# NAVIGATING RISKS, SEIZE OPPORTUNITIES

## IDENTIFY, IMPROVE, INFLUENCE

SWAKSHAR BASU B.Com (Hons),
M.Com, FCPA, RIMS-CRMP

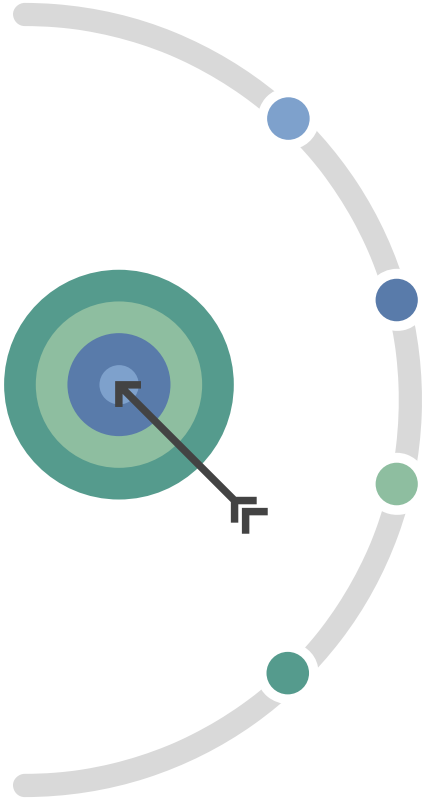
# Table of Content

# Learning Objectives

Learn and understand the fundamental concepts

- ❑ Design implementation plan
- ❑ Risk management process
- ❑ Develop risk competency
- ❑ Influencing decision-making

# Recap



01

## Align organisational model

Understand business model, Internal and External Analysis, Organisational Culture, Behavioural Bias

02

## Why ERM

Inter-connected vs silo, Global risks ranked by severity, Proactive, Prevents regulatory breach, Agility

03

## Risk Strategy

Establishing a Risk Strategy approach, Risk appetite, tolerance, Leadership Support and Risk Response

04

## Risk Culture and Governance

Culture of awareness, risk training, Incident management, 3 Lines, Core Components, Governance Structure (Top Down/ Bottom Up)

# Section Header

1

# Implementation Plan


## Define

Scope of risk management and set priorities for implementation (critical process or enterprise-wide)

## Methodology

Data Collection and information gathering, engage key stakeholders, familiarisation

## Information

Organise, prioritise and analyse data collected

## Timelines

Key Milestones, budgets, deliverables, tools, communicate and implementation

## Skill

Risk trainings to build risk competencies, resources required

# Implementation Roadmap

Timeline

04/ 2025

Phase 1: Foundation

Establish risk policy and framework, roles and responsibilities

06/2025

Phase 2: Context

Risk categories, risk appetite, risk committee members, reporting structure

08/2025

Phase 3: Setting the scope

Establish risk culture and awareness, deliver risk trainings

10/2025

Phase 4: Implementation

Identify risks, launch ERM and risk register

12/2025

Phase 5: Risk Reporting

Assessment and reporting, risk response

2026

Phase 6: Monitor

Risk Update, Review, reassess and continuous monitoring

# Risk Management Process

The process has been modelled using ISO 31000 to outline the stages of risk management

## Risk Reporting

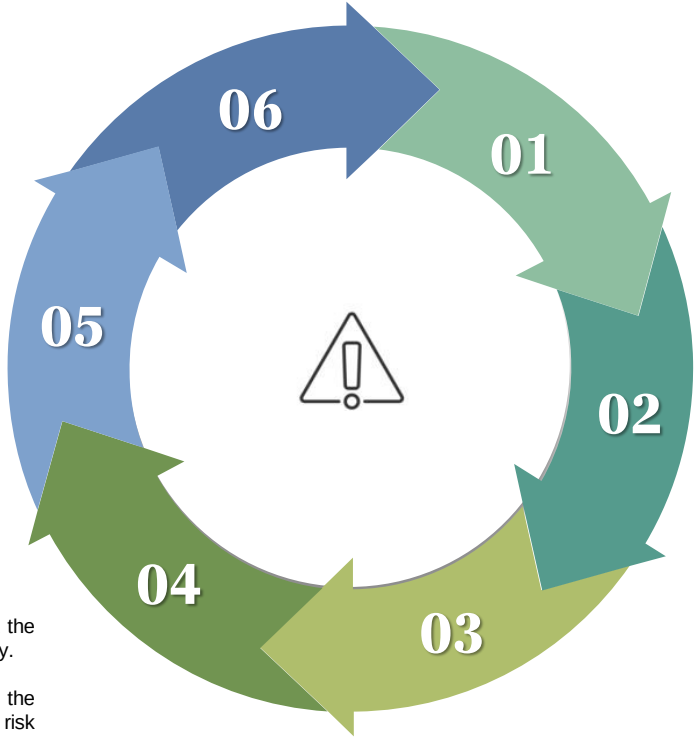
- Risk report presented to the Risk Committee, highlighting material risks and mitigation progress.
- Risk prioritization and reporting at aggregate level.
- Implement risk dashboards tracking risk status, mitigation progress and emerging risks/ trends.

## Risk Monitoring

- Monitor material risk exposures and track progress of mitigations.
- Risks rated moderate or above must be reviewed at least quarterly to assess the progress of treatment actions and changes in business environment.
- Risks rated as Low and Very Low should be reviewed at least once every six months.
- Key risk indicators reporting.

## Risk Treatment

- Select appropriate risk response and review against the risk appetite for the category of risk and per risk policy.
- Risk treatment - Avoid, Reduce, Transfer, or Accept.
- Mitigation action plan must be clearly documented in the risk register. Examples include avoid concentration risk by opening new routes through strategic partnerships, reduce cyber threats by enhancing cyber resilience
- High rated risks without any risk mitigation must have a risk acceptance rationale documented and endorsed by the Risk Committee.




## Establish the Context

- Define context and align with the strategic objectives such as reorganization of the Group, strategic management of capital, long term growth prospects.

## Risk Identification

- Establish a robust risk identification process with all Business Unit Risk Owners with clear documentation of root cause and consequence.
- Identify methods- SWOT, Brainstorming sessions
- Use of risk assessment tools such as Risk registers, a central repository to log and track risks.
- Historical data- past incidents review and trends to identify recurring risks and vulnerabilities.

## Risk Analysis

- Consider effectiveness of current controls in place.
- Conduct analysis of residual risks against criteria to assess likelihood (Rare, Unlikely, Possible, Likely and Almost Certain) and impact (Insignificant- Severe)
- Risk rating using (e.g., 1-5 scale for likelihood and impact) to facilitate prioritization of risks.
- Analyse against risk thresholds or set tolerance limits.
- Root cause analysis- Ishikawa, Bow Tie Analysis, SWOT
- Scenario analysis or stress testing methods.

# Key Questions

## Risk Identification

- What events or occurences could threaten the outcomes?
- Can this reoccur? If so, what factors would cause the event to recur?
- What is the root cause of this risk?
- What is the impact of the risk to the business? Affects single or multiple BUs?

## Risk Analysis


- How is the risk assessed with the risk scales of impact and likelihood?
- What controls are currently in place? (*Assess risk vs existing controls*)
- What is our risk appetite? Are risks identified inter-linked to another?
- Assessment is subjective, however recent data, incidents, claims, internal/ external information can be used to support assessment.

## Risk Treatment

- Is the cause and effect of the risk clear?
- What risk response is chosen? (*If residual risk is not acceptable or tolerable, or exceeds risk appetite, then the risk should be treated*)
- Are risk owners aware on where the risk mitigations should be documented?

## Risk Monitoring

- How is risk monitoring performed? (*ERM to use risk register to monitor and establish an appropriate monitoring and reporting regime to track)*
- Is a risk owner identified? (*Risk owner is responsible to update risk treatment plan*)
- Is there an automatic way to track and monitor the risks?

## Risk Reporting

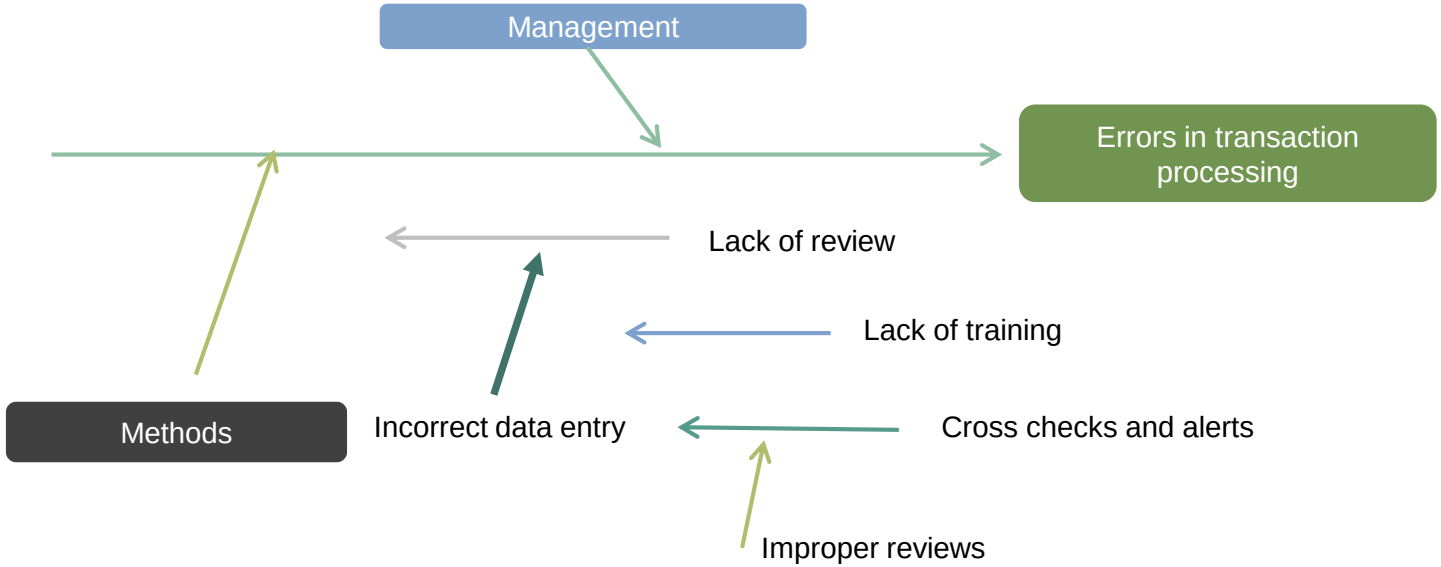
- Is risk reporting effective? Is risk information being regularly updated?
- Does the risk reporting help in decision-making and provide valuable insights?

# Ishikawa Analysis

## Root Cause Analysis Techniques

Ishikawa or ‘fishbone’ diagram uses the Ishikawa diagram along with techniques such as ‘5 whys’ to work out the root cause of risk events. The main categories on an Ishikawa diagram could include processes, people, management, money and environment. These form the bones (ribs) of the fish of which the first of the whys are asked

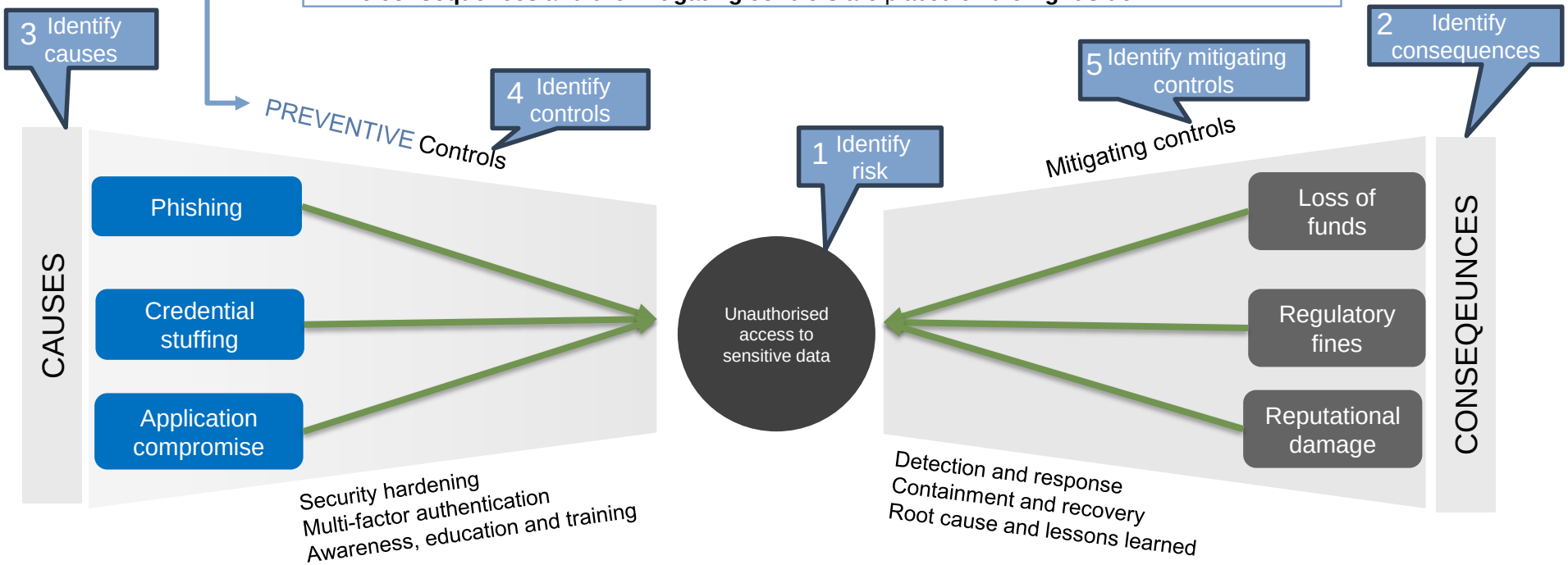
The analysis asks 5 whys about why errors occurred in transaction processing. Note that each successive ‘why’ is indicated in different colours.



# Bow Tie Analysis

***A risk bow tie diagram*** *is used to depict a RISK event that have multiple causes and consequences with varying complexities*

- The **EVENT** is placed in the **central knot**
- **Causes and controls** used to prevent the event are placed on the **left side** of the bow
- The **consequences and the mitigating controls** are placed on the **right side**.



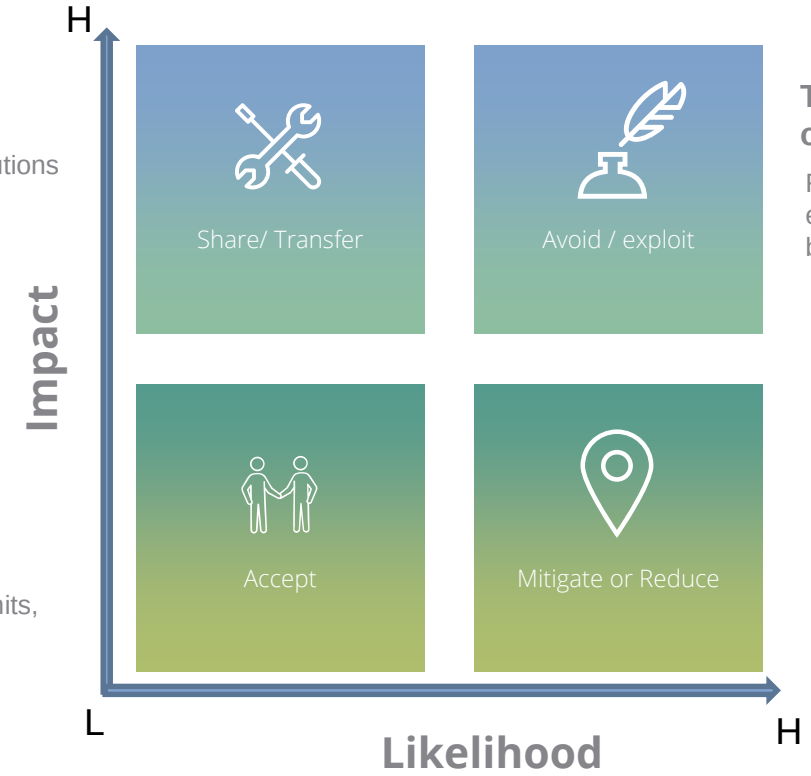
# Poll Question:

What methods and techniques do you use to identify risks:

- ❑ Brainstorming
- ❑ Checklists
- ❑ Facilitated workshops
- ❑ Risk questionnaires
- ❑ Focus groups

# Risk response

**Risk transfer**
Insurable risks and solutions




**Terminate / exploit opportunity**
Risk reward analysis, avoid risk if exceeds risk appetite, exploit if benefits outweigh risks

**Tolerate the risk**
Risk is within tolerance limits, impact is low

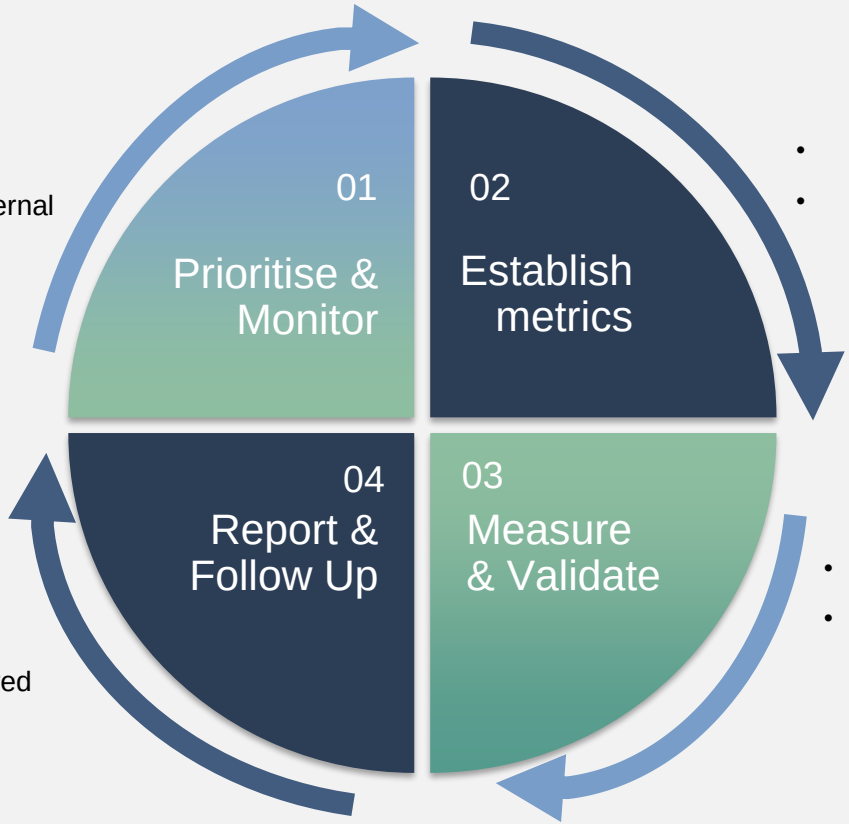
**Mitigating controls**
Reduce risk impact to acceptable level, implement risk controls

For any risk exposure that is deemed to be not acceptable, risk response should be defined. Risk response should be adapted to the context and tailored to either reduce (or remove) the likelihood of occurrence, velocity, and/of the magnitude of the impact.

ERM processes used for assessment purposes are **Risk and control self assessment** and **Event data collection**

# Monitoring risks

- Identify priorities for risk monitoring
- Monitor changes in internal and external

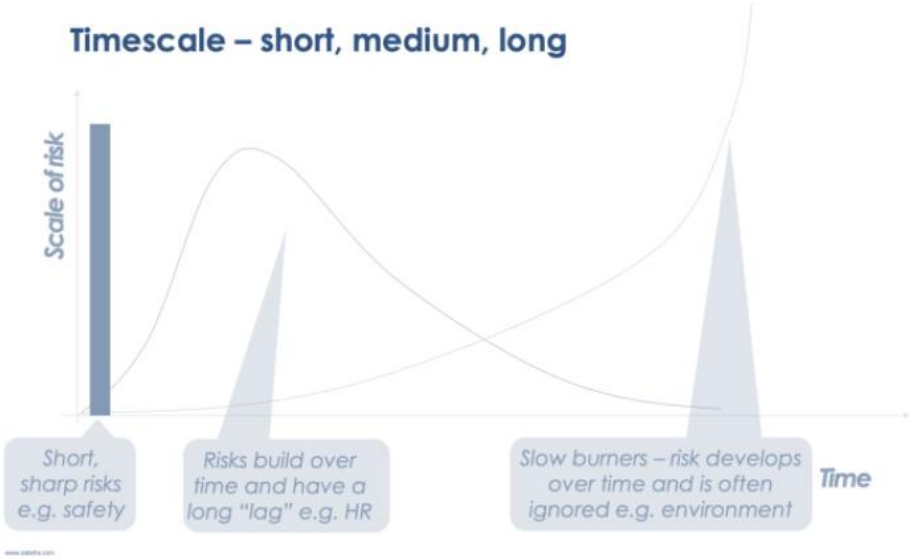



- Develop Key Risk Indicators
- Establishing monitoring schedule

- Develop risk reporting
- Communicate actionable information
- Conduct follow-up activities as required

- Measure against risk limits
- Validate performance

# Managing risks




Proactive risk management involves anticipating the velocity of risk and impact to business. Good internal controls help to reduce the evolving risks when it is least expected.

# Risk Taxonomy Categories

Risk category- Level 1

Risk factors- Level 2

| STRATEGIC | FINANCIAL | OPERATIONAL | COMPLIANCE | TECHNOLOGY |
|---|---|---|---|---|
| Market expansion | Liquidity | Labour shortages | Regulatory risk (MAS, IMDA, ACRA, US SEC) | IT Security & Cyber |
| Supply Chain disruption | Interest rate | Transportation delays | Vendor onboarding (Due diligence) | IT Governance |
| Changes in customer demand/ behaviour | FX risk | Delivery errors | Data breach (PDPA) | IT System failures |
| Geopolitical (tariffs, political uncertainty, intrastate violence ) | Credit risk | Business Continuity | ESG violations | |
| | Capital Management | Health and Safety | | |
| | Debt | | | |

- Risk can "**fall between the silos**" that none of the silo leaders can see. As a result, a **<u>significant risk that may be on the horizon can go unnoticed</u>**
  - Example: demographic shifts occurring in the marketplace whereby population shifts towards large urban areas are happening at a rapid pace than anticipated. This oversight can impact strategy of a retail organization that continues to look for real estate locations in outlying suburbs
- Individual functions may not understand how an individual response to a risk might trigger a significant risk in another part of the business
  - Example: Due to growing concerns about cyber risks, IT function may tighten security protocols but in doing so, employees find the new protocols confusing and frustrating, which lead to costly "work arounds"

Risks can arise in any part of the business, affecting either one or multiple functions. It is important to have the strategic lens when evaluating risks.

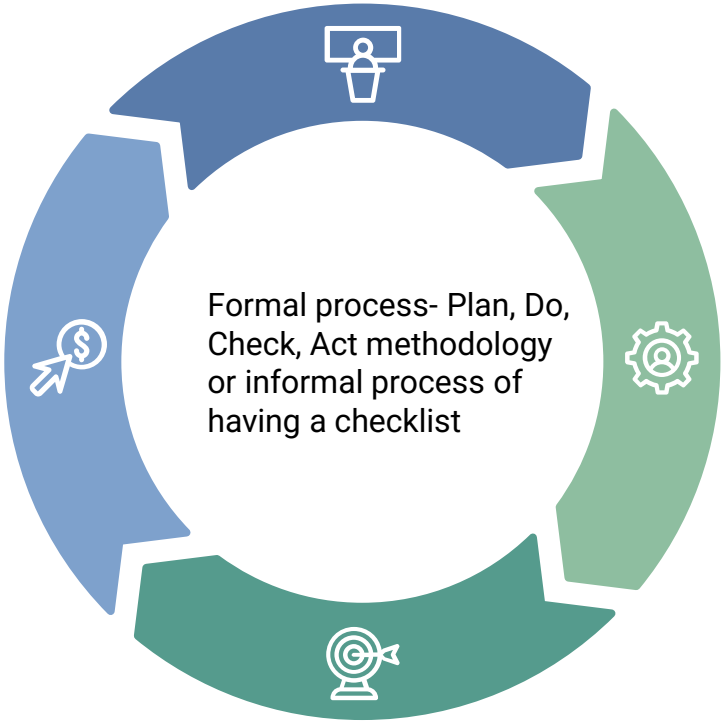
# Section Header

2

# Improve risk management process

## Continuous improvement

Formal review of Strategy, Culture, Capabilities and identify aspects of risk process that needs improvement




## Validate

Validation of continuous improvement options with stakeholders

## Operations

Monitor results and reassess as necessary

## Implementation

Implement options

# Risk trainings

## Strategy

Must align with specific business goals
Gap assessment and future roadmap

## Gap Analysis

Conduct gap assessment and upskilling needs

## Training

Develop appropriate training schedules and curriculum development to address gaps

## People

Evaluate effectiveness and build risk competencies for Senior Leaders, Risk Champions and Front Office managers

# Poll Question:

What can a risk management professional recommend to protect an organization's critical infrastructure from a cyber attack:

- ❑ Implement password
- ❑ Buy a cyber liability insurance
- ❑ Ensure employees do not post on social media
- ❑ Monitor internet usage

# Section Header

3

# Influence Risk-based Decisions

Facilitate risk dialogue and discussons

Integrate risk management into day to day business

Evaluate which decisions have the biggest impact

Understand risk attitudes of key decision maker and influencers

Identify stakeholders at each stage of decision making