Enterprise Risk Management

CA. Abhiram Budhkar

October 2013

J B Nagar CPE Study Circle

What is Risk?

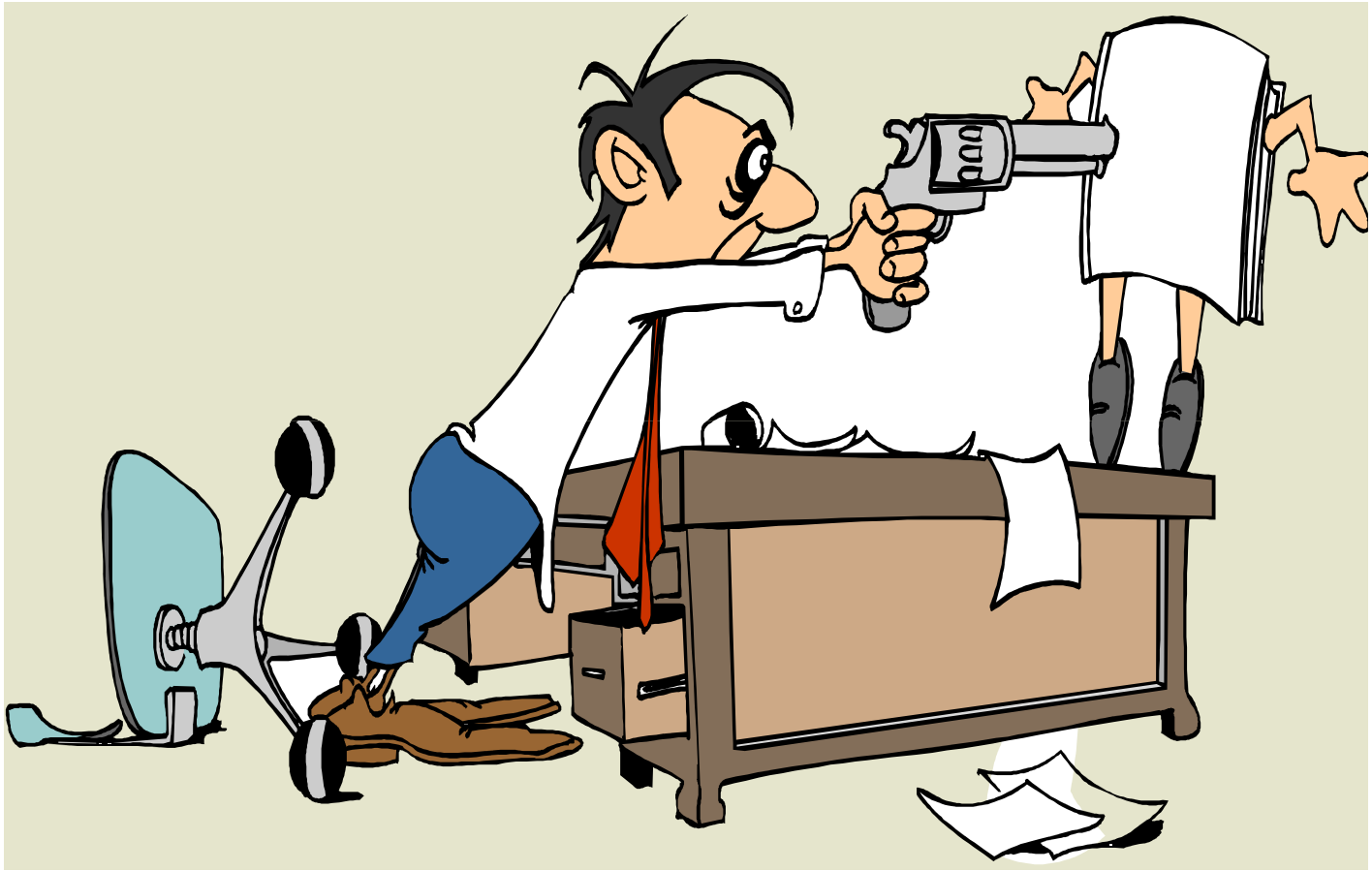
"The potential for loss or sub-optimization of gain caused by an event (or series of events) that can adversely affect the achievement of a company's objectives"

Risk Response – Taking no risks at all

“A ship in harbor is completely safe…….

But that is not what ships are for.”

Risk Averse?

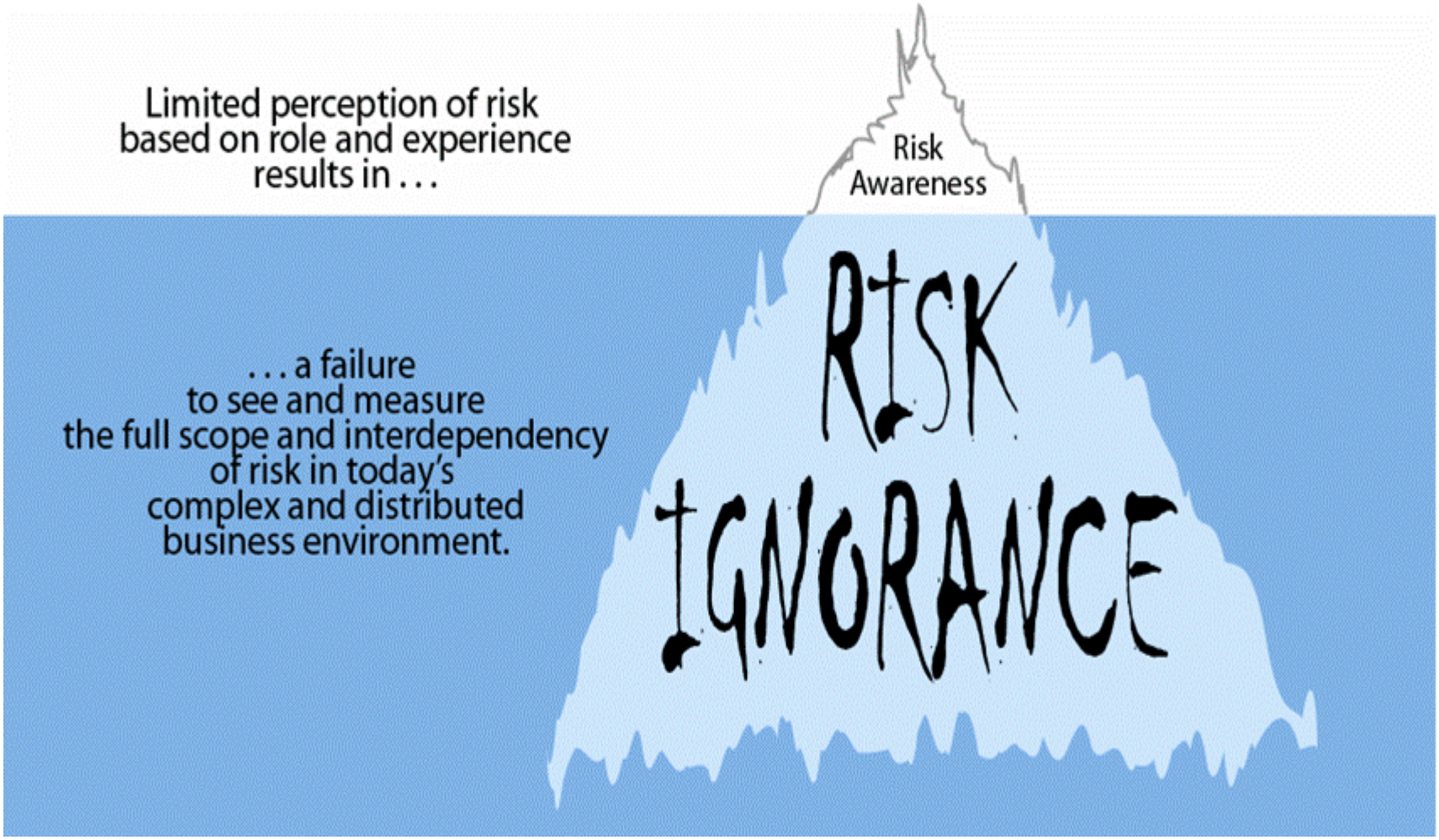


Risk Response – Taking extreme / uncontrolled risks

“You cant jump off the cliff and build your wings on the way down”

Risk Response - Taking calculated & controlled risks

The iceberg of risk



Companies Act 2013 – Risk Management Requirements

Clause 134 (n): A statement indicating development and implementation of a risk management policy for the company including identification therein of elements of risk, if any, which in the opinion of the Board may threaten the existence of the company, shall be prepared.

Clause 177 (4) (vii): Every Audit Committee shall act in accordance with the terms of reference specified in writing by the Board which shall inter alia and include evaluation of internal financial controls and risk management systems.

Schedule IV (II): The independent directors shall help in bringing an independent judgment to bear on the Board's deliberations especially on issues of risk management and satisfy themselves on the integrity of financial information and that financial controls and the systems of risk management are robust and defensible.

Clause 49 (IVC) – Requirements on Risk Management

"The company shall lay down procedures to inform Board members about the **risk assessment and minimization procedures**.

These procedures shall be periodically reviewed to ensure that executive management controls risk through means of a **properly defined framework**"

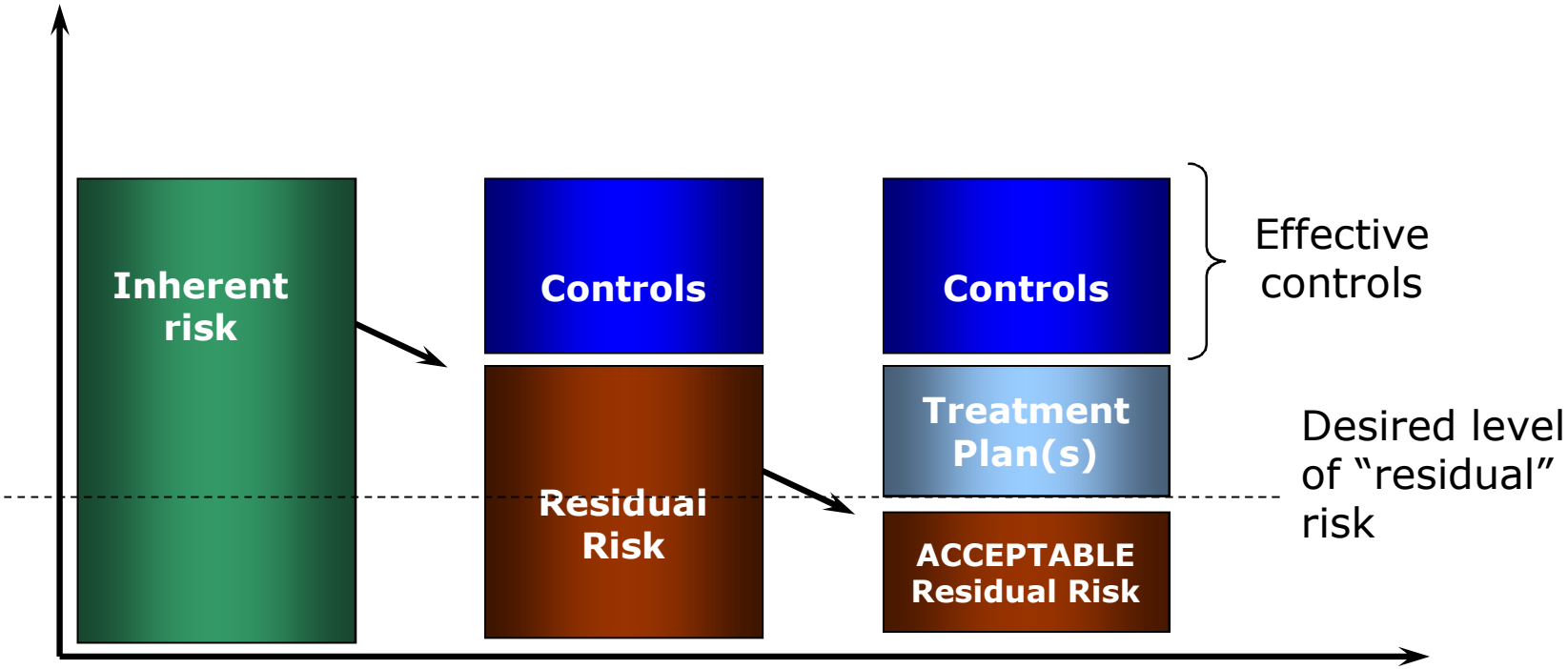
Enterprise Risk Management – is a process…

- Initiated by an entity's board of directors, reflecting "The Tone at the Top"
- Effected by management and other personnel
- Applied across the enterprise
- Designed to identify potential events, risk or opportunity, that may affect the achievement of entity's objective
- Developing response to the risk, "Within entity's risk appetite"
- Ensures timely information of the risk, monitoring of the mitigation process and appropriate escalation within the organization
- To provide reasonable assurance regarding the achievement of entity's objectives.

(Source: COSO Enterprise Risk Management Integrated Framework 2004, COSO)

Risk Management Objective

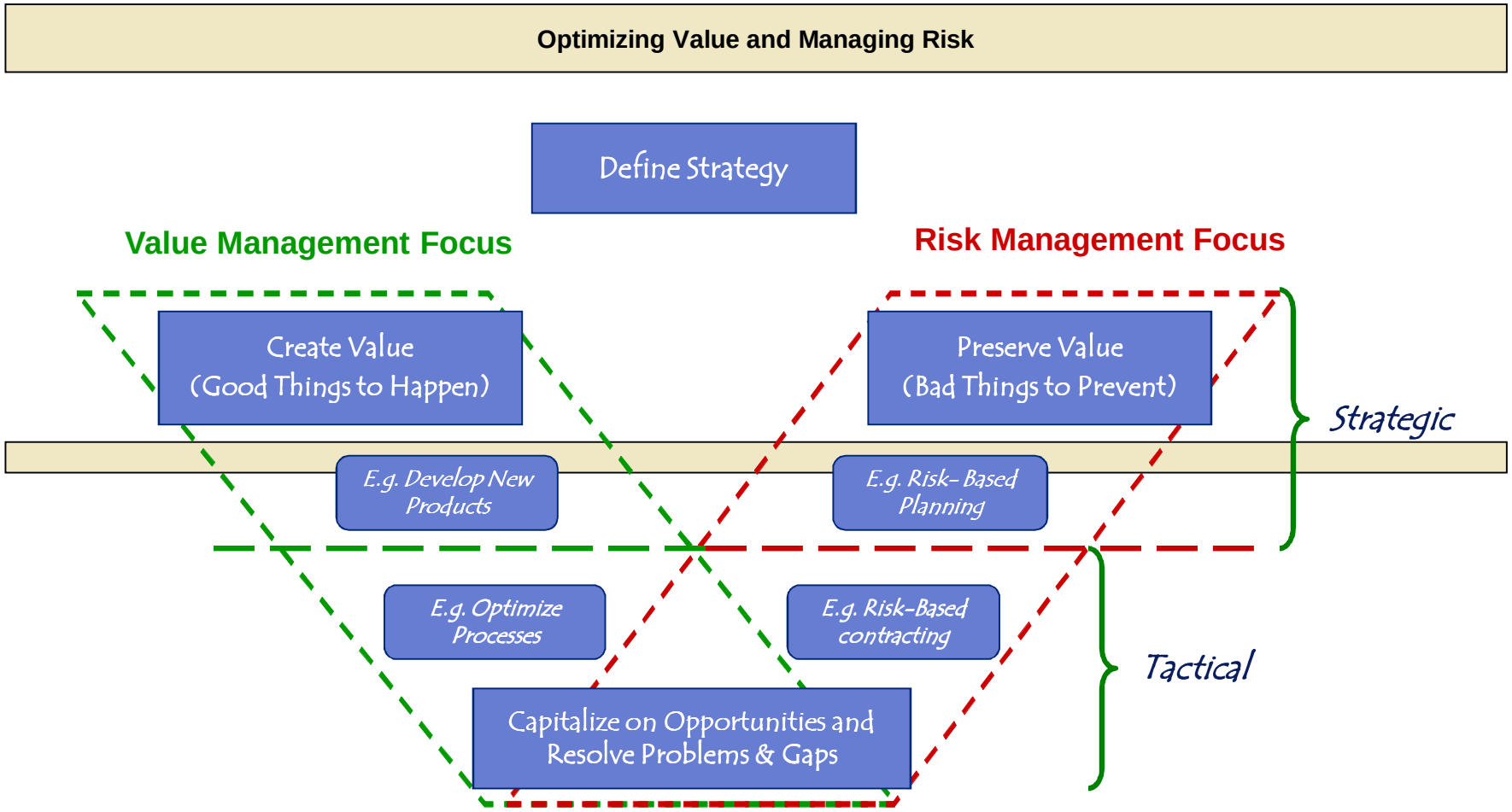
Objective of risk management process is to bring the inherent level of risks to a desired level of acceptable risks



Bridging the Gap…

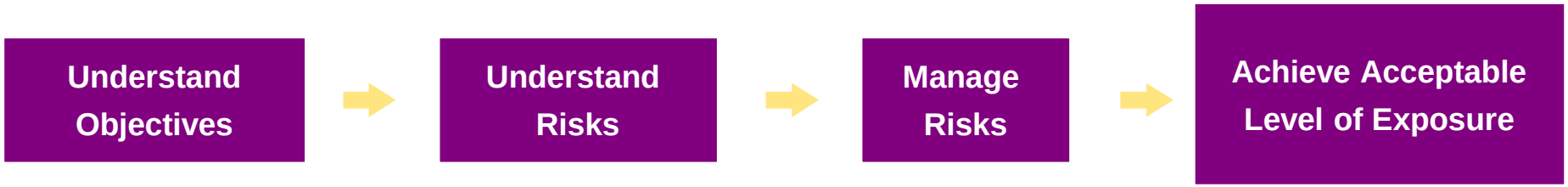
Traditional Risk Management Practices	How ERM can help in adding Value to an Organization
Operating in Silos	Understanding the interaction of different risks and leveraging the expertise that resides within Silos
Speaking Different Languages	Actively manages communication between silos to ensure consistency of terminology, measurement, understanding and reporting of risks
Lacking Centralized Risk Information	Provides a Portfolio view of risks and Centralized Risk Information is contained in the form of a Risk Register
Assessing Risk to Preserve Value	Protect the value of its existing assets as well as create new or future value for all key stakeholders

What is Enterprise Risk Management (ERM)



Graph from Institute on IT Governance (ITGI)

Enterprise Risk Management Framework



What are you trying to accomplish?	**What gets in your way of achieving your objectives?**	**What are you doing to manage this?**	**What is your level of exposure?**
Things toward which efforts are directed	**Challenges or obstacles that could impact your objectives**	**Current control activities to manage risk**	**Finding the right balance of controls**

The COSO ERM Framework

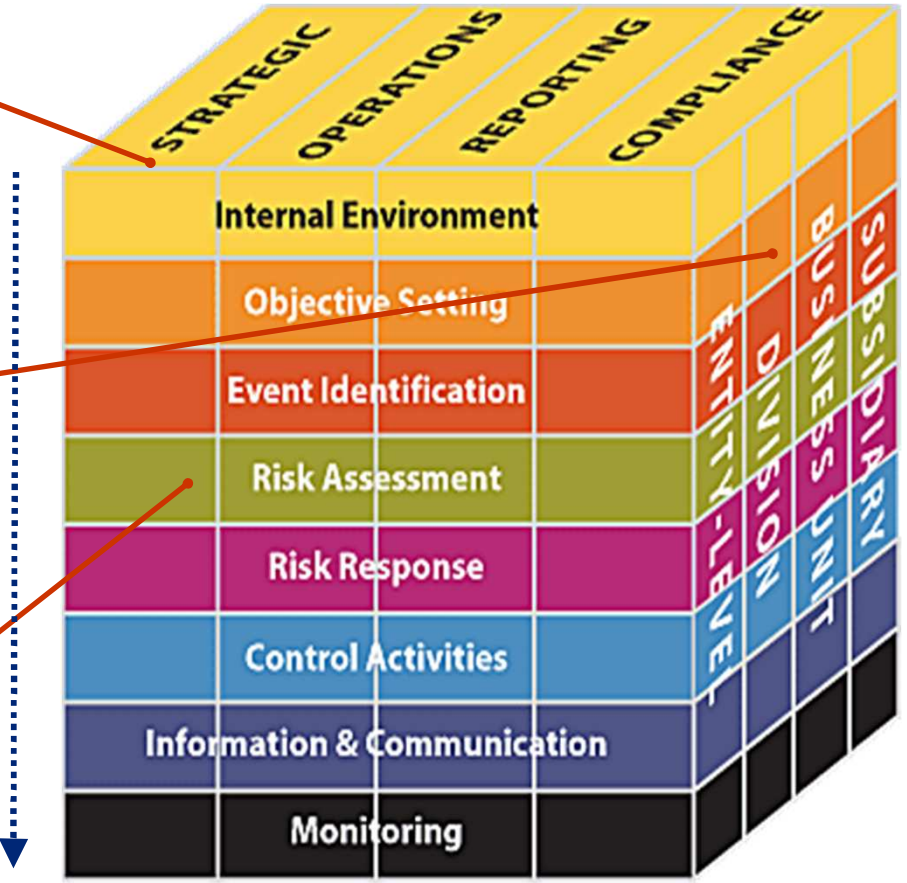
Entity risk can be viewed in the context of four categories:

- Strategic
- Operations
- Reporting
- Compliance

ERM considers activities at all levels of the organization:

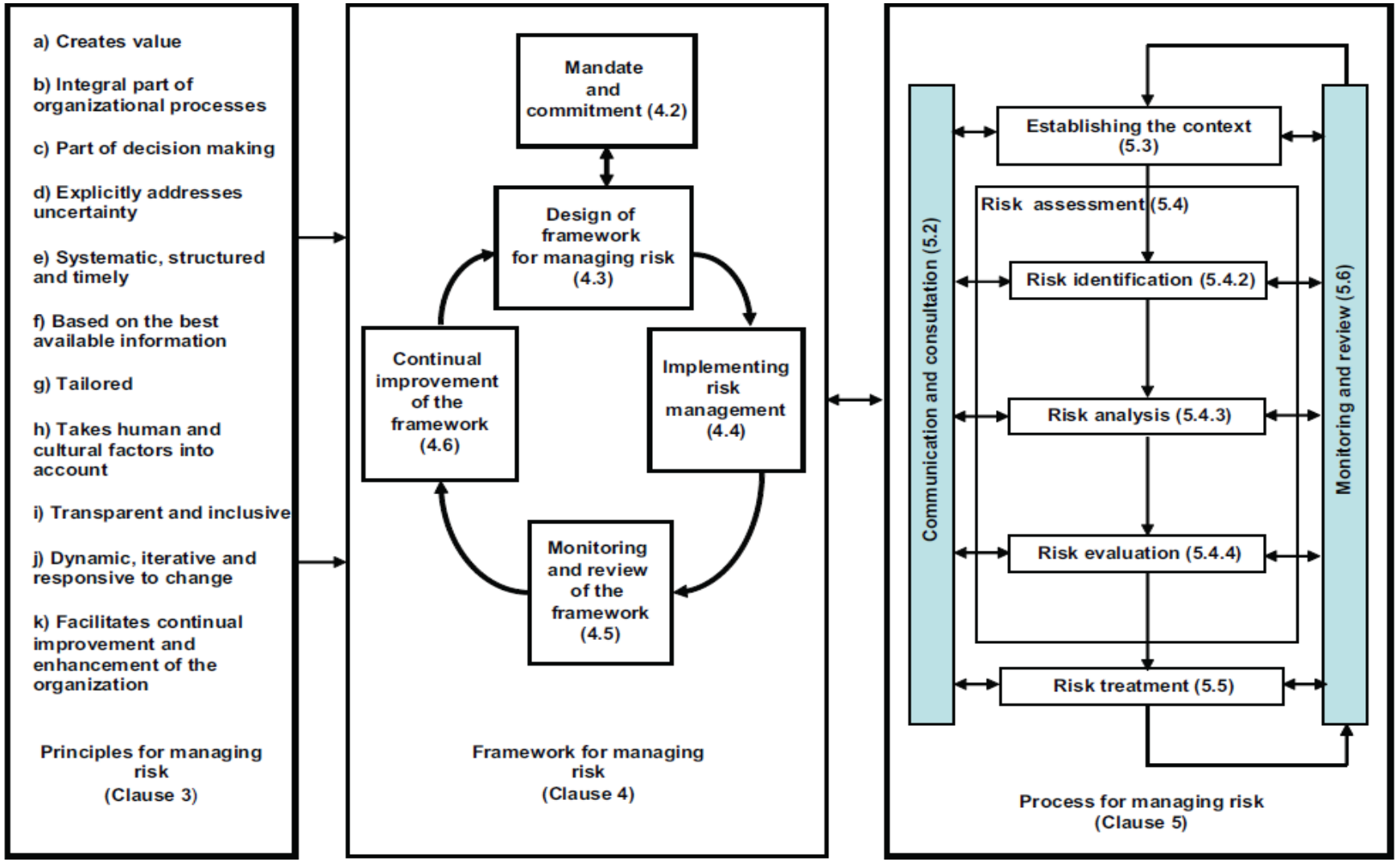
- Enterprise-level
- Division
- Business unit
- Subsidiary level

The eight components of the framework are interrelated

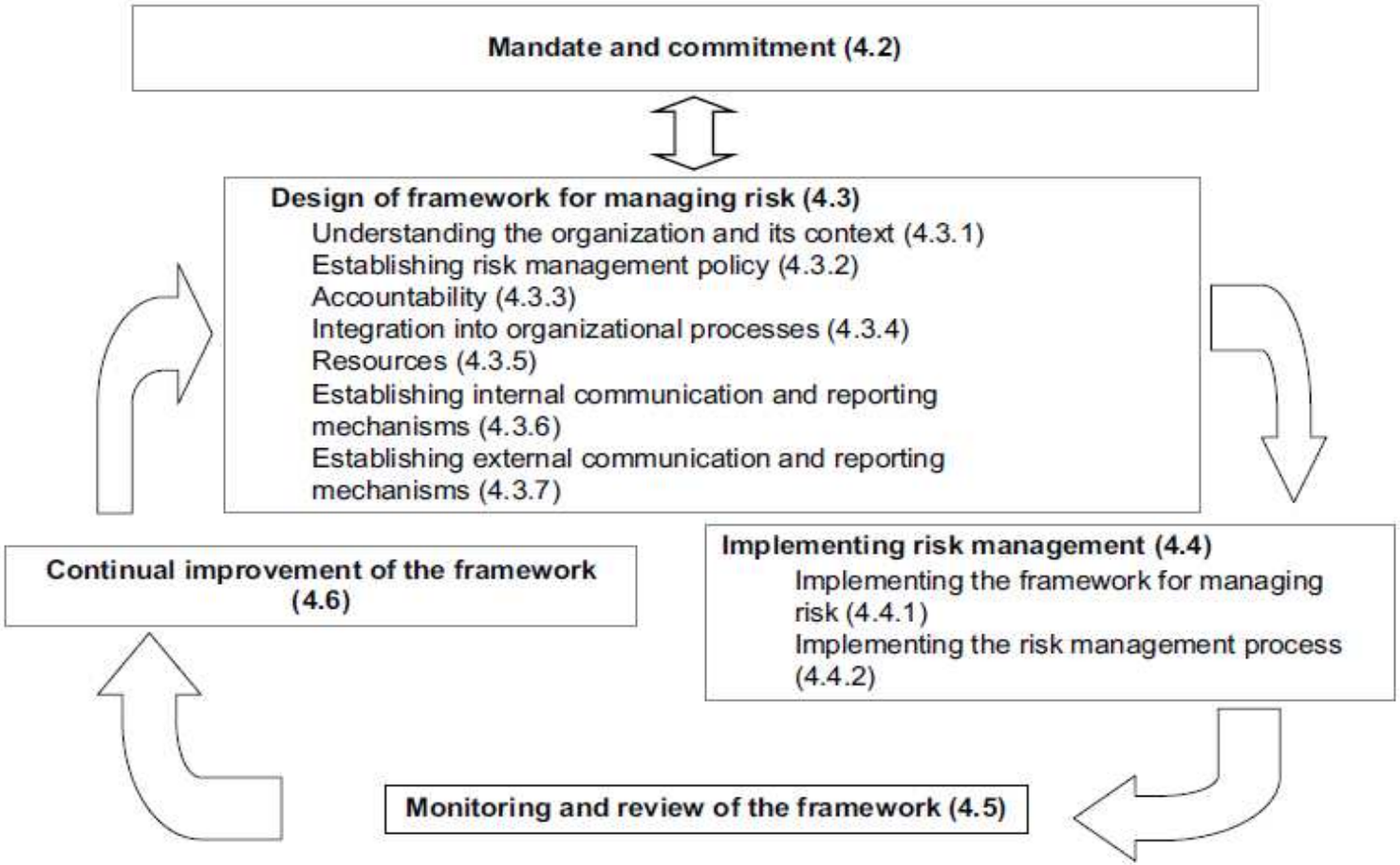


Implementation of ERM

ISO/FDIS 31000 – Relationship between risk management principles, framework and process



ISO/FDIS 31000 – Relationship between the components of the framework for managing risk



The framework suggested by ISO is not intended to prescribe a management system, but rather to assist the organization to integrate risk management into its overall management system. Therefore, organizations should adapt the components of the framework to their specific needs.

ERM in Summary

- A common approach to identifying, managing and communicating risk
- A process for aligning risks and objectives
- A process to provide accountability and transparency of risks at all levels of the organization
- A process for building risk management into an organization's culture and processes

ERM Process – Key Attributes

Risk Identification

- Consider the source of risk information [Survey, Interviews, Facilitated Discussion, Internal Reports, Secondary Research, Risk Database]
- Ensure representation from all key stakeholders

Risk Assessment

- Objective is to validate risks
- Have risk ranking criteria defined in advance
- Ensure involvement of key stakeholders
- Assign risk owner
- Document process and assumptions

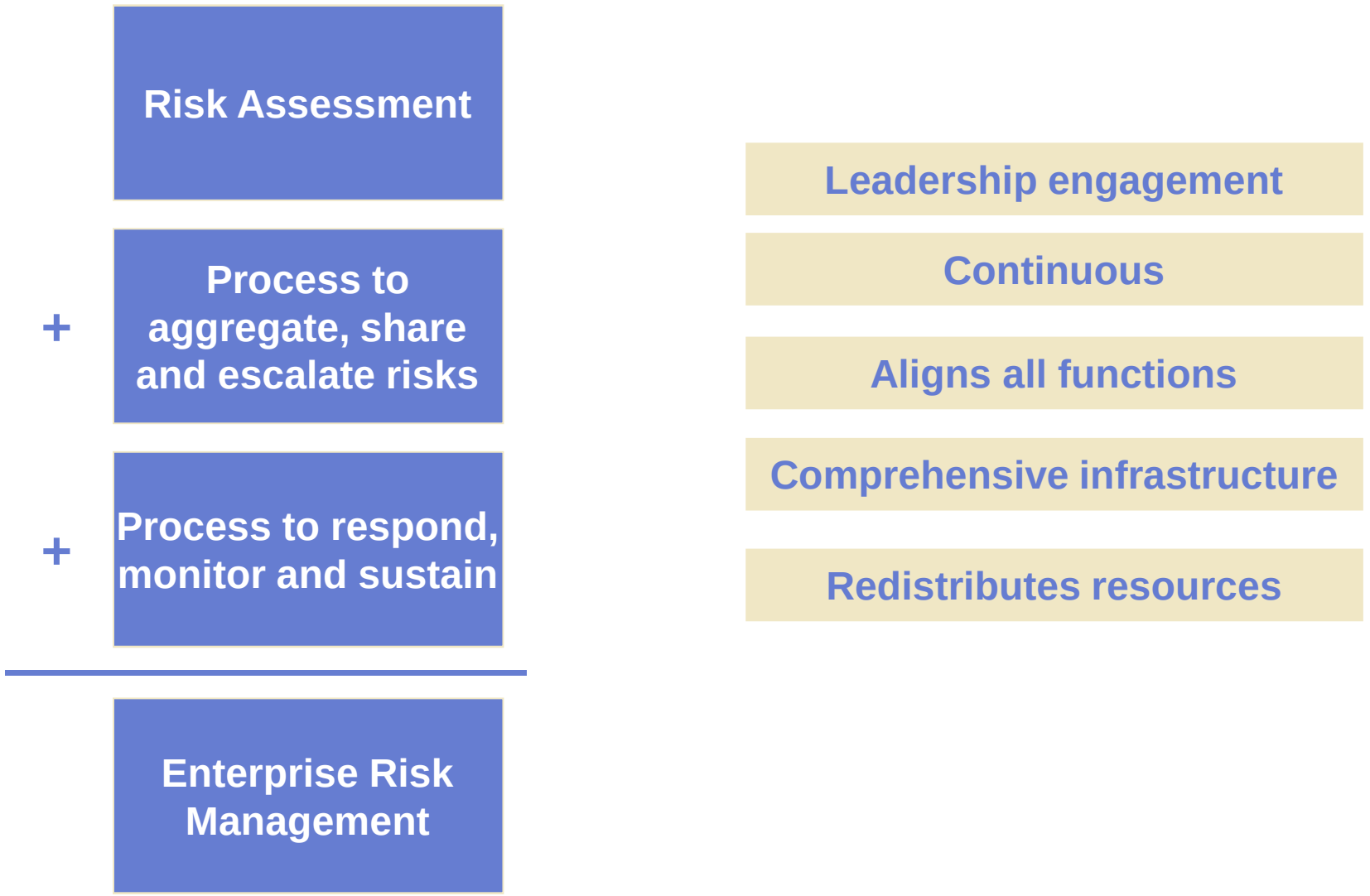
Risk Response

- Outline available risk response options
  - Accept, Reduce, Transfer, Avoid, Share
- Develop criteria to asses response options
  - Ease of implementation/Impact on objectives
- Consider stakeholders perspective of response selected
- Establish performance measures

Risk Monitoring

- Establish risk communication plan in advance
  - Timeliness of updates
  - Format of communication
- Form clear line of accountability
- Have consequences in place for non-performance

ERM is More Than Just Risk Assessment…



Company's "risk culture" provides the foundation of its ERM program

Definitions of "risk culture"

- In a typical risk culture, people will do the right things when risk policies and controls are in place
- In a good risk culture, people will do the right things even when risk policies and controls are ***not*** in place
- In a bad risk culture, people will not do the right things regardless of risk policies and controls

Balancing the hard and soft side of risk management

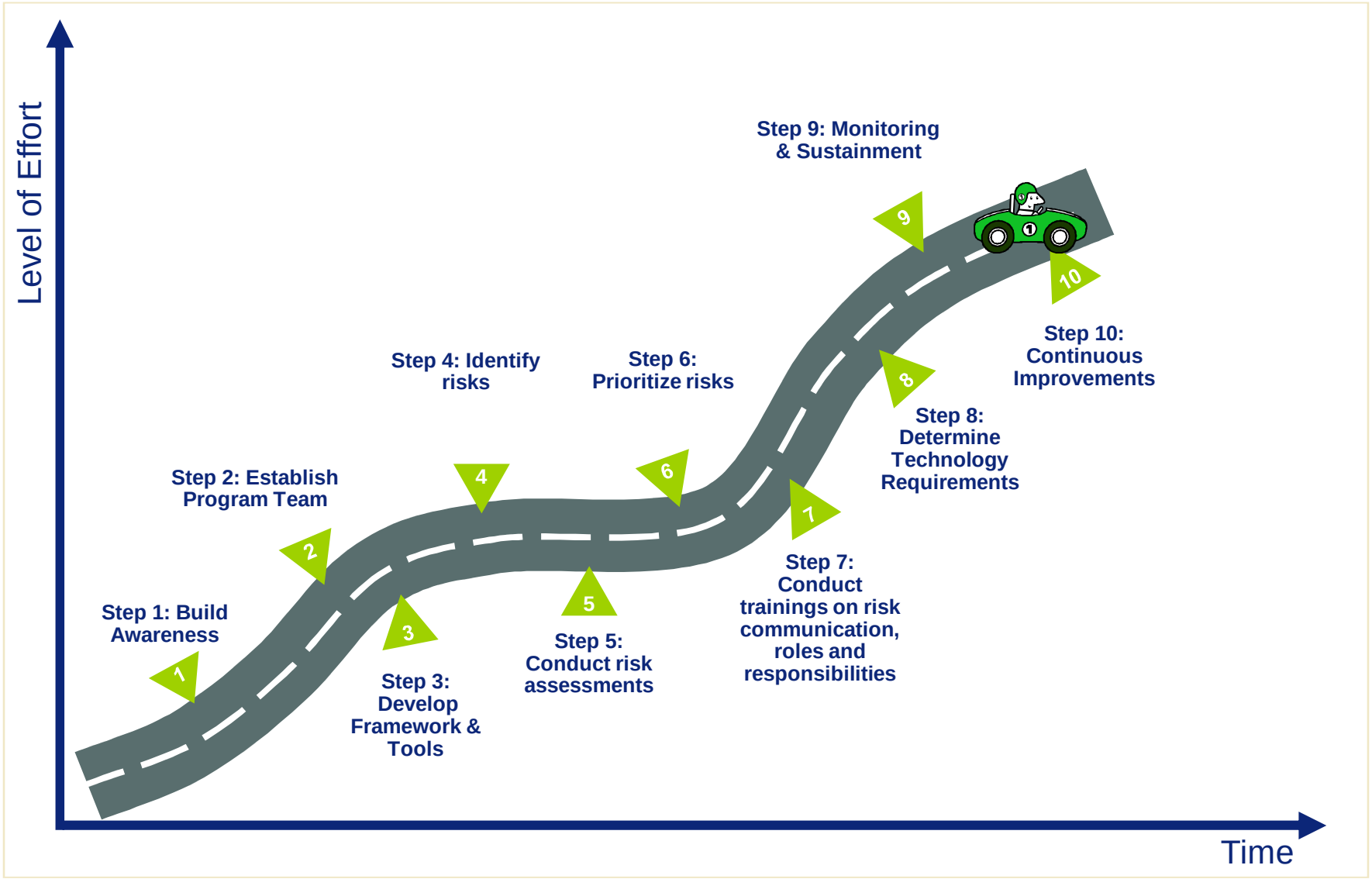
Hard Side

- Policies & procedures
- Risk organization
- Reporting and escalations
- Evaluation
- Systems

Soft Side

- Culture & values
- Skills
- Risk awareness
- Incentives
- Communication

Develop a roadmap for implementing ERM



Critical Success Factors

- Senior executive and board sponsorship
- Specific ownership of risks
- Common language of risk and assessment criteria
- Clear processes for communicating risk management and escalating issues
- Address risks to value creation and value protection

Concluding Thoughts…..

Risk is no longer something to be faced…… it has become a set of opportunities open to choice