Federal Enterprise Risk Management Overview – Module 1

ERM training series

AFERM Association for Federal Enterprise Risk Management

EY Building a better working world

Today's Presenters

Baback Bazri, CISA, CISSP

Mr. Baback Bazri is a Principal in Ernst & Young LLP (EY) Government and Public Sector (GPS) Consulting Services practice. Mr. Bazri is the EY GPS Risk Leader, for which he oversees all risk management services, to include enterprise risk management, data privacy and protection risk, cybersecurity, governance, risk and compliance (GRC) activities, and mission risk for all EY Federal clients. He is recognized for organizing, simplifying and managing risk frameworks to provide organizational value, efficiencies and cost savings.

Kamalu Nkele, M.Fin., CISA, RIMS-CRMP-FED, PMI-RMP

Kamalu is a Manager with EY's Government and Public Sector practice where he specializes in enterprise and information systems risk management. Kamalu has centered his experience around creating collaborative risk management solutions across several federal agencies while aligning with OMB Circular A-123, the COSO Enterprise Risk Management Integrated Framework, NIST, the GAO Greenbook and other industry leading guidance.

Caroline Hudson-Hale, CISSP

Caroline is a Senior in EY's GPS practice, where she focuses on strategic management of risk, performance, and security for the federal government. She brings five years of Governance, Risk, and Compliance (GRC) access management and process control experience in commercial professional services and manufacturing sectors to her agency clients.

Transforming enterprise risk management into a competitive advantage

Enterprise risk management, or ERM, is evolving and the expectations for it are rapidly increasing. Traditional ERM frameworks with a narrow focus on "protecting" the enterprise and passive "heat map" risk reporting may not meeting agency needs and expectations. Federal organizations want and need more from ERM. A forward thinking ERM framework is uniquely positioned to meet these evolving desires.

Notably, as Federal organizations' expectations continue to increase, ERM continues to gain higher visibility and interest at all levels of government. This means that ERM will continue to be a strategic priority for agencies.

Focusing on this ERM paradigm shift and elevated visibility, this series of ERM training sessions is designed as an opportunity to provide an in-depth look at how to evolve to a forward thinking ERM program. After completing the series of ERM training sessions ERM professionals will be able to:

- Discuss how ERM benefits leadership
- Identify ERM opportunities for improvement
- Implement advanced ERM thinking

Session Objectives

Module 1 – Federal ERM Training for ERM professionals, will provide an overview of ERM principles. At the end of this session participants will have the foundational knowledge to apply the key elements of the program. Specifically participants should be able to:

- Define enterprise risk management (ERM)
- Highlight the forces that are leading to transformation of ERM programs
- Provide a ERM process overview, highlighting key activities and deliverables
- Describe key activities needed to sustain a forward thinking ERM Program
- Describe the key differences between Internal Audit (IA) and ERM risk activities

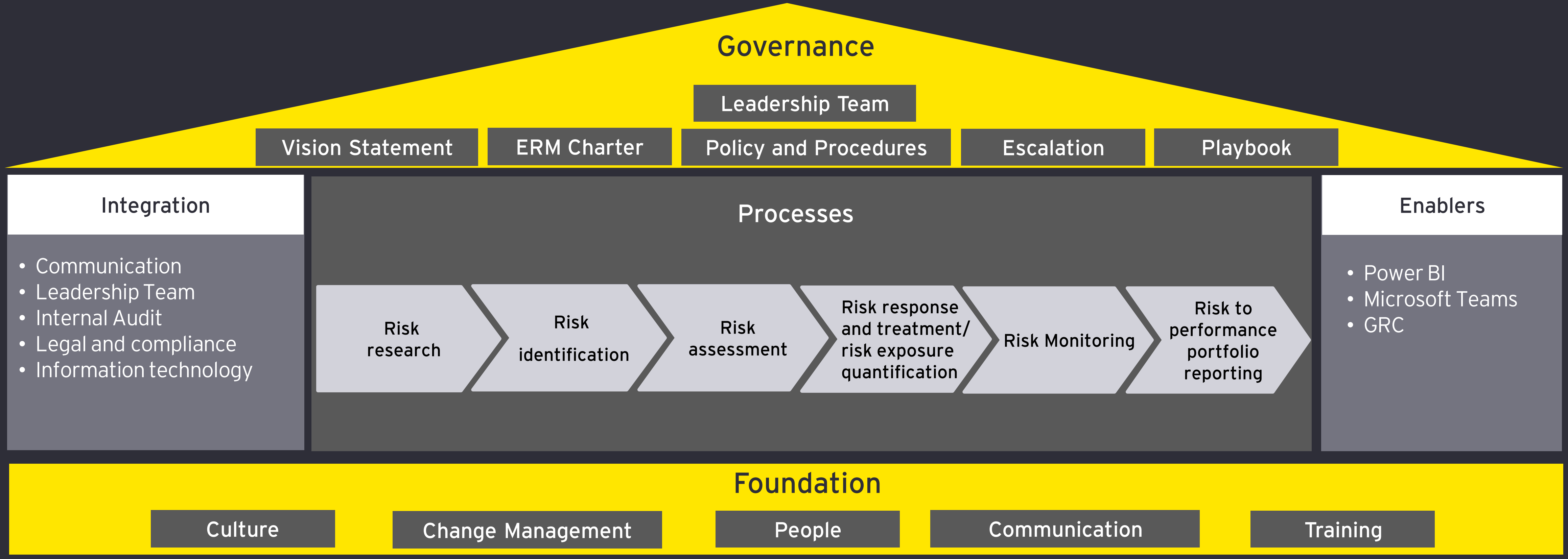
RISK: A **future uncertainty** that has the potential to create a **variance to stated objectives**

Enterprise Risk Management: The culture, capabilities and practices, integrated with strategy-setting and its performance, that organizations rely on to manage risk in creating, preserving and realizing value.[1]

[1] Enterprise Risk Management (ERM) as defined by the Committee of Sponsoring Organizations (COSO)

Functional ERM Framework

ERM is more than a framework – it enables a better foundation for managing risks and communicating about risk across the organization



Governance

Leadership Team

Vision Statement | ERM Charter | Policy and Procedures | Escalation | Playbook

Integration

- Communication
- Leadership Team
- Internal Audit
- Legal and compliance
- Information technology

Processes

Risk research → Risk identification → Risk assessment → Risk response and treatment/ risk exposure quantification → Risk Monitoring → Risk to performance portfolio reporting

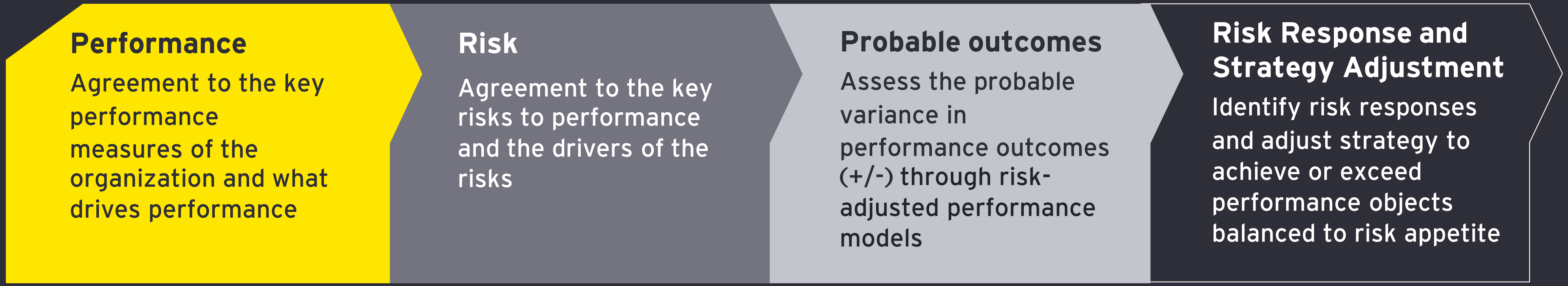
Enablers

- Power BI
- Microsoft Teams
- GRC

Foundation

Culture | Change Management | People | Communication | Training

ERM methodologies focus on the achievement of strategic goals and performance objectives



Performance

Agreement to the key performance measures of the organization and what drives performance

Risk

Agreement to the key risks to performance and the drivers of the risks

Probable outcomes

Assess the probable variance in performance outcomes (+/-) through risk-adjusted performance models

Risk Response and Strategy Adjustment

Identify risk responses and adjust strategy to achieve or exceed performance objects balanced to risk appetite

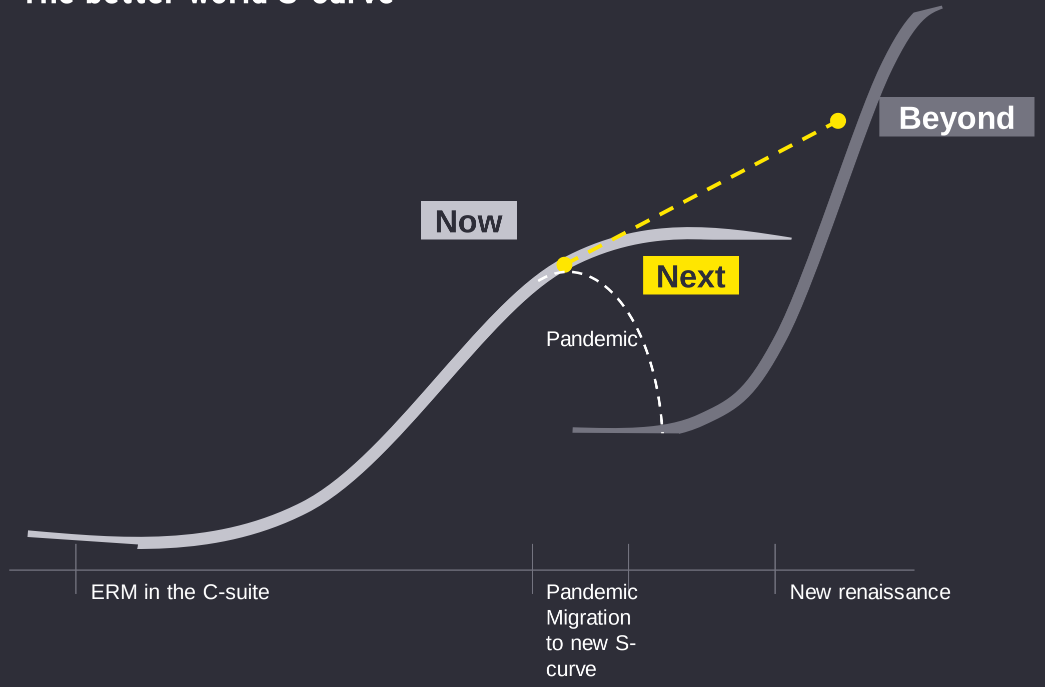
Why it matters to organizations?

This methodology demonstrates the alignment between the performance dimensions that an organization does not want to compromise and its enterprise risks.

This enhanced alignment supports informed decision-making on what actions to augment, eliminate or exploit in order to increase the probability of executing to or beyond performance targets.

The goal of ERM is to equip leaders with the risk insights needed to support decision-making and deliver business results

The better world S-curve



Now

Rapid impact and readiness assessment

- Rapid assessment to diagnose pain points
- Understand the gaps where assistance should be allocated given limited resources

Pandemic-driven risk review (PDRR)

- Evaluate the impact of the pandemic on an organization's risk profile
- Capture new risks that are surfacing connected with the pandemic
- Review and develop response plans appropriately

Next

Scenario and response planning

- Model scenario outcomes and quantify exposures to assist objective risk-enabled decision-making across the organization
- Redefine risk tolerance
- Consider risk and reward more easily

Risk intelligence and monitoring

- Use key risk indicators (KRIs) to support active risk monitoring
- Develop efficient KRI update processes that inform leaders with relevant and timely information

Beyond

ERM program transformation

- Cement ERM as a value-added business function
- Recap lessons learned and advise on improved frameworks, processes and technical requirements
- Prepare ERM to play a larger role in creating cultural awareness of risk

Advanced ERM

- Continuously align processes with the evolving environment
- Stay updated with industry/ regulatory standards
- Enhanced real-time risk dashboards enabled by automation technology and visualization tools

Forward thinking ERM programs surpass "traditional" ERM

1	2	3	4
Data-driven risk insights; quantitative risk exposure informs resource allocation decisions	Risk embedded into strategic planning/ confidence to take and benefit from risks	Objective risk monitoring and reporting focused on sustainable growth and performance	Enhanced governance; risk escalation routines, defined risk tolerance and performance (risk) appetite
► Develop clearer risk ownership ► Enable three-lines-of-defense organizational model to sustain solutions and focus on high-value risk areas ► Enable coordinated risk processes	► Find the opportunity in risk ► Benefit from the upside potential of risk ► Drive performance and value-creation through risk opportunities	► Reduce the downside potential of risk ► Develop mature and predictive risk management practices ► More effectively leverage technology to efficiently manage risk	► Anticipate and predict risks ► Gather and interpret risk insights to make better decisions ► Improve ability to provide a comprehensive view of risk to decision-makers

Knowledge check 1

What are the key market focuses that are resulting in the transformation of "traditional" ERM frameworks?

A. Technology disruption

B. Changing business models

C. Increasing leadership focus

D. Budget priorities

E. All of the above

Knowledge check 1 - Answer

What are the key market focuses that are resulting in the transformation of “traditional” ERM frameworks?

A. Technology disruption

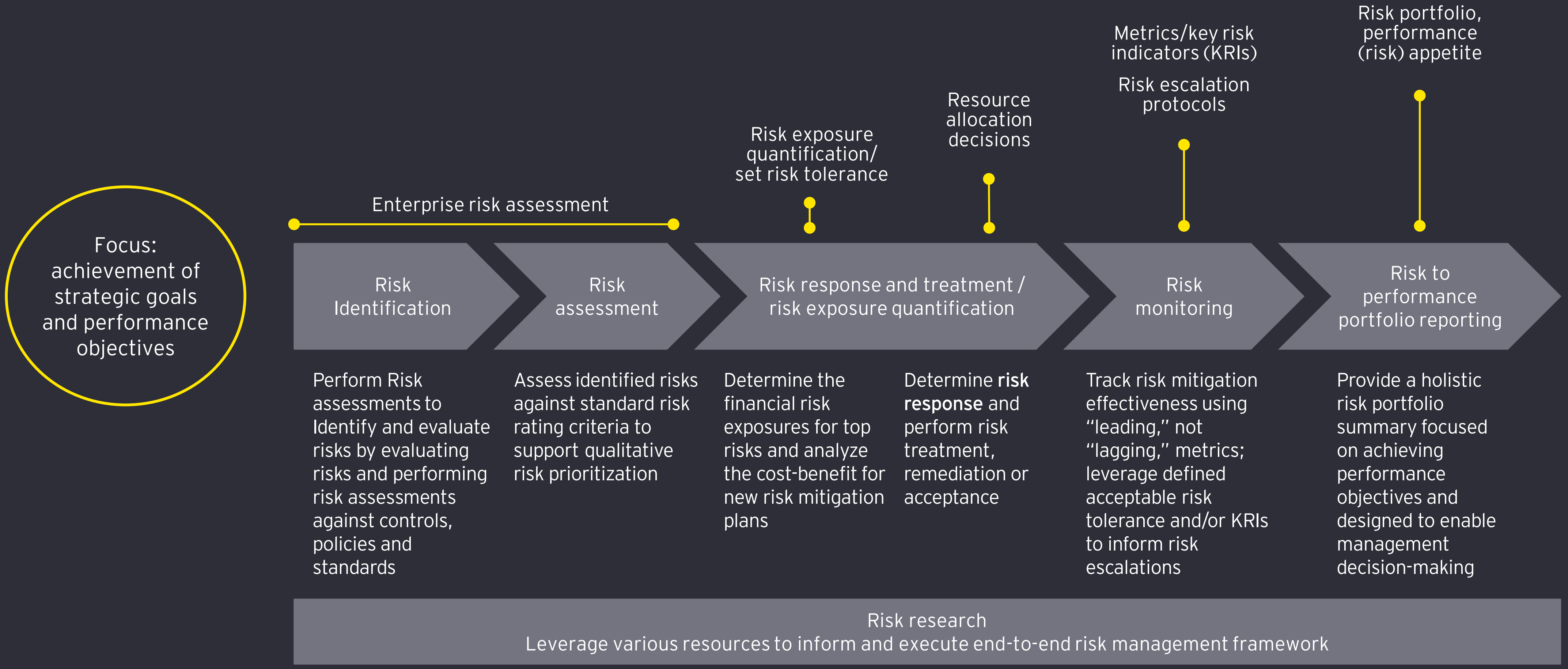
B. Changing business models

C. Increasing leadership focus

D. Budget priorities

[✓ E. All of the above]

ERM end-to-end life cycle



Focus: achievement of strategic goals and performance objectives

Enterprise risk assessment

Risk Identification

Perform Risk assessments to Identify and evaluate risks by evaluating risks and performing risk assessments against controls, policies and standards

Risk assessment

Assess identified risks against standard risk rating criteria to support qualitative risk prioritization

Risk exposure quantification/ set risk tolerance

Resource allocation decisions

Risk response and treatment / risk exposure quantification

Determine the financial risk exposures for top risks and analyze the cost-benefit for new risk mitigation plans

Determine **risk response** and perform risk treatment, remediation or acceptance

Metrics/key risk indicators (KRIs)

Risk escalation protocols

Risk monitoring

Track risk mitigation effectiveness using "leading," not "lagging," metrics; leverage defined acceptable risk tolerance and/or KRIs to inform risk escalations

Risk portfolio, performance (risk) appetite

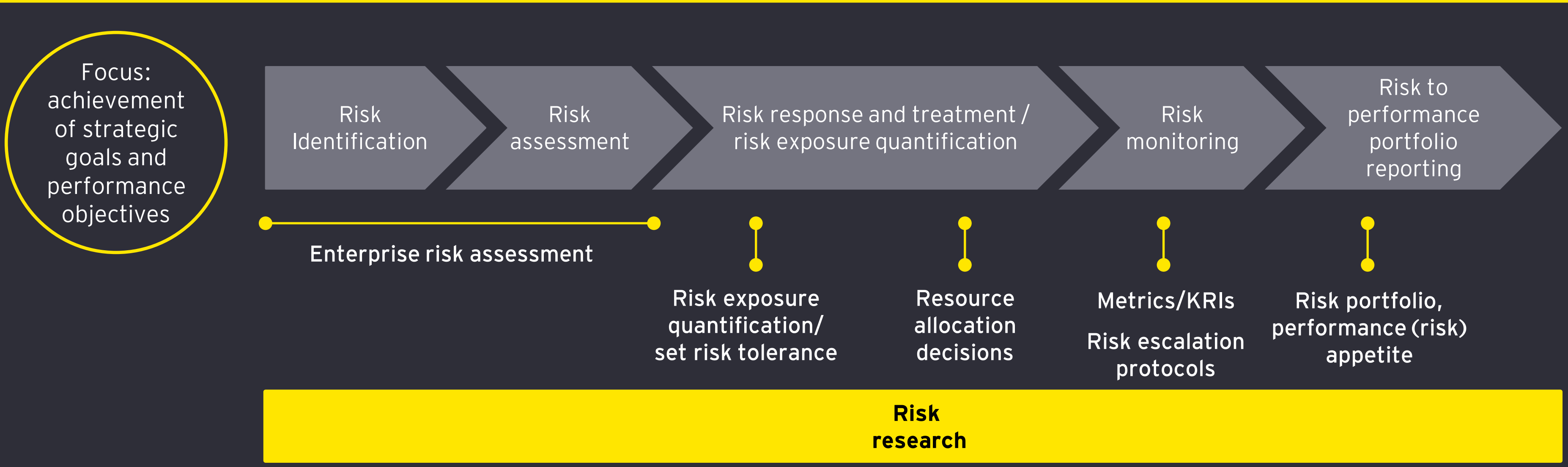
Risk to performance portfolio reporting

Provide a holistic risk portfolio summary focused on achieving performance objectives and designed to enable management decision-making

Risk research

Leverage various resources to inform and execute end-to-end risk management framework

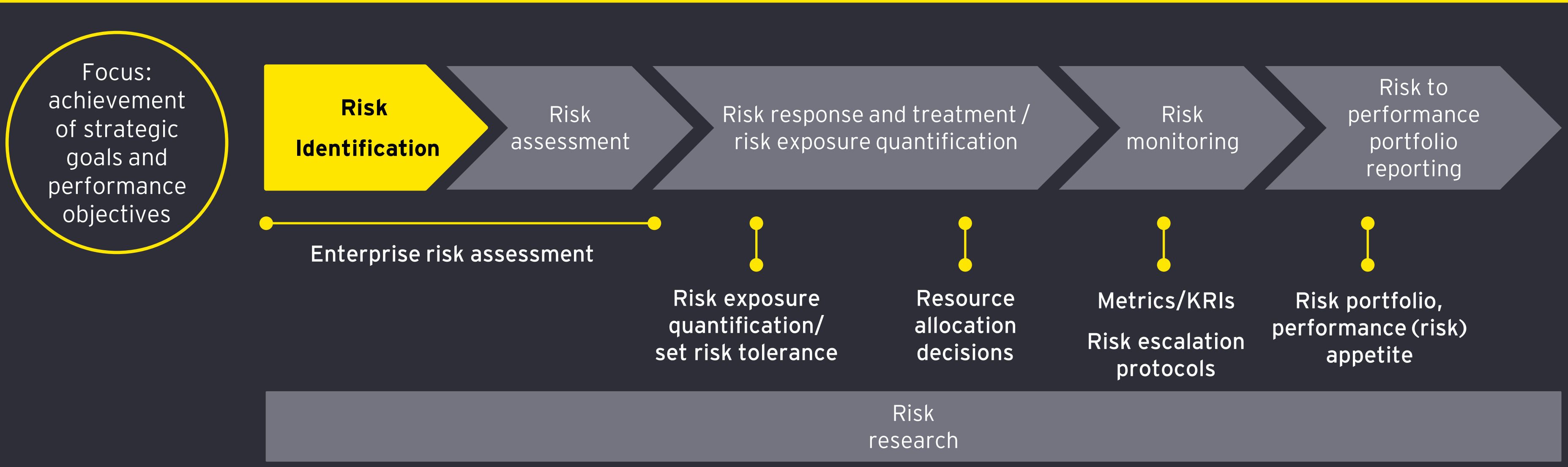
Risk research


Focus: achievement of strategic goals and performance objectives
Risk Identification
Risk assessment
Risk response and treatment / risk exposure quantification
Risk monitoring
Risk to performance portfolio reporting
Enterprise risk assessment
Risk exposure quantification/ set risk tolerance
Resource allocation decisions
Metrics/KRIs
Risk escalation protocols
Risk portfolio, performance (risk) appetite
Risk research

Key activities

- Leverage various resources and tools to research new risks or opportunities facing your agency
- Discover risks or opportunities that have not been previously identified
- Consider emerging risks within your agency
- Map the current risk portfolio to the risk universe to identify any risk previously unidentified

Risk identification


Focus: achievement of strategic goals and performance objectives
Risk Identification
Risk assessment
Risk response and treatment / risk exposure quantification
Risk monitoring
Risk to performance portfolio reporting
Enterprise risk assessment
Risk exposure quantification/ set risk tolerance
Resource allocation decisions
Metrics/KRIs
Risk escalation protocols
Risk portfolio, performance (risk) appetite
Risk research

Key activities

- Identify and report risks and/or opportunities to the achievement of strategic goals and objectives
- Think broadly and consider risks and opportunities within the following risk categories:
  - Strategic
  - Operational
  - Compliance
  - Financial
- Collect and document key risk information, including:
  - The risk name
  - Definition of the risk (scenario)
  - What are the root cause(s) of the risk/opportunity?
  - How will the risk/opportunity impact performance?
  - What are the current and/or potential mitigation efforts?

Knowledge check 2

How does ERM demonstrate alignment on goals and performance objective?

A. Agreeing on key performance measure
B. Identifying key risks and drivers to achieving performance objectives
C. Assessing probable variances in performance outcomes
D. Identifying risk owners
E. A, B and C
F. All of the above

Knowledge check 2 - Answer

How does ERM demonstrate alignment on goals and performance objective?

A. Agreeing on key performance measure

B. Identifying key risks and drivers to achieving performance objectives

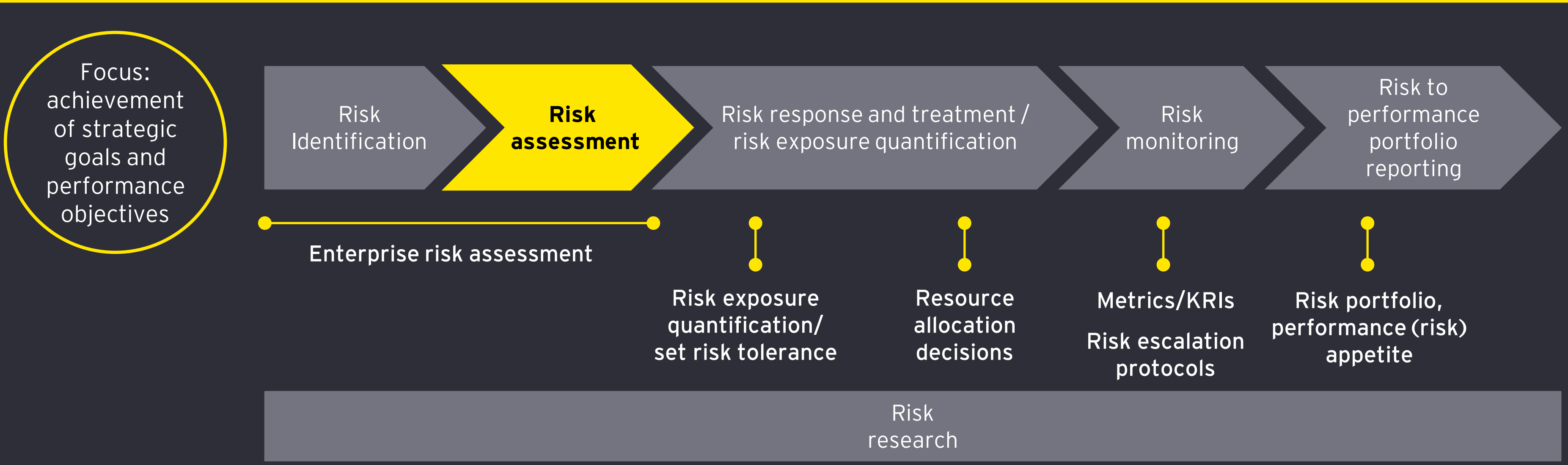
C. Assessing probable variances in performance outcomes

D. Identifying risk owners

E. A, B and C

[✓ F. All of the above]

Risk assessment



Focus: achievement of strategic goals and performance objectives

Risk Identification

Risk assessment

Risk response and treatment / risk exposure quantification

Risk monitoring

Risk to performance portfolio reporting

Enterprise risk assessment

Risk exposure quantification/ set risk tolerance

Resource allocation decisions

Metrics/KRIs

Risk escalation protocols

Risk portfolio, performance (risk) appetite

Risk research

Key activities

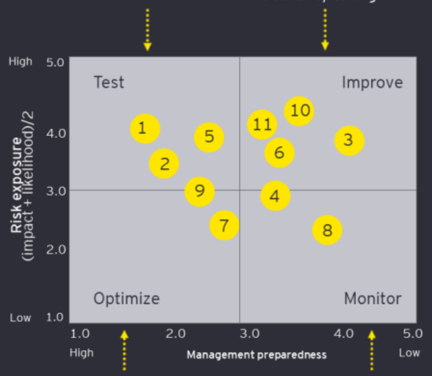
- ► Align on top risks and opportunities
- ► Assess risks using a consistent five-point rating scale for the following criteria:
    - ○ Impact (strategic, operational, reputational, regulatory/compliance, financial)
    - ○ Likelihood
    - ○ Management preparedness
- ► Categorize the risks on the appropriate level of potential improvement and/or monitoring efforts (improve, test, monitor, optimize)

New ERM methodologies move beyond "heat map" reporting and instead use insightful 2x2 action matrices designed to promote end-to-end risk management.

Illustrative

Risks in this quadrant inform the basis of the audit plan

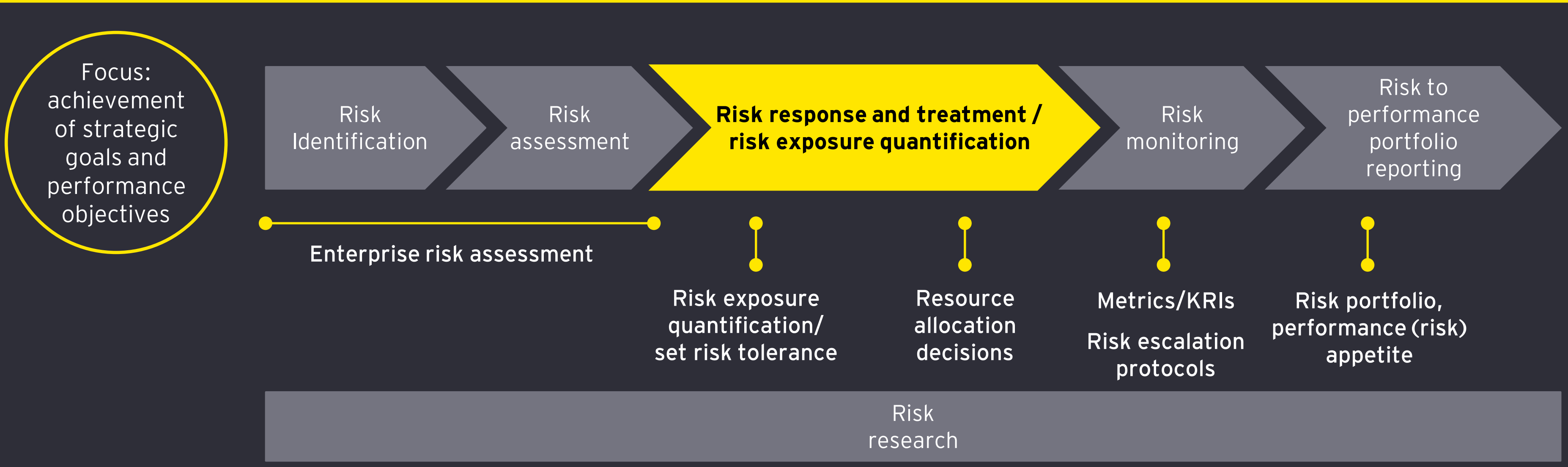
Risks in this quadrant should be the focus of executive management and board reporting



Risks in this quadrant are potentially "over-managed;" evaluate and reallocate resources, if necessary

Risks in this quadrant include emerging risks, requiring ongoing monitoring

Risk response and treatment - risk exposure quantification

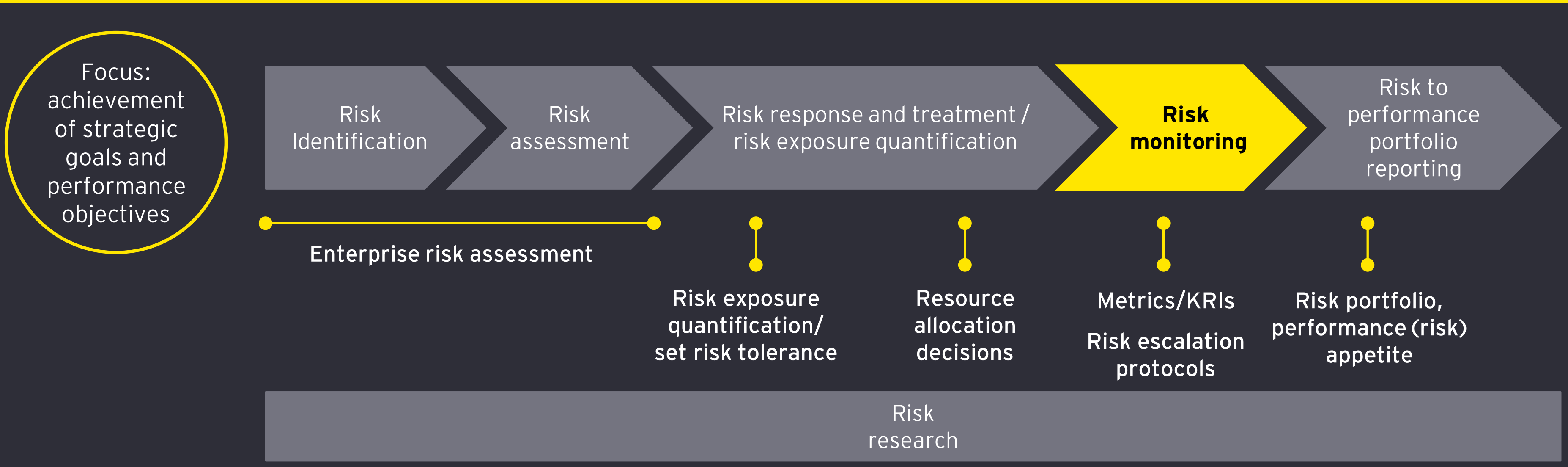


Focus: achievement of strategic goals and performance objectives
Risk Identification
Risk assessment
Risk response and treatment / risk exposure quantification
Risk monitoring
Risk to performance portfolio reporting
Enterprise risk assessment
Risk exposure quantification/ set risk tolerance
Resource allocation decisions
Metrics/KRIs
Risk escalation protocols
Risk portfolio, performance (risk) appetite
Risk research

Key activities

- Determine the risk response to determine the risk treatment, remediation or acceptance
- Risk owners, supported by the ERM team, determine the financial risk exposure for respective risk(s) via a structured workshop process that:
  - Identifies four to six specific risk scenarios
  - Quantifies risk exposure (leading practice)
  - Identifies and procures both internal and external data to substantiate the risk quantification
  - Incorporates input from internal and subject-matter resources (SMRs) to substantiate the risk quantification
  - Calculates the risk exposure using Monte Carlo simulations for each of the defined scenarios
  - Makes sure risk owners "own" the results

Risk monitoring



Focus: achievement of strategic goals and performance objectives
Risk Identification
Risk assessment
Risk response and treatment / risk exposure quantification
Risk monitoring
Risk to performance portfolio reporting
Enterprise risk assessment
Risk exposure quantification/ set risk tolerance
Resource allocation decisions
Metrics/KRIs
Risk escalation protocols
Risk portfolio, performance (risk) appetite
Risk research

Key activities

- Build upon the financial risk exposure analysis and establish ongoing tracking metrics
- Respective risk owners, supported by the ERM department, will establish:
  - Three to five KRIs
  - Risk tolerances
- Respective risk owners are responsible for updating a "risk owner dashboard" that summarizes:
  - The risk drivers
  - The financial exposure
  - Risk mitigation activities, both current and proposed
  - Data metrics

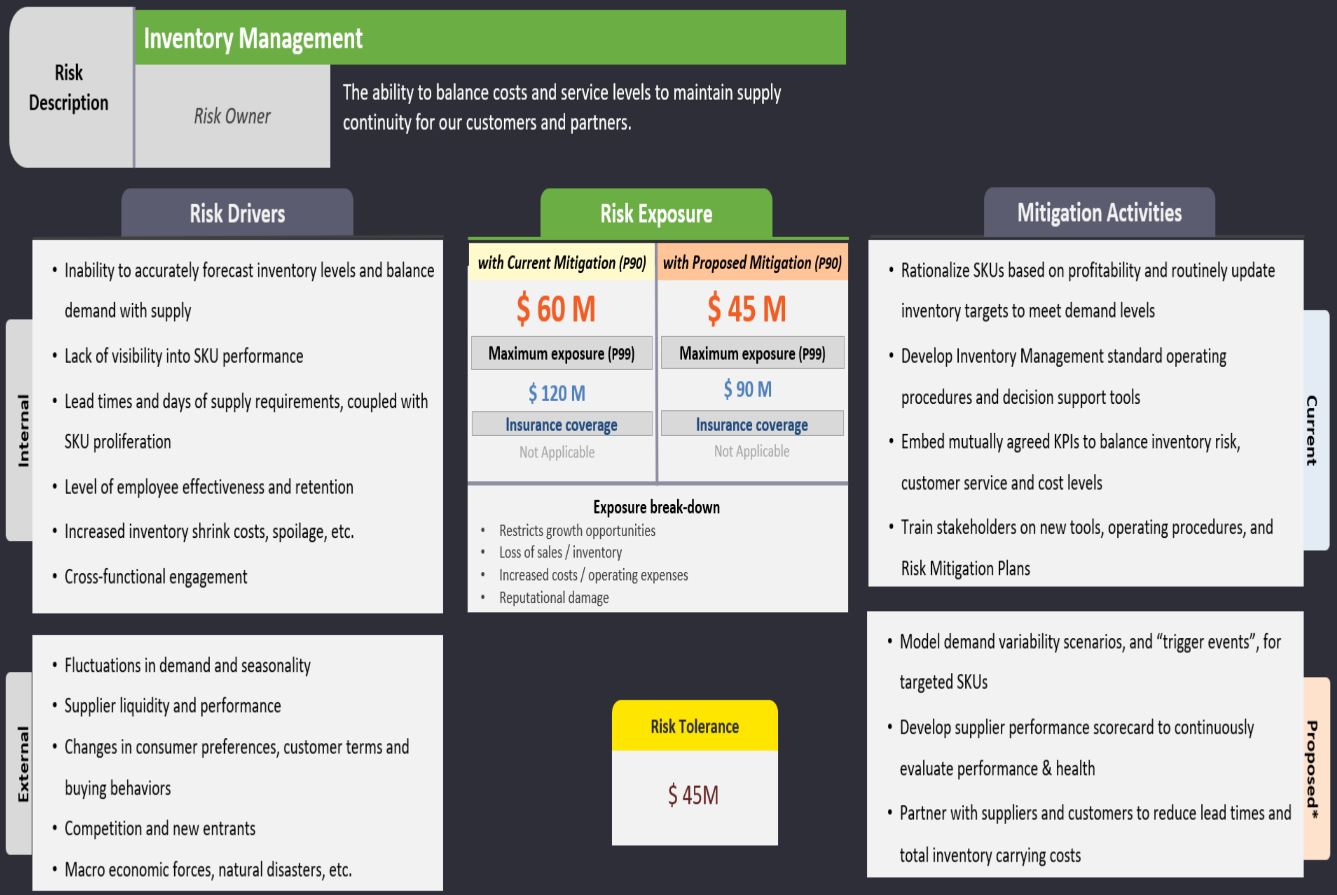
ERM enables insightful risk dashboard monitoring

The ERM team quantifies financial risk exposures for top risks

Why a risk dashboard matters to organizations:

- Quantifies the financial risk exposure for top risks
- Supports actionable risk tolerance discussion based on objectivity, not subjectivity
- Informs cost-versus-benefit decisions to prioritize risk mitigation investments

Illustrative ERM risk dashboard



Risk Description

Inventory Management

Risk Owner

The ability to balance costs and service levels to maintain supply continuity for our customers and partners.

Risk Drivers

Internal

- Inability to accurately forecast inventory levels and balance demand with supply
- Lack of visibility into SKU performance
- Lead times and days of supply requirements, coupled with SKU proliferation
- Level of employee effectiveness and retention
- Increased inventory shrink costs, spoilage, etc.
- Cross-functional engagement

External

- Fluctuations in demand and seasonality
- Supplier liquidity and performance
- Changes in consumer preferences, customer terms and buying behaviors
- Competition and new entrants
- Macro economic forces, natural disasters, etc.

Risk Exposure

with Current Mitigation (P90)	*with Proposed Mitigation (P90)*
$ 60 M	$ 45 M
Maximum exposure (P99)	Maximum exposure (P99)
$ 120 M	$ 90 M
Insurance coverage	Insurance coverage
Not Applicable	Not Applicable

Exposure break-down

- Restricts growth opportunities
- Loss of sales / inventory
- Increased costs / operating expenses
- Reputational damage

Risk Tolerance

$ 45M

Mitigation Activities

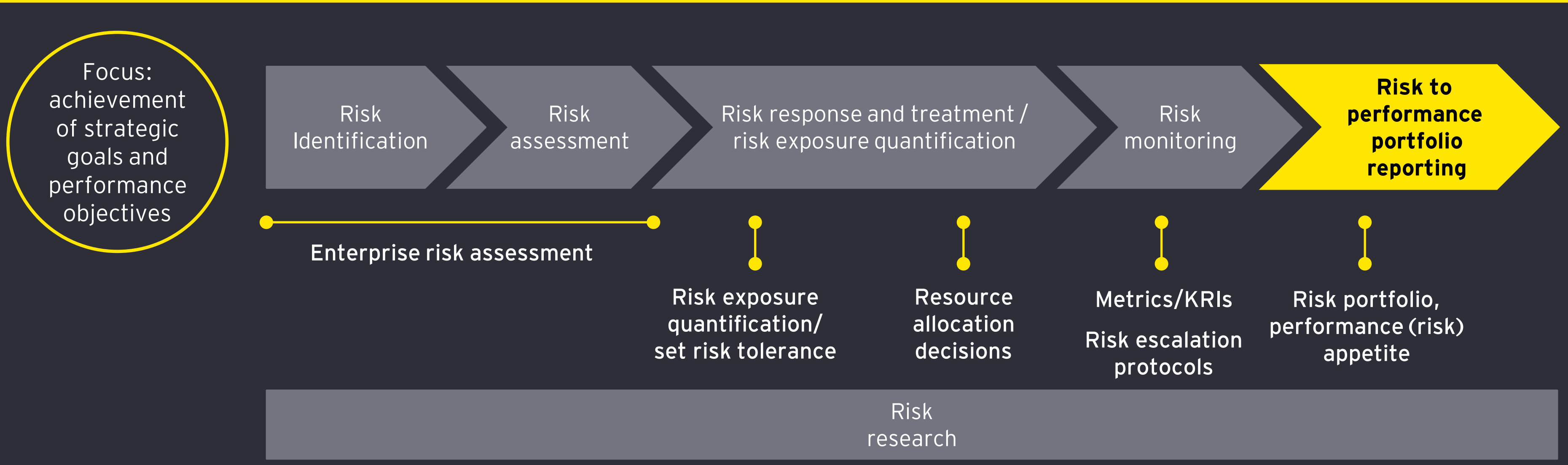
Current

- Rationalize SKUs based on profitability and routinely update inventory targets to meet demand levels
- Develop Inventory Management standard operating procedures and decision support tools
- Embed mutually agreed KPIs to balance inventory risk, customer service and cost levels
- Train stakeholders on new tools, operating procedures, and Risk Mitigation Plans

Proposed*

- Model demand variability scenarios, and "trigger events", for targeted SKUs
- Develop supplier performance scorecard to continuously evaluate performance & health
- Partner with suppliers and customers to reduce lead times and total inventory carrying costs

Risk to performance portfolio reporting



Focus: achievement of strategic goals and performance objectives

Risk Identification

Risk assessment

Risk response and treatment / risk exposure quantification

Risk monitoring

Risk to performance portfolio reporting

Enterprise risk assessment

Risk exposure quantification/ set risk tolerance

Resource allocation decisions

Metrics/KRIs

Risk escalation protocols

Risk portfolio, performance (risk) appetite

Risk research

Key activities

- The ERM team will aggregate the individual risk exposures into a summarized risk portfolio perspective.
- During existing meetings, the executive risk team (e.g., ERC/RMC) will review the risk portfolio and reach consensus on:
  - Individual risk tolerances
  - The inorganization's risk appetite
- To support actionable resource allocation decisions during these executive risk meetings, the risk owners should include the following information in the executive risk exposure dashboard:
  - Risk mitigation plans so that risk tolerances are achieved (e.g., what is the “go-to-green” plan?)
  - The required investments ($, people, etc.) to go to green

Knowledge check 3

What is the foundational component of the enterprise risk management life cycle?

A. Risk identification

B. Risk assessment

C. Risk response and risk exposure quantification

D. Risk monitoring

E. Both A & B

F. All of the above

Knowledge check 3 - Answer

What is the foundational component of the enterprise risk management life cycle?

A. Risk identification

B. Risk assessment

C. Risk response and risk exposure quantification

D. Risk monitoring

[✓ E. Both A & B]

F. All of the above

Key success factors to sustain a forward thinking ERM Program

An organization's ERM program will continuously evolve to meet organizational needs. As such, the ERM department conducts regular "sustain" activities throughout the year to make sure the ERM framework is effective, integrated into existing routines and meeting the needs of key stakeholders.

Three key sustaining activities include:

1. Integrating ERM into existing business planning processes
2. Developing appropriate training to help ingrain ERM into the culture
3. Establish an ERM communications strategy to make sure ERM is recognized as an important management process

Knowledge check 4

What are the keys to sustaining an ERM program and framework?

A. Integration into existing routines

B. Training

C. Ongoing communication

D. Employees

E. A, B and C

F. All of the above

Knowledge check 4 - Answer

What are the keys to sustaining an ERM program and framework?

A. Integration into existing routines

B. Training

C. Ongoing communication

D. Employees

[✓ E. A, B and C]

F. All of the above

Internal Audit (IA) Risk Assessment and ERM Risk Assessment objectives and differences

Given the alignment of internal controls and ERM under OMB Circular A-123, there are often synergies in the risk assessment process that can be obtained jointly in the data collection process and meetings with common stakeholders. Although objectives, process and focus on risk mitigation can differ, as noted below, synergies can be gained from conducting integrated risk assessments.

	Enterprise Risk	
	Internal audit (IA)	Enterprise risk management (ERM)
Objective	▸ **Identify auditable risks and provide reasonable assurance** that controls have been implemented by the business management and are operating effectively.	▸ Align on the top broad/high level/strategic **risks that would impact the organizations ability to deliver its strategic goals and performance management objectives**
Risk assessment process	▸ Assess risks against standard risk rating criteria to prioritize risks that can be audited.	▸ Assess risks against risk rating criteria to prioritize top risks (i.e., broad and high level) facing the whole organization.
Risk mitigation	▸ Provides assurance that internal controls, policies, procedures, activities are in place for the organization to achieve financial, operational, and compliance objectives.	▸ **Align on an actionable risk profile** that categorizes risk response actions (improve, test, monitor, optimize) ▸ **Prioritize risk mitigation activities on 'improve' risks**

Typical challenges Agencies face in their ERM programs

1. **Bolt-on:** Stand-alone activity not linked to strategy and conducted outside of the “rhythm of the business;” ERM not explicitly linked to strategic planning and annual planning activities

2. **Process:** Qualitative: lacks the usage of objective key risk indicators (KRIs) and quantified risk exposure to support risk informed decision-making, including resource allocation decisions

3. **Compliance-focused:** Check-the-box/paper exercise designed to meet reporting requirements and not to support the achievement of strategic goals and performance management objectives

4. **Engagement and impact:** Stops at enterprise risk assessment (ERA): heavy, manual surveys centered on data collection and risk assessment that takes weeks to months rather than focusing on more value-added risk response planning

5. **Unsustainable governance:** Does not drive accountability for mitigation plans and/or defined risk escalation routines to action dynamic risk management

Awareness of Typical ERM triggers and pain points

Changes in executive management, reporting structures, participants, or other stakeholders leadership positions

- Increased risk management expectations
  - *Communicate value, benefits, roles, and responsibilities*
- Change in strategic direction
  - *Demonstrate the link to performance to validate performance outcomes*

- Inefficient risk assessment process or executive discussions
  - *Focus on meaningful metrics*
- Outdated or misaligned KRIs and KPIs
  - *Refresh data alignment and evaluate data sources*

Shift from qualitative to quantitative analytics

Wrap Up

Questions?