Internal Audit's Role in Enterprise Risk Management

Outline

- Why Enterprise Risk Management
- Definition
- Difference between traditional risk management and ERM
- Roles
- Maturity model
- Enterprise Risk Management - Frameworks
- Enterprise Risk Management - key terms
- Enterprise Risk Management - Risk Categories
- Enterprise Risk Management - Risk Implementation
- Enterprise Risk Management Process
- Enterprise Risk Management – Tools
- Summary
- Conclusion

Why Enterprise Risk Management?

Definition

ERM deals with risks and opportunities affecting value creation or preservation, defined as follows:

COSO

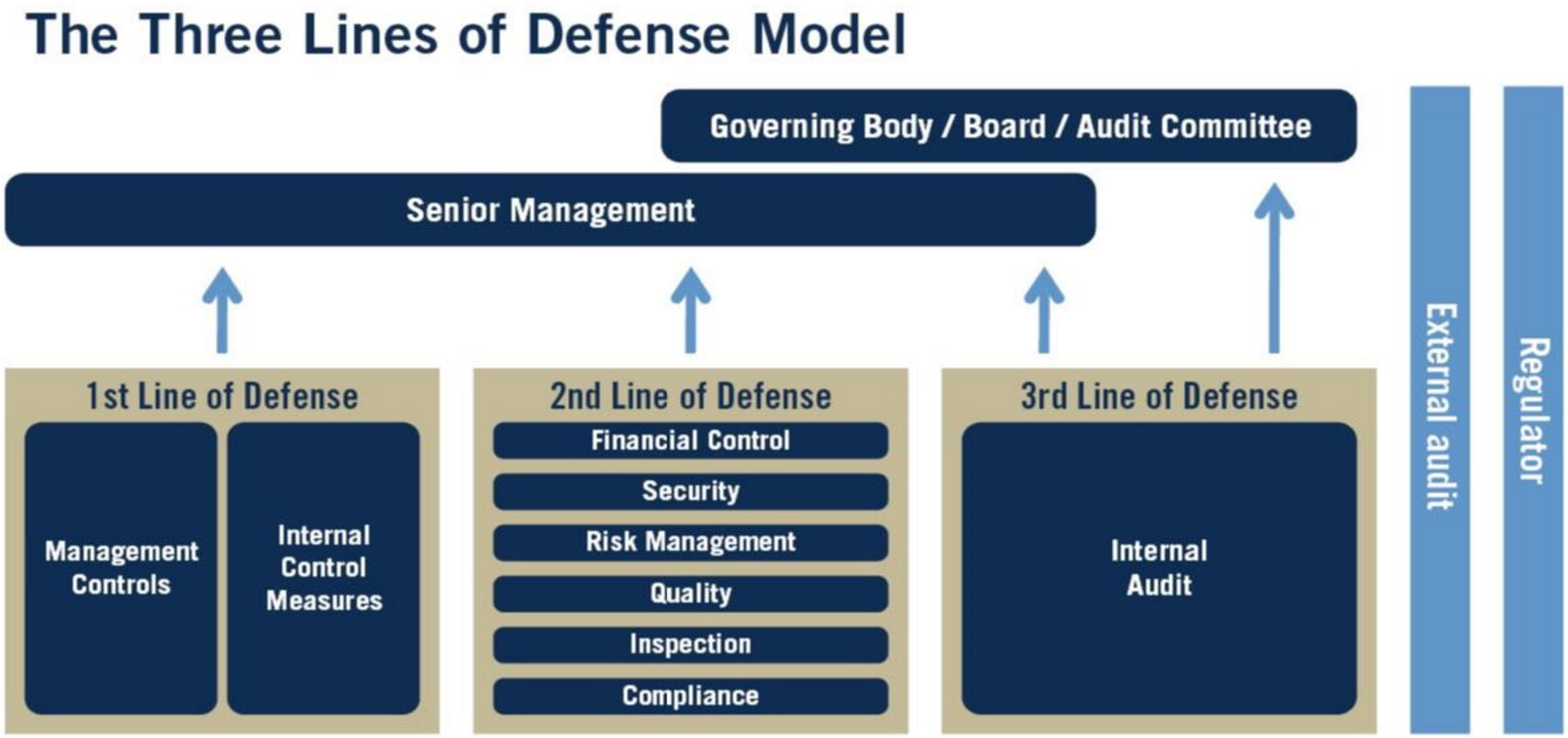
> ERM is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

ERM is the leading approach to managing and optimizing risks, enabling an organization to determine how much uncertainty and risk are acceptable to an organization.

Difference between traditional risk management and ERM

Traditional risk management	Enterprise Risk Management
Fragmented	Integrated
Ad hoc	Continuous
Historical focused	Forward focused
Cost based	Value-based
Risk silos	Systematic
Functionally-driven	Process-driven

Roles – Three Lines of Defense



Source: The Institute of Internal Auditors, Inc.

Roles – Groups involved in Enterprise Risk Management

Risk Governance	**Board of Directors (and the Audit Committee)** • Foster a risk Intelligent culture • Approve risk appetite • Ratify key components of the Enterprise Risk Management (ERM) programme • Discuss enterprise risks with executive management				**Technology (all pervasive):** • Provide periodic/ real-time dashboards to oversee risks • Make monitoring and reporting easier • Support timely maintenance and pre-empt problems • Facilitate risk escalations
Risk Infrastructure and Management	**Executive management:** • Define the risk appetite • Evaluate proposed strategies against risk appetite • Provide timely risk-related information	**Enterprise risk group:** • Aggregate risk information • Identify and assess enterprise risks • Monitor risks and risk response plans	**Internal Audit:** • Provide assurance on effectiveness of the ERM programme, and the controls and risk response plans for significant risks	**Risk Management:** • Create a common risk framework • Provide direction on applying framework • Implement and manage technology systems • Provide guidance and training	
Risk Ownership	**Business units:** • Take intelligent risks • Identify and assess risks • Respond to risks • Monitor risks and report to enterprise risk group		**Support functions:** • Provide guidance/support to the enterprise risk group and business units		

Source: https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/audit/deloitte-uk-erm-a-risk-intelligent-approach.pdf

Roles – Internal auditing's role in ERM

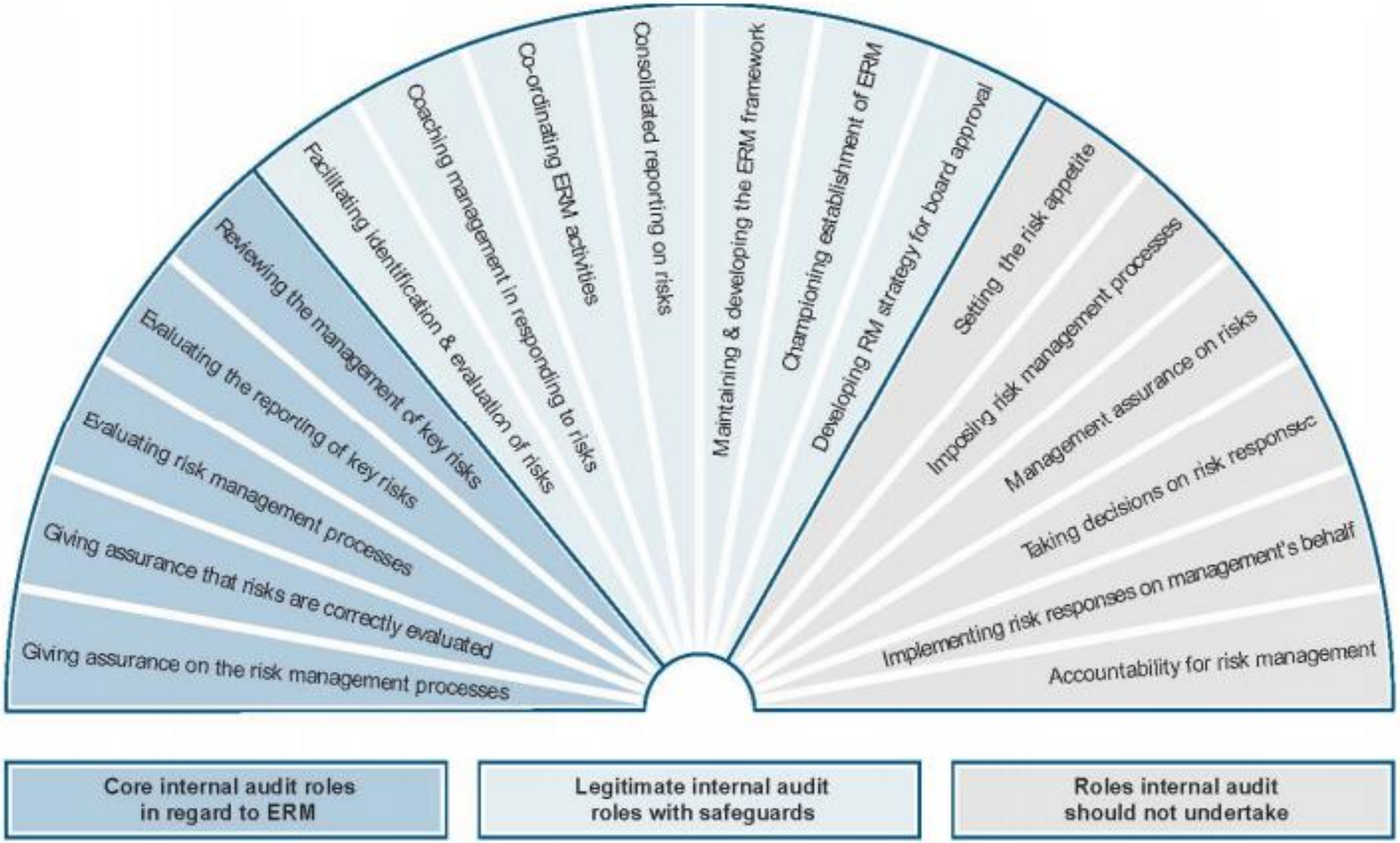
Internal auditors will normally provide assurances on three areas:

1. Risk management processes, both their design and how well they are working;
2. Management of those risks classified as 'key', including the effectiveness of the controls and other responses to them; and
3. Reliable and appropriate assessment of risks and reporting of risk and control status.

Internal audit activity may undertake are the following consulting roles:

1. Making available to management tools and techniques used by internal auditing to risks and controls;
2. Being a champion for introducing ERM into the organization, leveraging its expertise in risk management and control and its overall knowledge of the organization;
3. Providing advice, facilitating workshops, coaching the organization on risk and control and promoting the development of a common language, framework and understanding;
4. Acting as the central point for coordinating, monitoring and reporting on risks; and
5. Supporting managers as they work to identify the best way to mitigate a risk.

Roles – Internal auditing's role in ERM



Source: IIA position paper: The role of internal auditing in Enterprise-wide Risk Management

Roles – Internal auditing's role in ERM

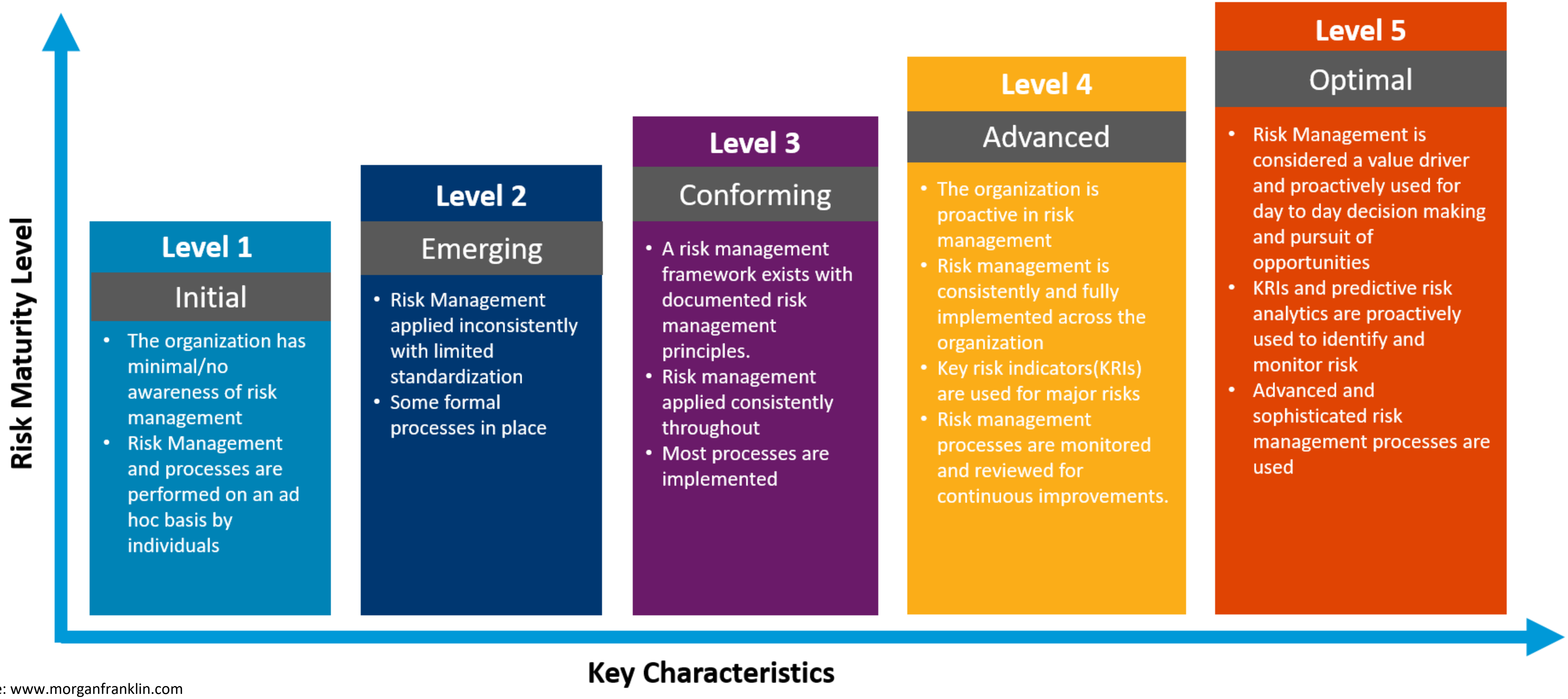
Safeguards

Internal auditing may extend its involvement in ERM, as shown in the previous figure, provided the following conditions apply:

1. It should be clear that management remains responsible for risk management.
2. The nature of internal auditor's responsibilities should be documented in the internal audit charter and approved by the audit committee.
3. Internal auditing should not manage any of the risks on behalf of management.
4. Internal auditing should provide advice, challenge and support to management's decision making, as opposed to taking risk management decisions themselves.
5. Internal auditing cannot also give objective assurance on any part of the ERM framework for which it is responsible. Such assurance should be provided by other suitably qualified parties.
6. Any work beyond the assurance activities should be recognized as a consulting engagement and the implementation standards related to such engagements should be followed.

Maturity model

ERM Maturity Model



Source: www.morganfranklin.com

Enterprise Risk Management Frameworks

There are two well known frameworks:

1. COSO ERM framework
2. ISO 31000

Enterprise Risk Management – Key terms

Risk - A potential event with an undesirable/negative outcome, including the potential failure to capitalize on an opportunity.

Impact - Estimated financial cost that would be realized if a risk event were to occur. It is determined using the impact on revenue over a 36 month period.

Likelihood - The probability that a risk will occur.

Risk appetite - A target level of loss exposure that the organization views as acceptable, given business objectives and resources

Risk tolerance - Degree of variance from the it's risk appetite that the organization is willing to tolerate

Risk owner - The Risk Owner is the individual identified to lead the development and implementation of the Risk Mitigation plan

Risk management framework - components that support and sustain risk management throughout an organization.

Risk profile - A comprehensive view of the risks faced by the organization.

Risk assessment - The process of identifying and analyzing risk.

Risk retention - If an identified Risk is within Risk Retention, then current controls are retained, maintained, and the identified Risk is monitored.

Threat - Something with the potential to cause damage, injury, or loss.

Enterprise Risk Management – Risk Categories

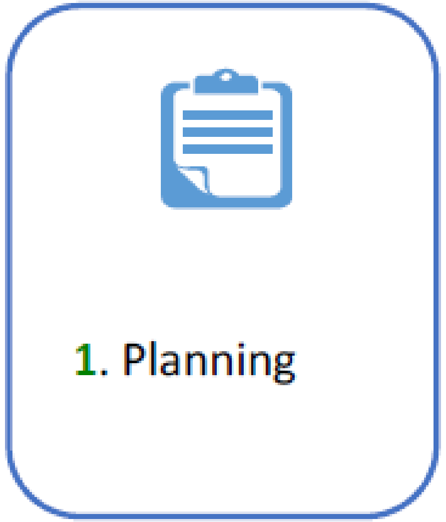
CATEGORY 1 **Preventable Risks**	CATEGORY 2 **Strategy Risks**	CATEGORY 3 **External Risks**
Risks arising from within the company that generate no strategic benefits	Risks taken for superior strategic returns	External, uncontrollable risks
RISK MITIGATION OBJECTIVE		
Avoid or eliminate occurrence cost-effectively	Reduce likelihood and impact cost-effectively	Reduce impact cost-effectively should risk event occur
CONTROL MODEL		
Integrated culture-and-compliance model: Develop mission statement; values and belief systems; rules and boundary systems; standard operating procedures; internal controls and internal audit	Interactive discussions about risks to strategic objectives drawing on tools such as: • Maps of likelihood and impact of identified risks • Key risk indicator (KRI) scorecards Resource allocation to mitigate critical risk events	“Envisioning” risks through: • Tail-risk assessments and stress testing • Scenario planning • War-gaming

Enterprise Risk Management Implementation

Figure 1: **ERM Implementation Steps**

The implementation in five phases as shown below:

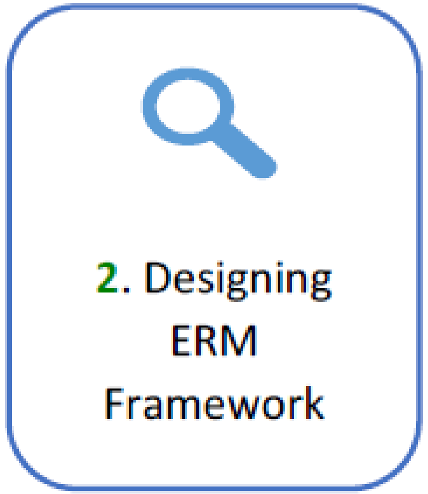
Enterprise Risk Management Implementation



Phase one – Planning the Project:

Focuses on identifying the project implementation team, establishing and reviewing agreements, planning and organizing the tasks.

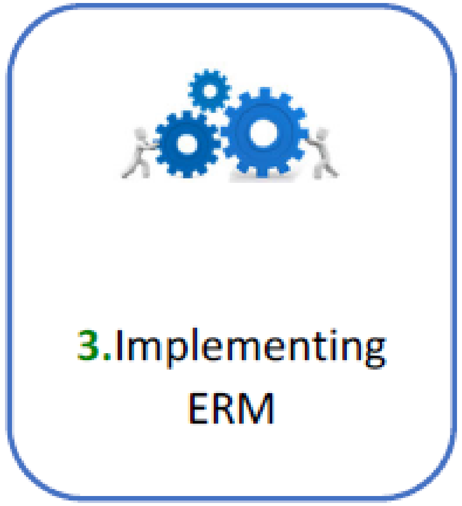
Enterprise Risk Management Implementation



Phase two – Designing ERM Framework:

Focuses on the design and development of overarching ERM governance including org. structure, ERM policy, risk classification system, common risk terminology, and tools and templates.

Enterprise Risk Management Implementation



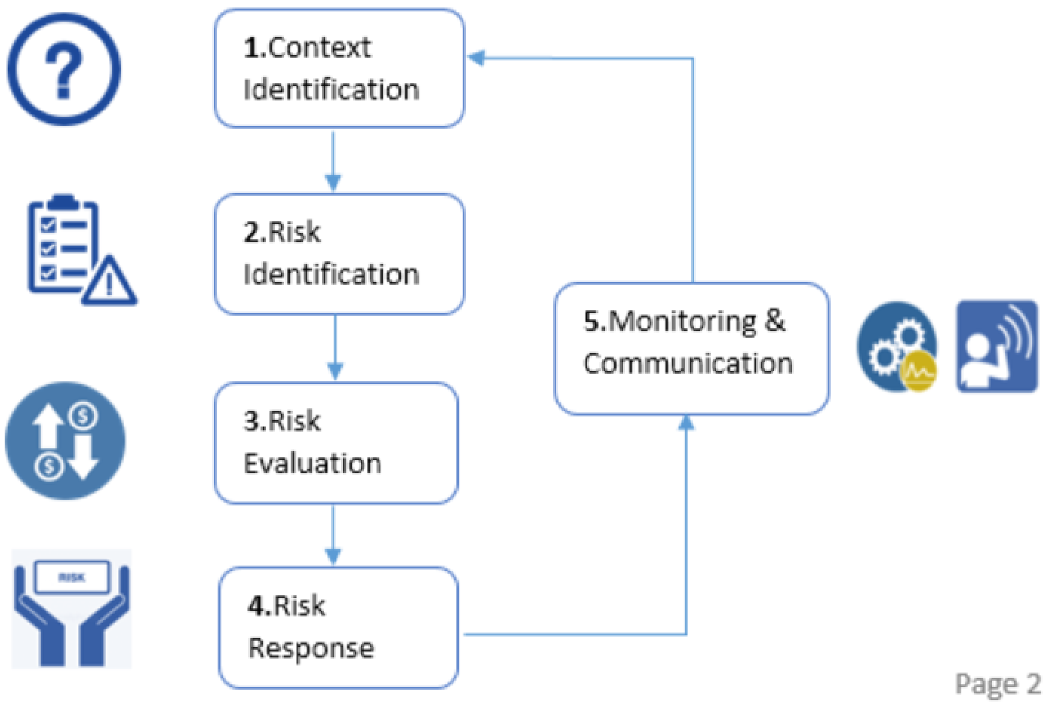
Phase three – Implementing ERM:

Phase three – Implementing ERM:

Focuses on identifying, evaluating, documenting and reviewing the organization’s risk portfolio. It also involves developing and monitoring responses to the identified risks. Activities in this phase are as shown in the following diagram:

Enterprise Risk Management Process

Figure 2: ERM Process



Page 2 o

1. Context Identification – Leadership identifies the context with reference to which risks will be identified e.g. strategic objectives, business process, auditable entities, or entire enterprise.

2. Risk Identification – Leadership identifies enterprise risks and their sub-related risks within the identified context.

3. Risk Evaluation – Leadership prioritizes risks based on impact, likelihood and/or other dimension.

4. Risk Response – Leadership assesses the controls in place, determines and implements appropriate activities, tools or other mechanism to modify the risks to a tolerable level.

5. Monitoring & Communication – Leadership reviews risks and risk action plans for ongoing effectiveness, communicating with stakeholders, and learning from experience.

Enterprise Risk Management Implementation

4. Measuring

Phase four – Measuring:

Focuses on identifying the effectiveness of the ERM framework. Activities in this phase include:

a. Monitor and review risk performance indicators to evaluate ERM contribution.

b. Review the risk awareness within the enterprise.

c. Review the alignment of risk management within the organization’s activities.

Enterprise Risk Management Implementation

Phase five – Learning:

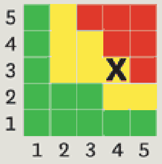
Focuses on identifying the effectiveness of the ERM framework. Activities in this phase include:

a. Report ERM implementation results to stakeholders.

b. Use feedback to make improvements to the ERM framework.

c. Align ERM with other management tasks.

Enterprise Risk Management – Tools

STRATEGIC OBJECTIVE	RISK EVENT	OUTCOMES	RISK INDICATORS	LIKELIHOOD/ CONSEQUENCES	MANAGEMENT CONTROLS	ACCOUNTABLE MANAGER
Guarantee reliable and competitive supplier-to-manufacturer processes	Interruption of deliveries	Overtime Emergency freight Quality problems Production losses	Critical items report Late deliveries Incoming defects Incorrect component shipments		Hold daily supply chain meeting with logistics, purchasing, and QA Monitor suppliers' tooling to detect deterioration Risk mitigation initiative: Upgrade suppliers' tooling Risk mitigation initiative: Identify the key supply chain executive at each critical supplier	Mr. O. Manuel, director of manufacturing logistics

STRATEGIC OBJECTIVE	ASSESSED RISKS	CRITICAL RISKS	TREND
Achieve market share growth	4	1	↔
Satisfy the customer's expectations	11	4	↑
Improve company image	13	1	↔
Develop dealer organization	4	2	↔
Guarantee customer-oriented innovations management	5	2	↓
Achieve launch management efficiency	1	0	↔
Increase direct processes efficiency	4	1	↔
Create and manage a robust production volume strategy	2	1	↓
Guarantee reliable and competitive supplier-to-manufacturer processes	9	3	↔
Develop an attractive and innovative product portfolio	4	2	↓

Risk Event Card

The organization uses risk event cards to assess its strategy risks. First, managers document the risks associated with achieving each of the company's strategic objectives. For each identified risk, managers create a risk card that lists the practical effects of the event's occurring on operations. Below is a sample card looking at the effects of an interruption in deliveries, which could jeopardize the organization's strategic objective of achieving a smoothly functioning supply chain.

Risk Report Card

The organization summarizes its strategy risks on a Risk Report Card organized by strategic objectives (excerpt below). Managers can see at a glance how many of the identified risks for each objective are critical and require attention or mitigation. For instance, the organization identified 11 risks associated with achieving the goal "Satisfy the customer's expectations." Four of the risks were critical, but that was an improvement over the previous quarter's assessment. Managers can also monitor progress on risk management across the company.

Enterprise Risk Management – Tools

Risks		Current Management and Mitigation	Risk Rating with Existing Controls	Changes to Controls	Change to Control Effectiveness	Risk Rating after Changes to Controls	Accountable Person/Department
1	Domestic terrorism (animal rights activists, eco-terrorists, stem-cell research opponents, etc.)	System-wide liaison with law enforcement; additional training of campus law enforcement; improved security measures; hardening of buildings; communication and response protocols	Adequately controlled	Continue current efforts with current controls.	No Change	Adequately controlled	UC Police
2	Catastrophic natural event (earthquake, fire, etc.)	Mission continuity UC Ready; seismic safety and retrofitting programs; emergency management	Potentially poorly controlled	Continue current efforts with current controls.	No Change	Potentially poorly controlled	EH&S
3	Pandemic	Mission continuity UC Ready	Potentially poorly controlled	Creation of specific pandemic plans and emergency management protocol.	Moderate improvement	Adequately controlled	EH&S
4	Laboratory safety	ISEM Policy; safety programs; BSAS funding; Safety Program Guidelines for Principal Investigator; hazardous waste management programs	Potentially over-controlled	Move BSAS funds to other priorities	Moderate decrease	Adequately controlled	EH&S
5	Facilities and grounds safety	Building Maintenance Services; Grounds and Landscape Service, focused on operations.	Poorly controlled	Increase BSAS funding	Moderate improvement	Potentially poorly controlled	PPCS
6	Conflicts of interest in financial transactions and agreements	Annual Conflict of Interest Reporting Systemwide by Designated Officials; Business Contract Policies; Conflict of Interest Coordinators; Whistle Blower system; Administrative Responsibilities Handbook (Principles of Conflict of Interest)	Potentially over-controlled	Continue current efforts with current controls.	No Change	Potentially over-controlled	Administration
7	Budget impairment	General ad-hoc interaction with Legislature and Governor.	Poorly controlled	External financing program; Budget Officers; UC President working with Governor and Legislature	Significant improvement	Potentially poorly controlled	Senior leadership

Enterprise Risk Management – Tools

Questions to Board is interested in:

1. Is there an ERM process?
2. Who is leading that process?
3. Is it a board agenda item, how often, how much time?
4. Is there a common risk language that fosters communication?
5. Is there a process for assessing, prioritizing and risks?
6. Is there a gap analysis of the current and desired risk management capabilities, and what vision along with goals and objectives?
7. Is there a structured process to update the risk profile, appetite, and tolerances as new changes enter the environment?
8. How effective are those changes communicated to internal and external stakeholders?

Enterprise Risk Management – Tools

Specific questions:

1. Has an ERM glossary been created?
2. Have employee orientations related to risk management been done?
3. Is monitoring assigned to specific individuals who also communicate the results of the monitoring activity to appropriate levels in the organization?
4. Have formal communication mechanisms, such as a central web site or newsletter, been established? Is communication occurring on a regular basis?
5. Have management discussions occurred, with decisions made about how much risk the organization is willing to accept in key areas?
6. Has systematic documentation of risks and controls occurred in all functional areas of the organization?
7. Has the risk analysis resulted in the identification of the organization’s top risks?
8. Have alternative risk management strategies been identified for all of the identified the top risk areas? Do strategies respond to changing social, environmental, and legislative conditions?
9. Do strategies respond to changing social, environmental, and legislative conditions?
10. Have any risk-management-related or other internal control measures/activities been identified for elimination?
11. Have benefits of assuming additional risk been identified?
12. Have competitive needs or reputation been discussed at a strategic level?

Enterprise Risk Management – Additional resources

- IIA position paper: The role of internal auditing in enterprise-wide risk management
- Deloitte whitepaper: Enterprise Risk Management, A ‘risk-intelligent’ approach
- A Risk Practitioners Guide to ISO 31000: 2018
- University of Wisconsin System: Enterprise Risk Management Handbook

Summary

Enterprise Risk Management is an integral part of governance.

The board is ultimately responsible for risk management but has delegated to management the role of establishing and operating the Enterprise Risk Management program.

Internal audit's key role is to provide assurance to management and the board. It may provide consulting services but should apply safeguards.

Any internal auditor who cannot demonstrate the appropriate skills and knowledge should not undertake work in the area of risk management.

Conclusion

Contact Information:

Gregory Kigen

Day time phone: 940-369-7560

Principal Auditor, UNT System

Email: Gregory.Kigen@untsystem.edu