## MODULE E: OUTLINE

# Driving Enterprise Risk Management (ERM)

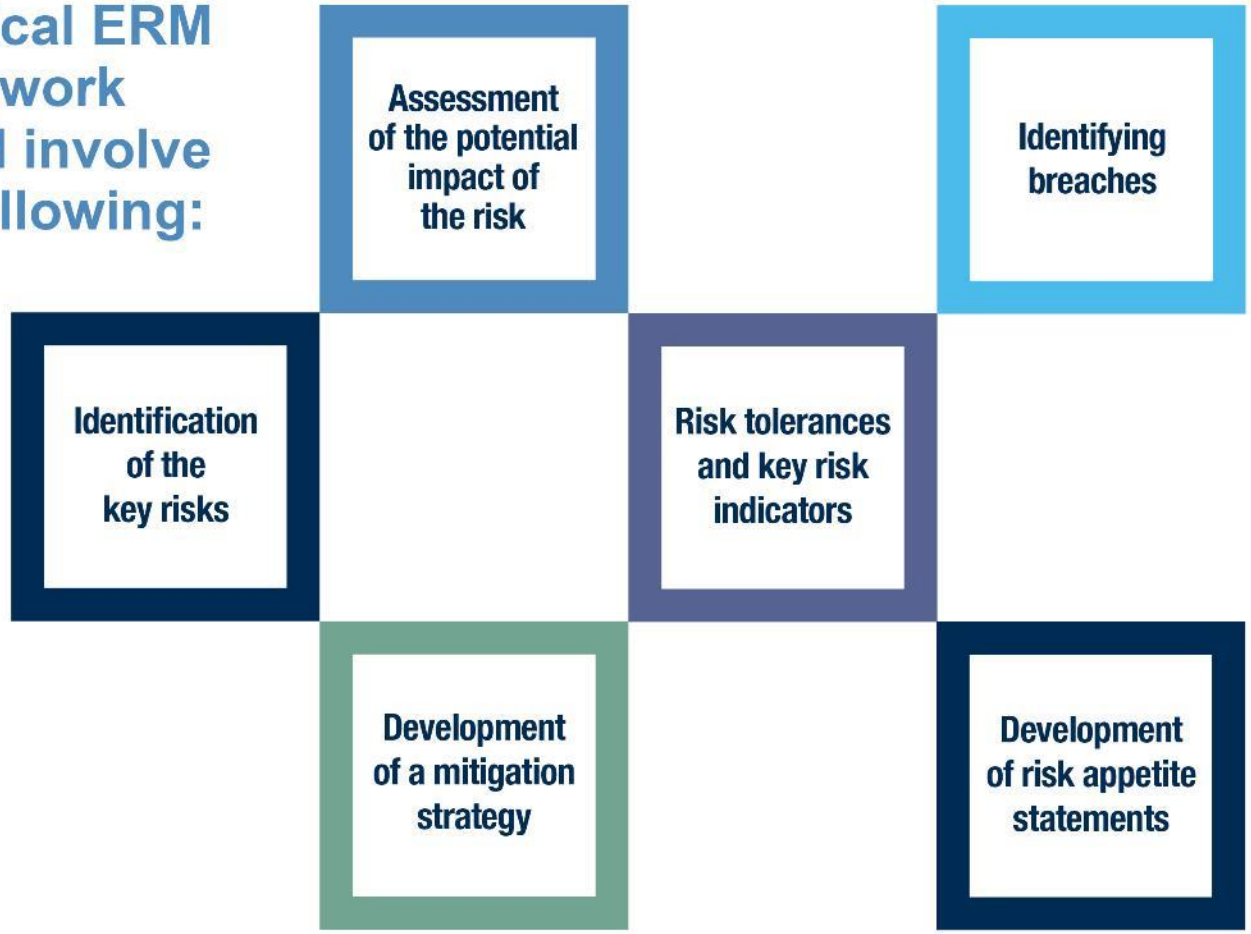
1. Implementing an ERM framework
2. The Board's responsibility for ERM
3. The Audit Committee's role in ERM
4. Dealing with cyber security

## 1 IMPLEMENTING AN ERM FRAMEWORK

- Every organization should have a set of beliefs and attitudes on risk
- Management must determine the organization's capacity, tolerance and appetite for risk to be approved by the Board
- Risk awareness should be built throughout all levels of the organization – tone at the top is critical
- Risk management should be linked to company strategy and form part of the strategic planning process
- Internal Audit will typically help build the ERM framework and report on assurance over the effectiveness and efficiency of controls, risk mitigation strategies and any risk tolerance breaches

# 1 IMPLEMENTING AN ERM FRAMEWORK

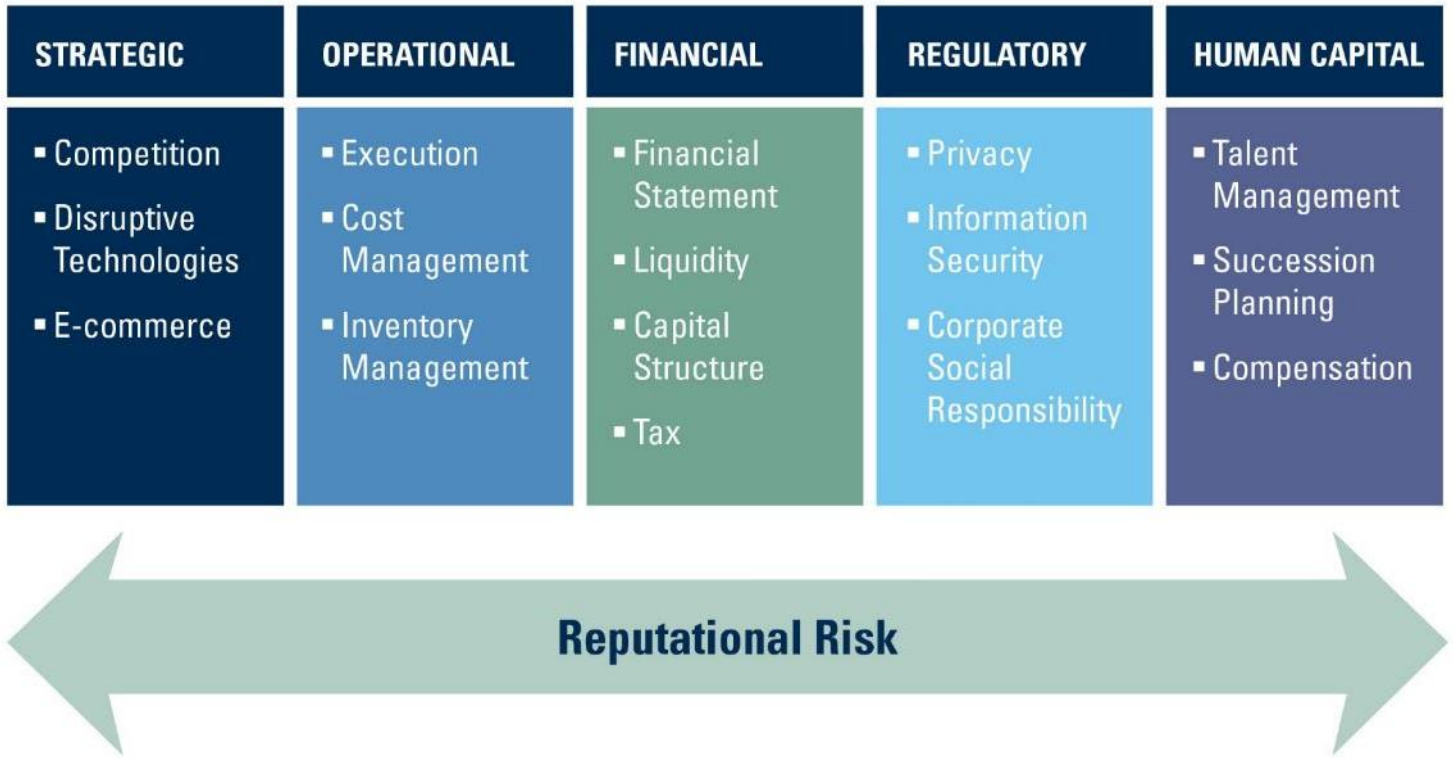
## A typical ERM framework would involve the following:



## 1 IMPLEMENTING AN ERM FRAMEWORK

# Identification of Key Risks

- Risks are typically broken down into the following 4 or 5 categories:



## 1 IMPLEMENTING AN ERM FRAMEWORK

### Risk Tolerances

- Sets the boundaries for risk taking at a granular level by risk
- Usually measured in the form of limits or thresholds
- Assists with day-to-day decision making and drives action by management and the Board
- The amount of risk an organization is willing to tolerate should be derived from the risk appetite statements

## 1 IMPLEMENTING AN ERM FRAMEWORK

### Key Risk Indicators

- A measure to indicate the potential state or trend of a risk
- Have a predictive value and can be an early warning signal
- LRIs may be leading, current or lagging measures

## 1 IMPLEMENTING AN ERM FRAMEWORK

### Risk Appetite Statements

- Risk appetite statements reflect the nature and amount of risk that an organization is willing to take
- They guide strategy setting and supports performance management
- A qualitative risk appetite statement is usually prepared for each risk category
- Risk appetite statements should be prepared by management based on their overall risk philosophy and capacity for managing risk
- In developing the risk appetite statements they should consider indicators such as the potential financial impact or impact on the organization’s ability to execute against its strategic plan

## 2 THE BOARD'S RESPONSIBILITY FOR ERM

- The Board is responsible for providing oversight of management's identification, assessment and mitigation of risk
- Making sure the company is identifying emerging risks and managing its risk profile are important parts of a Board's oversight duties
- The Board's role is to ensure that there is the proper balance of risk and reward by management
- Oversight of the ERM program usually takes place on a quarterly basis through reports to the Board or Audit Committee

## 3 THE AUDIT COMMITTEE'S ROLE IN ERM

- While the overall responsibility for risk oversight rests with the Board, the monitoring function or coordination of the process typically is passed to a single committee
- In many large or public companies, it is the Audit Committee that takes on this responsibility
- Where oversight is passed to the Audit Committee, its responsibility must be clearly set out in its mandate
- The Audit Committee must ensure that sufficient time is set aside to carry out its responsibilities

## 3 THE AUDIT COMMITTEE'S ROLE IN ERM

**Audit Committee members will want to:**

- Understand how the ERM process works and how management identifies, assesses and mitigates the identified risk
- Understand the top risks and ensure that they are communicated to the entire Board and allocated appropriately to committees
- Understand internal audit's role in risk management and the extent to which its audit plan covers the key risks
- Ensure that the risk register is not static as some risks will be added and others dropped as the strategy changes and the business plan is executed

# 3 THE AUDIT COMMITTEE'S ROLE IN ERM

## An Example of Risk Allocation

### BOARD OF DIRECTORS

- Health care reform
- Process and efficiency
- Competition
- Digital retail execution
- Disruptive technologies
- Customer insights and analytics
- Connected healthcare network
- Labor management
- Economic and trade
- Strategy development and execution

### AUDIT COMMITTEE

- Data management
- Associate and franchisee relationship management
- Inventory and shrink management
- Vendor management
- Business continuity
- Liquidity, capital availability and allocation
- Impairment of goodwill and long-lived assets
- Credit risk

### RISK AND COMPLIANCE COMMITTEE

- Information security
- Information systems and major implementations
- Distribution and supply chain
- Privacy
- Food safety
- Drug manufacturing, dispensing and patient services safety
- Regulatory
- Competition law
- Environmental protection
- Climate change
- Workplace health & safety
- Product and services safety – GM, apparel, health & beauty
- Social reform
- Trademark & control brand protection

### GOVERNANCE COMMITTEE

- Organizational change capacity and capability
- Colleague attraction, management, and succession planning
- Culture transformation
- Ethical business conduct

**2019 RESIDUAL RISK LEVEL**

High
Moderate
Low

# 3 THE AUDIT COMMITTEE'S ROLE IN ERM

## An Example of Monitoring Risks

| | | | | | Q1 2017 | |
|---|---|---|---|---|---|---|
| Rank | ERM Risk | Risk Owner | Short Term Outlook | Long Term Outlook | Key Updates & KRI Breaches | Other Updates |
| 1 | Healthcare Reform | | | | | Yes – Pg. 11 |
| 2 | New Loyalty Program | | | | | Yes – Pg. 12 |
| 3 | Information Security | | | | | Yes – Pg. 12 |
| 4 | Information Technology Infrastructure and Operations | | | | 2 Breaches | Yes – Pg. 12 |
| 5 | Major System Implementations & Adoption | | | | Key Update; 1 Breach | Yes – Pg. 13 |
| 6 | Competition | | | | | Yes – Pg. 13 |
| 7 | Food Safety & Public Health | | | | | Yes – Pg. 14 |
| 8 | Data Management | | | | | Yes – Pg. 14 |
| 9 | Regulatory | | | | | |
| 10 | Dispensing and Patient Services Error | | | | | Yes – Pg. 14 |
| 11 | Privacy | | | | Key Update | |
| 12 | eCommerce | | | | | Yes – Pg. 15 |
| 13 | Social Media | | | | 1 Breach | Yes – Pg. 15 |
| 14 | Organizational Change Management | | | | | |
| 15 | Retail Shift from Brick & Mortar to Digital | | | | | |
| 16 | Competition Law Compliance | | | | | |
| 17 | Economic | | | | | |

- High Risk
- Moderate Risk
- Low Risk

# 3 THE AUDIT COMMITTEE'S ROLE IN ERM

## What does good ERM look like?

- A culture of risk management exists in the organization
- There is a shared understanding of how much risk the company wishes to take
- A common risk language so that everyone understands what different types of risk mean
- ERM is connected to strategy development
- Business unit leaders are accountable for managing their own risks
- Risk management practices are baked into how the company does business
- Emerging risks are continually highlighted and discussed
- Key risk indicators are developed and breaches of action plans reported on quarterly
- There is an executive level officer who is responsible for the ERM process