(s)
- The ERM owner/facilitator creates the risk list
- Survey
- Combination of techniques

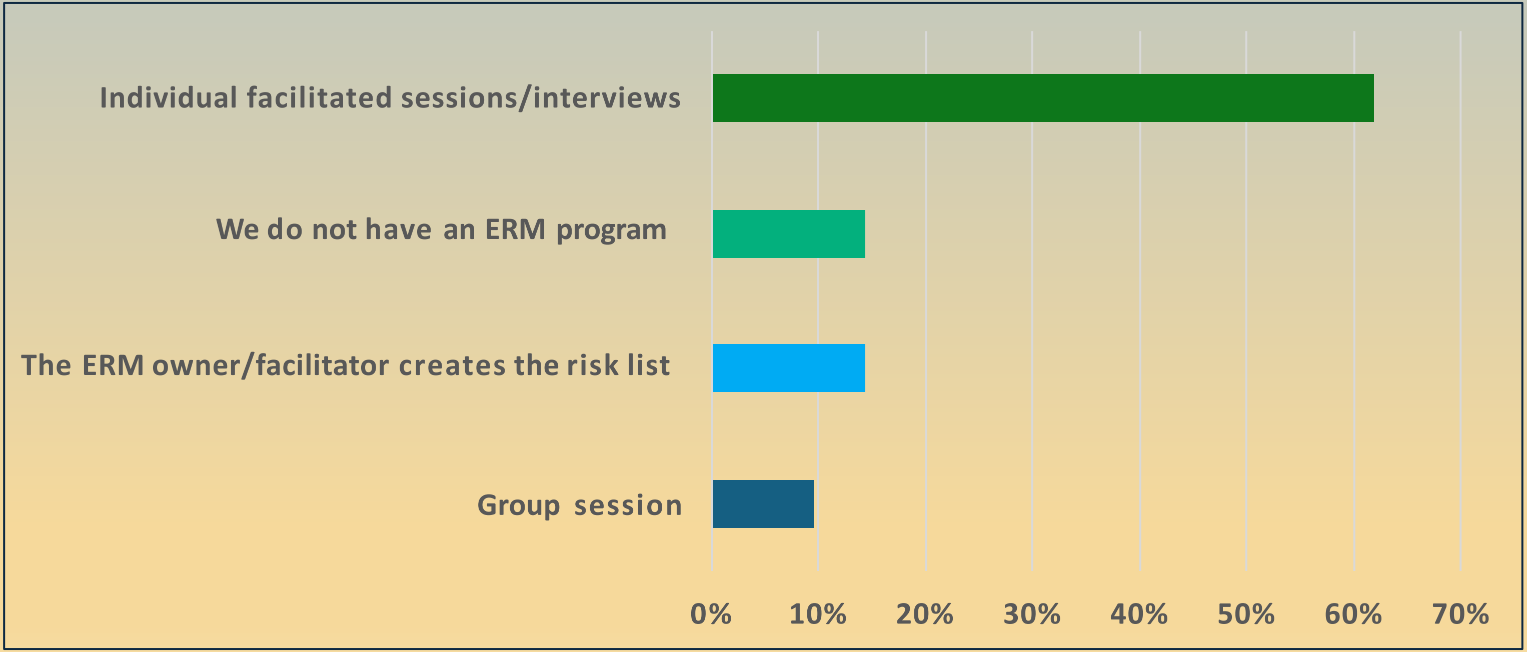
Considerations

- Participants – who & how many?
- Identifying emerging risks
- Company culture
- ERM purpose

Risk Identification Techniques

Pros		Cons
• Candid / confidential / focused • Clarification opportunities	**Individual interviews**	• Inefficient • Lack of dynamic discussion • Narrow perspective
• Collaborative insights • Dynamic discussions • Efficient	**Group session(s)**	• Scheduling challenges • Limits participation • Peer pressure or groupthink • Hesitation to contribute
• Efficient • Clear ownership	**ERM owner list**	• Narrow perspective • Unidentified risks
• Broad participation	**Survey**	• Narrow perspective • Lack of clarity

Risk Identification – Benchmark Data



**Insights gathered from polling internal audit departments nationwide for benchmarking purposes.*

Risk Scoring Methodology

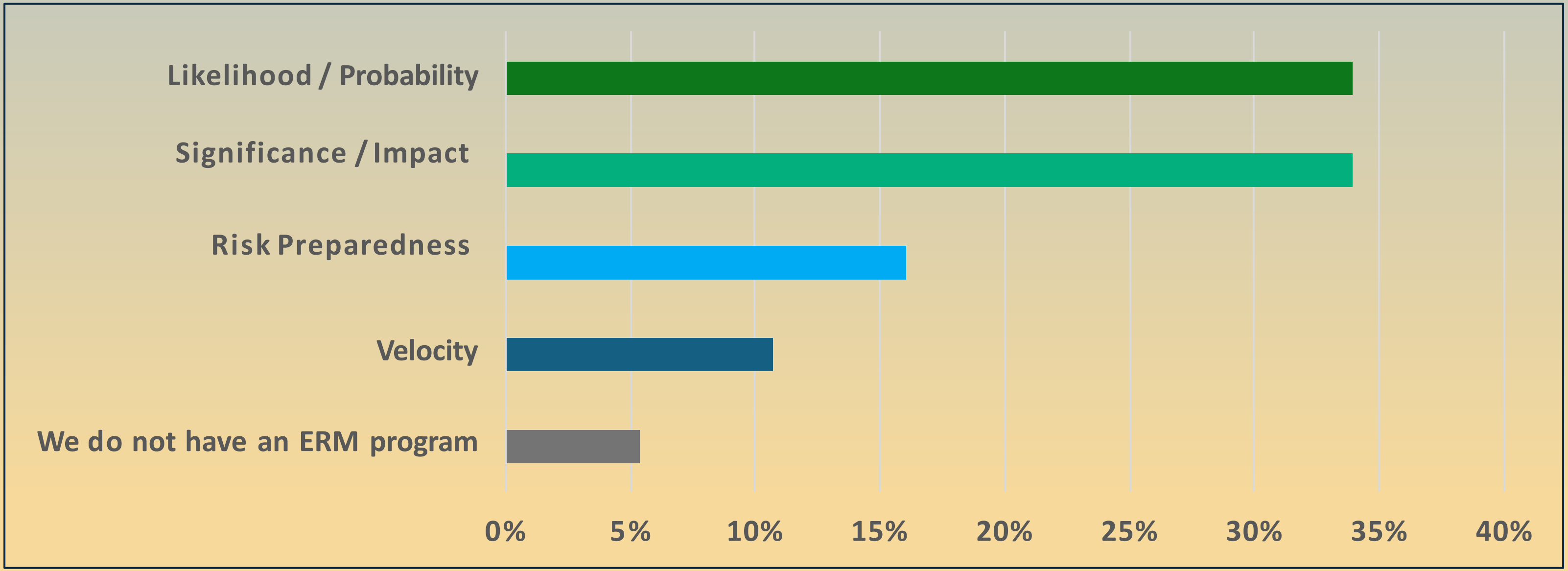
Risk Scoring

- Impact/Significance
- Likelihood/Probability
- Risk Preparedness
- Velocity

Defining the Risk Scores

- Quantitative Factors
- Qualitative Factors

Risk Scoring – Benchmark Data



**Insights gathered from polling internal audit departments nationwide for benchmarking purposes.*

Risk Assessment Methods

Methods

- Survey
- Individual facilitated sessions/ interviews
- Group session(s)
- Forced Ranking
- Combination of methods

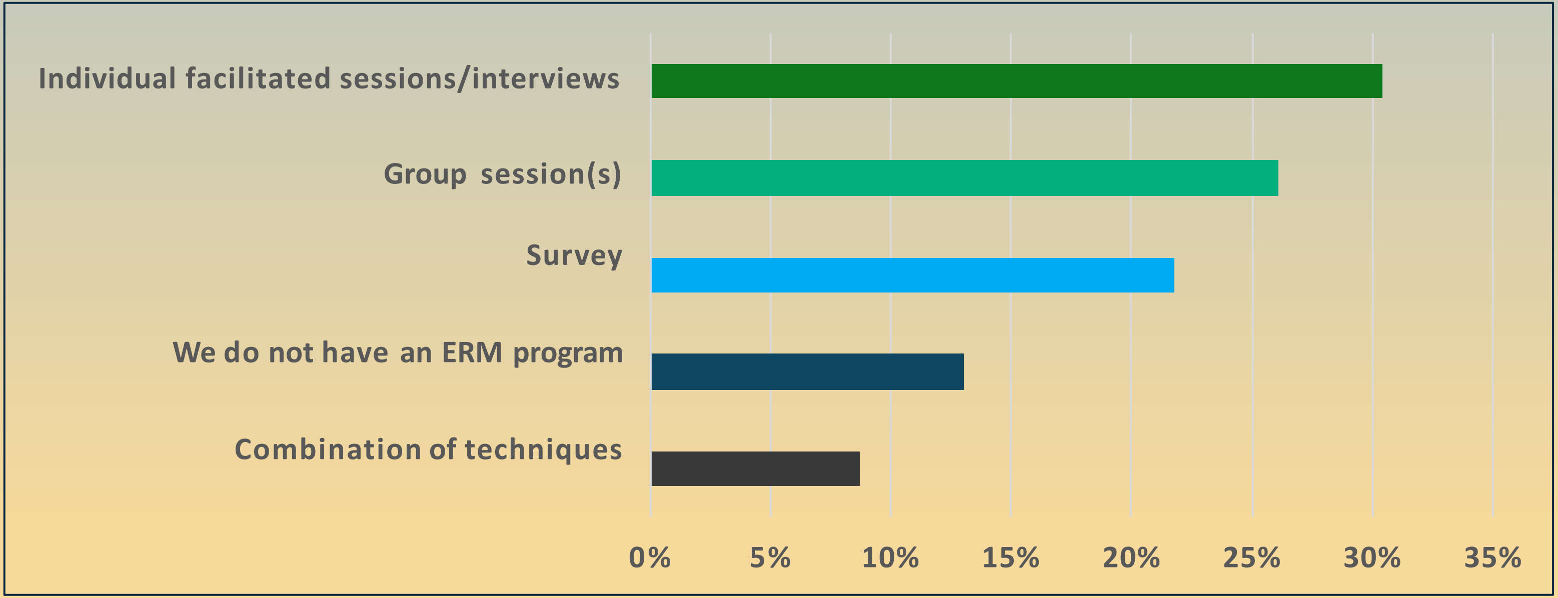
Considerations

- Participants – who & how many?
- Identifying emerging risks
- Company culture

Risk Assessment Methods

Pros		Cons
• Efficient • Anonymous • Broad participation	**Survey**	• Narrow perspective • Lack of dynamic discussion
• Candid / confidential / focused • Clarification opportunities	**Individual interviews**	• Inefficient • Limited participation and/or perspective
• Collaborative insights • Dynamic discussion • Efficient	**Group session(s)**	• Scheduling challenges/limits participation • Peer pressure or groupthink • Hesitation to contribute
• Efficient • Broad participation • Prioritization/clarity	**Forced ranking**	• Limited flexibility • Oversimplification

Risk Assessment – Benchmark Data



**Insights gathered from polling internal audit departments nationwide for benchmarking purposes.*

Monitoring & Managing

- Risk Owners
- Risk Strategies
- Monitor: Reporting & Oversight

Risk Owners

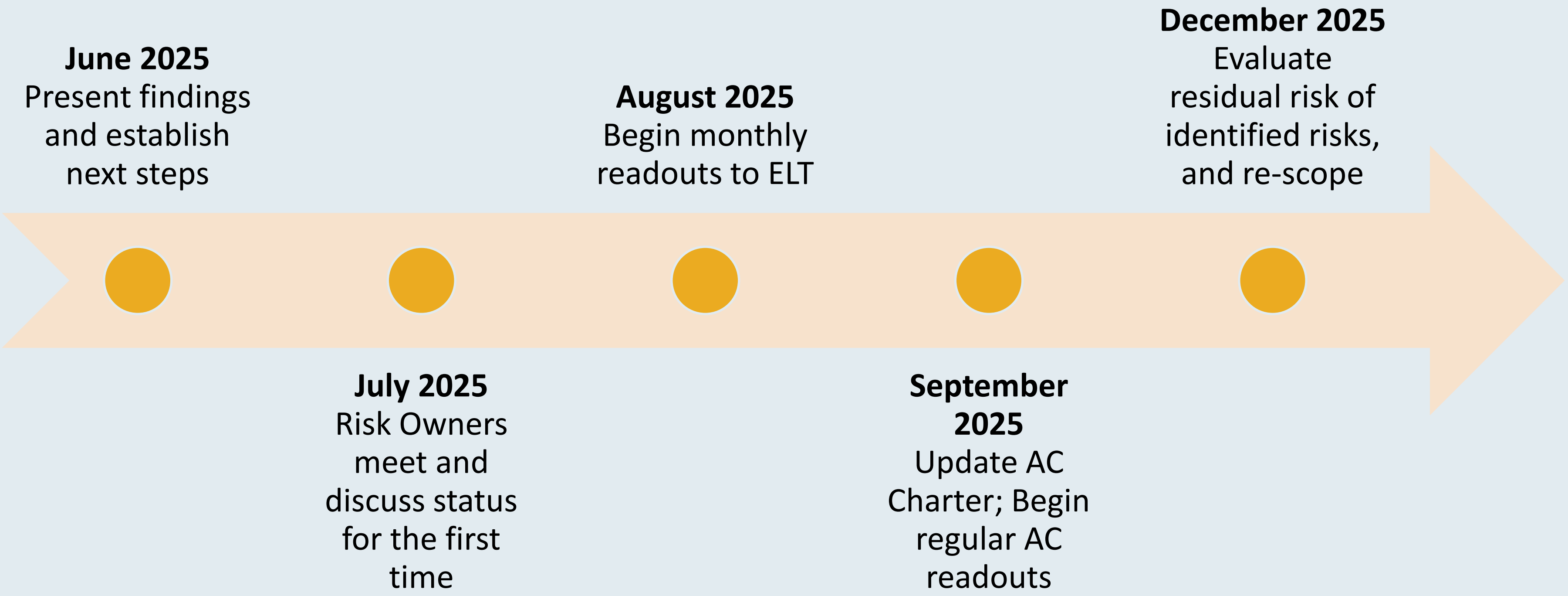
Responsible for actively managing and monitoring specific risks:

- Develop risk strategies
- Execute risk strategies
- Monitors and reports on key risk indicators

Understanding Owners

- **Risk Sponsors and Risk Owners**
  - Identify risk mitigation strategy and implement process
  - Re-evaluate risk score, inclusive of mitigation efforts
  - Provide updates to ELT on strategy, status, and resolutions
  - Risk Owners to meet monthly to stay apprised of status
- **Executive Leadership**
  - On an ongoing basis
    - Re-evaluate “top risks” in light of mitigation efforts
    - Scope in previously identified risks to the extent top risks are mitigated to a reasonable level or to the extent possible
  - Annually
    - Re-evaluate the Inherent Risk of previously identified risks
    - Evaluate new risks on an ongoing basis and evaluate Inherent Risk of each

Illustrative Timeline of the ERM Program



June 2025
Present findings and establish next steps

July 2025
Risk Owners meet and discuss status for the first time

August 2025
Begin monthly readouts to ELT

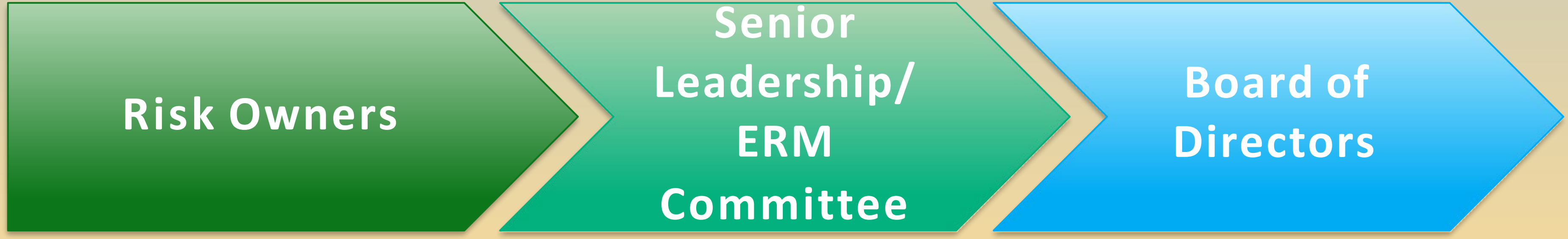
September 2025
Update AC Charter; Begin regular AC readouts

December 2025
Evaluate residual risk of identified risks, and re-scope

Risk Strategies

- Mitigate
- Transfer
- Accept
- Avoid

Risk Owners

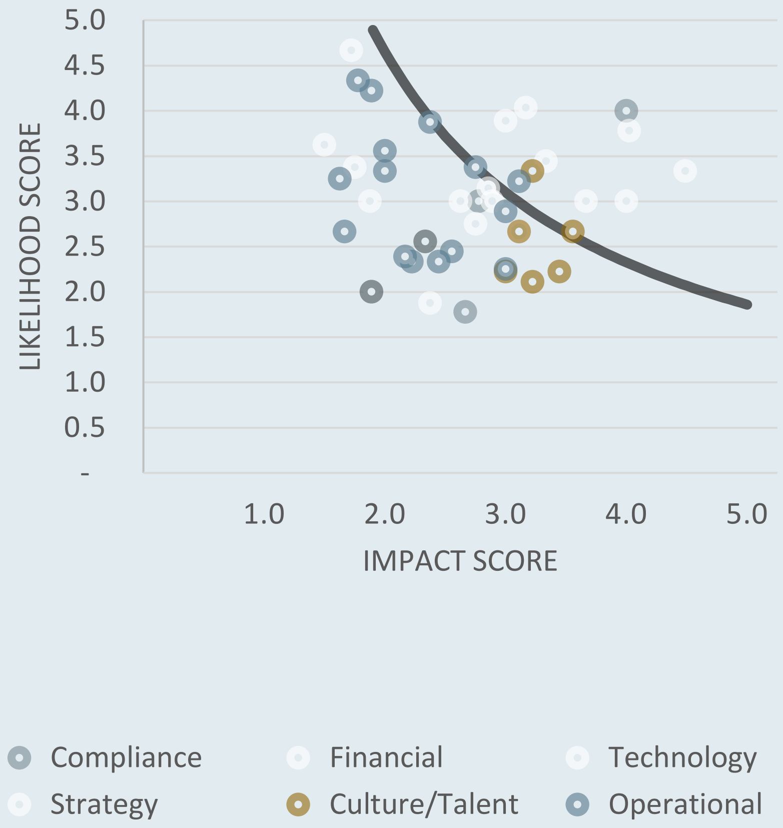


Risk Owners

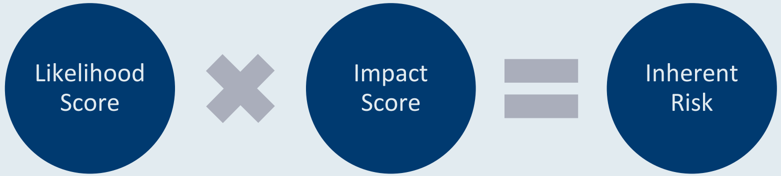
Senior Leadership/ ERM Committee

Board of Directors

Illustrative Risk Chart



- **Observations**
  - Regulatory and Reimbursement were highest risks
  - Provides opportunity to “divide and conquer”
- **Scoping**
  - Inherent risk of 9.3 or more
    - Scopes in top 12 risks
    - Reflected as all risks above and to the right of “Scoped-In Risks” line



Illustrative Risk Scoring

Risk	Risk Theme	Impact Score	Likelihood Score	Inherent Risk	Risk Sponsor(s)	Risk Owner(s)
1	FDA Regulatory Pathways	4.0	4.0	16.0	Name	Name
2	Reimbursement Pressures	4.0	3.8	15.2	Name	Name
3	Competitor Tactics	4.5	3.3	15.0	Name	Name
4	Cybersecurity	3.2	4.0	12.8	Name	Name
5	IT Strategy	4.0	3.0	12.0	Name	Name
6	Clinical Evidence	3.3	3.4	11.5	Name	Name
7	Product Concentration	3.0	3.9	11.0	Name	Name
8	SBWeb/MES	3.7	3.0	11.0	Name	Name
9	Turnover	3.2	3.3	10.7	Name	Name
10	Sales Channel Focus	3.1	3.2	10.0	Name	Name
11	Succession Planning	3.6	2.7	9.5	Name	Name
12	Manufacturing Footprint	2.8	3.4	9.3	Name	Name

Details in Appendix.

ERM Integration

- Training and Awareness Programs
- Embed into Strategic Planning and Decision Making
- Integrate into Operational Processes
- Assign Accountability

Thank you – Let’s Stay Connected!

Durran Dunn

Partner, CPA, CIA

Durran.Dunn@bpcpa.net

Polling Questions – for CPEs

1. What is the most significant barrier your organization faces in operating an effective ERM program?

- Lack of executive buy-in or sponsorship
- Limited resources or budget
- Siloed risk ownership across departments
- Inconsistent risk assessment methodologies
- Lack of a risk-aware culture
- Other

2. How mature would you rate your organization's current ERM program?

- Initial/ad hoc: Risk management is informal and reactive.
- Developing: Some formal processes are in place, but not fully integrated
- Established: Risk management is structured and integrated with key processes
- Advanced: Risk is embedded in strategic decision-making and performance management
- Not sure

3. What do you consider the most critical component in establishing an effective ERM program?

- Strong tone at the top and executive support
- Clearly defined risk governance and responsibilities
- Integration of risk management into strategic planning
- Robust risk identification and assessment processes
- Use of enabling technology and data analytics
- Other