protiviti®
Face the Future with Confidence

Enterprise Risk Management (ERM)

An understanding of key concepts for a sustainable implementation

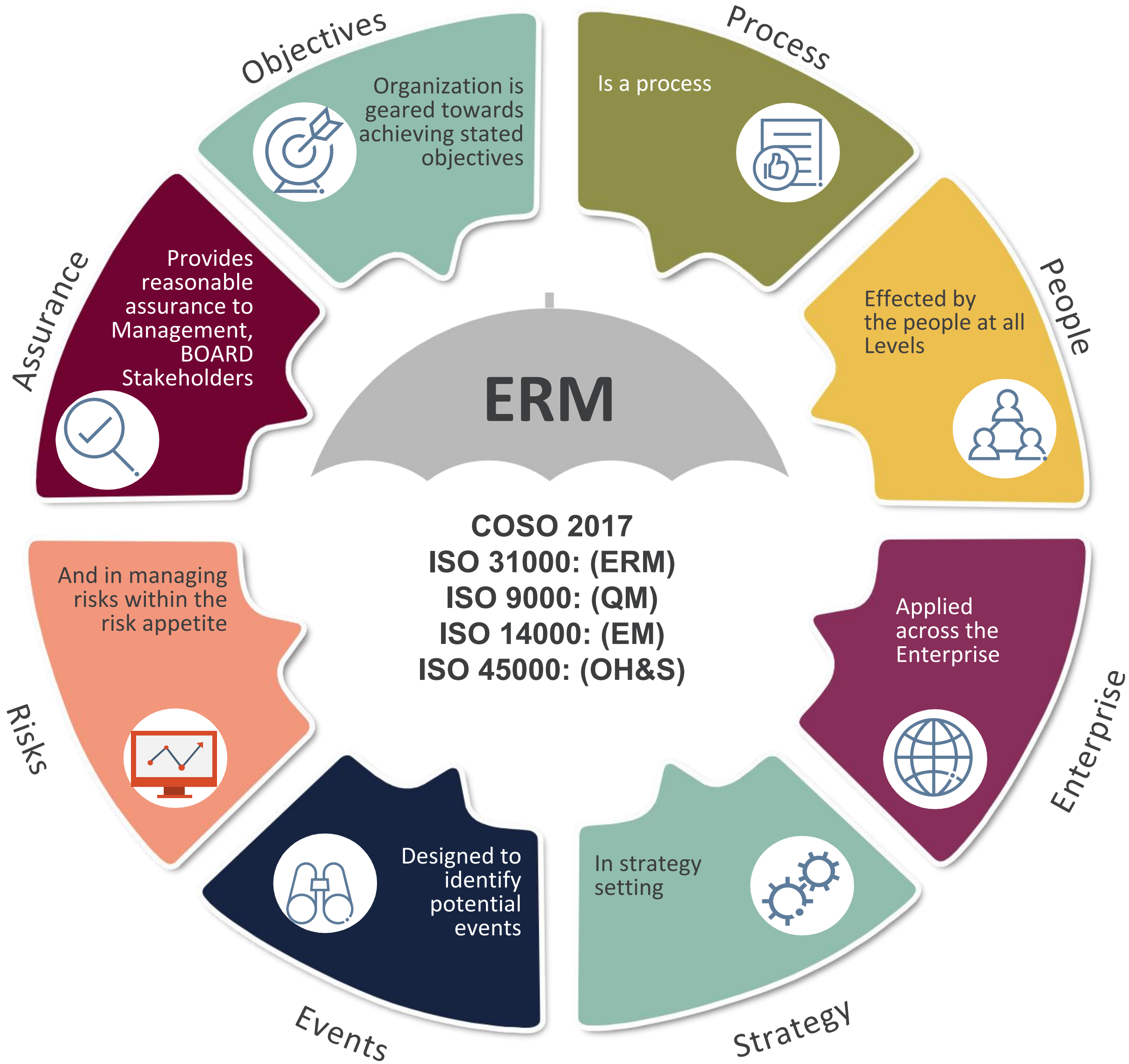
April 2020

Protiviti Perspective provided by Jimmy W., Toronto

Internal Audit, Risk, Business & Technology Consulting

ENTERPRISE RISK MANAGEMENT (ERM)

WHAT IS ERM?


Objectives
Organization is geared towards achieving stated objectives
Process
Is a process
People
Effected by the people at all Levels
Enterprise
Applied across the Enterprise
Strategy
In strategy setting
Events
Designed to identify potential events
Risks
And in managing risks within the risk appetite
Assurance
Provides reasonable assurance to Management, BOARD Stakeholders
ERM
COSO 2017
ISO 31000: (ERM)
ISO 9000: (QM)
ISO 14000: (EM)
ISO 45000: (OH&S)

REGULATORY EMPHASIS ON ERM

1 **Companies Act 2013 and SEBI's Clause 49**

The Board and audit committees have been given specific responsibilities in assessing the robustness of risk management framework implemented in the company.

2 **Section 134**

The Board's Directors report should include a statement on development and implementation of risk management framework for the company, including identification of risk which, as per the Board's opinion, could threaten the very existence of the company.

3 **Section 177**

The audit committee shall act in accordance with the terms of reference specified in writing by the Board, inter alia evaluation of risk management system.

4 **Schedule IV**

Independent directors are required to get assurance the systems of risk management are robust and defensible.

ERM BEYOND REGULATORY: FOCUS ON CULTURE, CAPABILITY & PROCESS BUILDING

Management, Board and the Stakeholders want more value from ERM

- Today, Organization's risk exposures are changing and evolving more rapidly than ever before.
- Several factors are contributing to this trend, such as globalization, growing speed of transactions, growing information sharing and big data, greater instability and volatility of markets, higher expectations from investors and more complex regulations.
- Many traditional ERM initiatives are no longer able to meet the strategic needs of the business as they are:

Risk listing activities carried out for compliance/assurance purposes

Standalone processes with no or limited integration with decision making

Often qualitative exercises, with limited or no quantification

Focused on day-to-day activities instead of strategic objectives

With limited or no impact on key decision-making

Towards a Risk-Informed Perspective

ORGANIZATIONS FOCUS OF ERM CONVERSATION

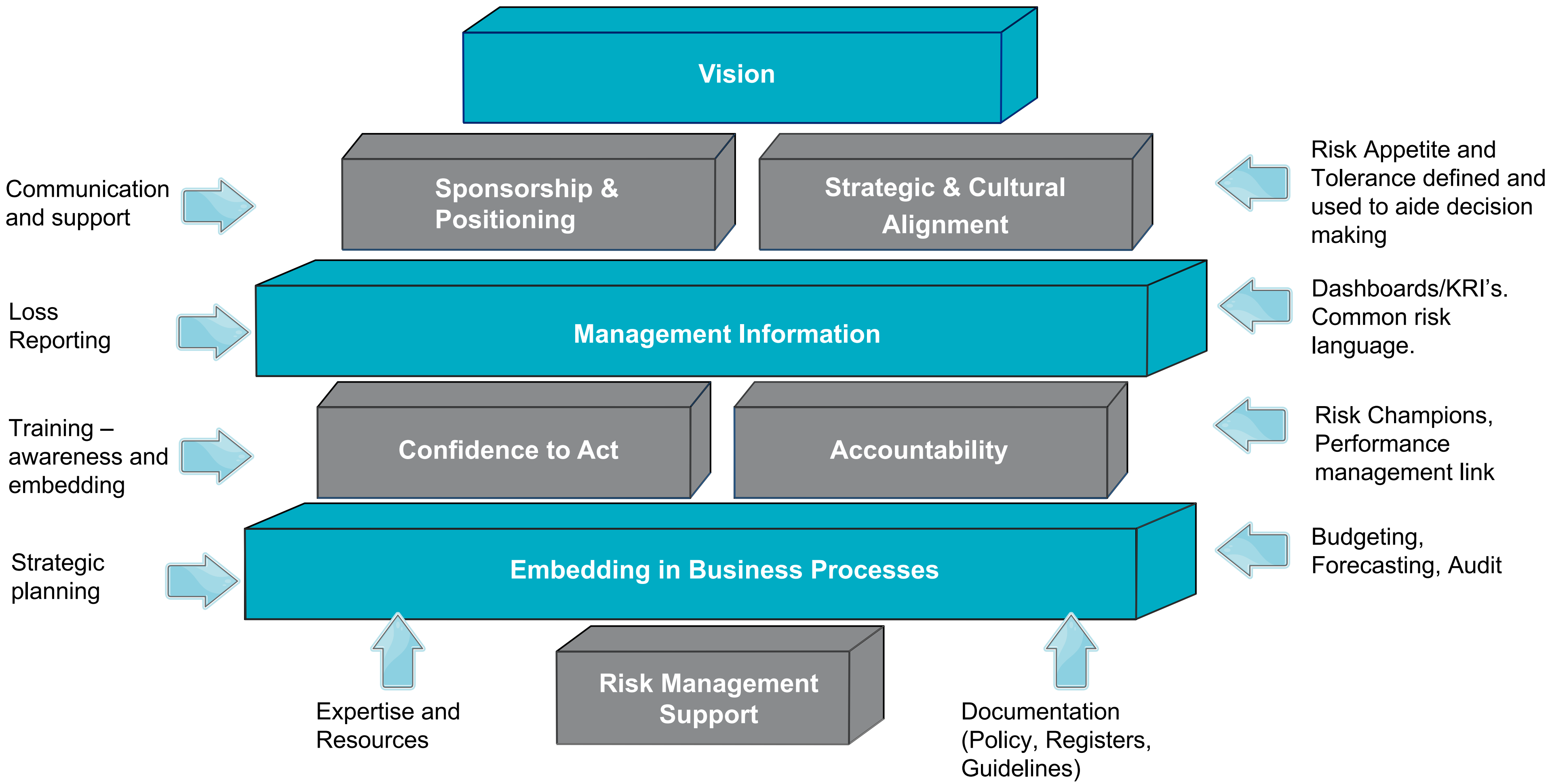
- Focused on what really matters
- Provide information that can
- drive strategic decisions
- Executive led

- Risks / Opportunities
- Qualitative / Quantitative
- Bottom-up / Top-driven

- Strategic planning
- Budgeting and forecasting
- Evaluation of Strategic / Investment Options
- Strategy and Business execution

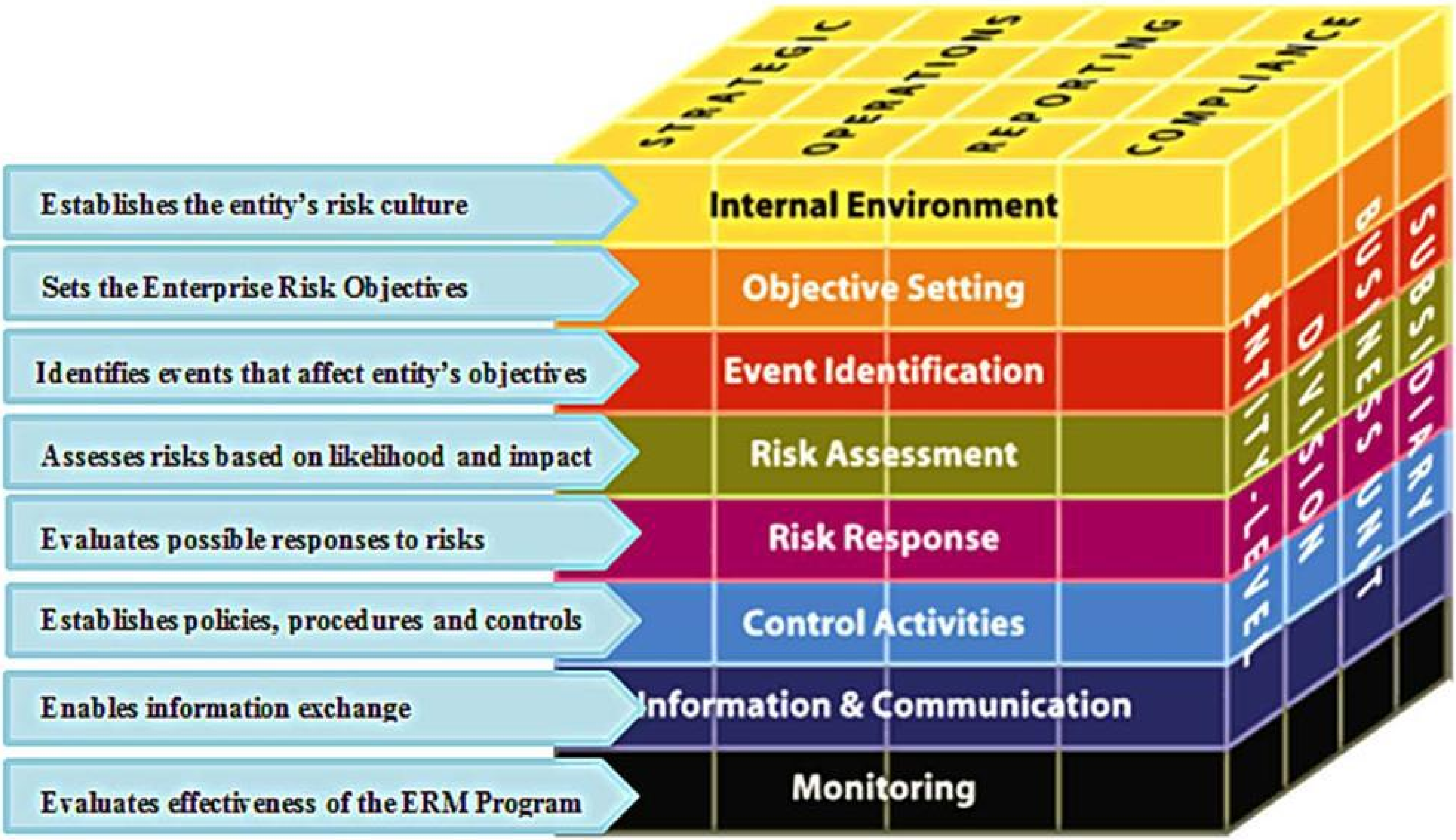
- Consider client's business characteristics and its cultural and organizational attributes
- Respond to specific stakeholders' expectations
- Align with market/industry requirements

ESSENTIAL BUILDING BLOCKS OF ERM



protiviti

ERM FRAMEWORKS: COSO 2017

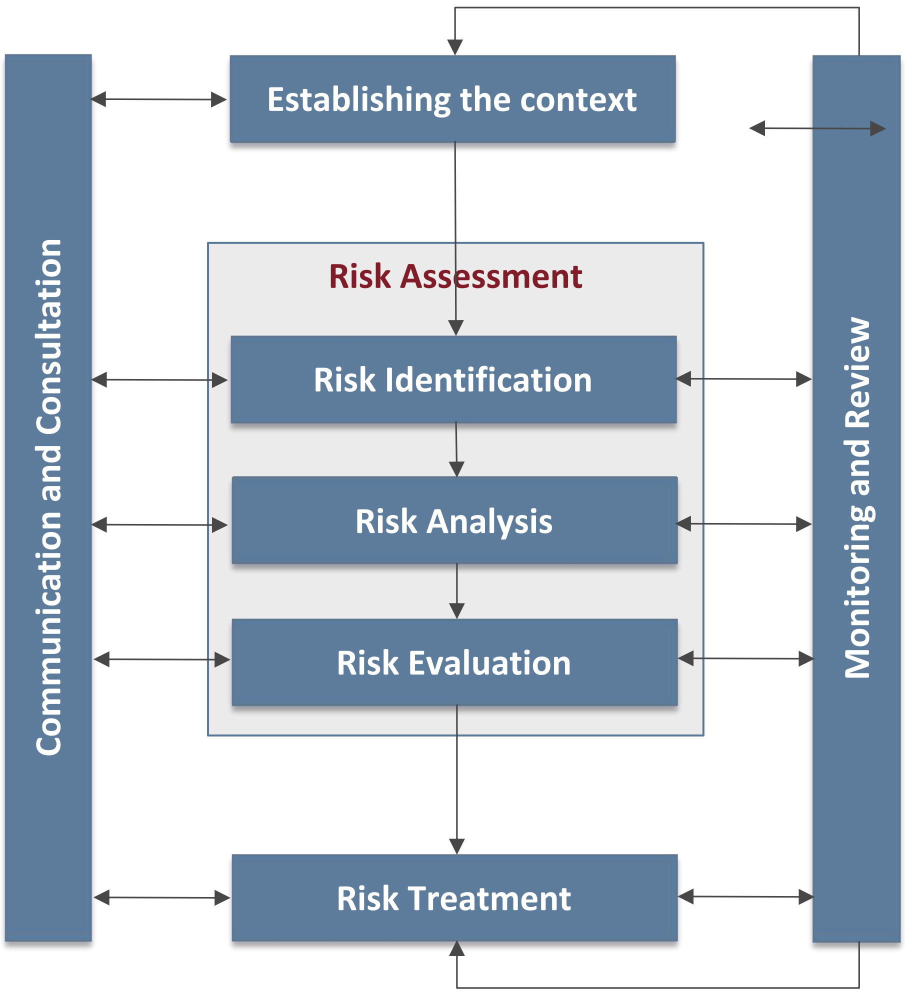


protiviti

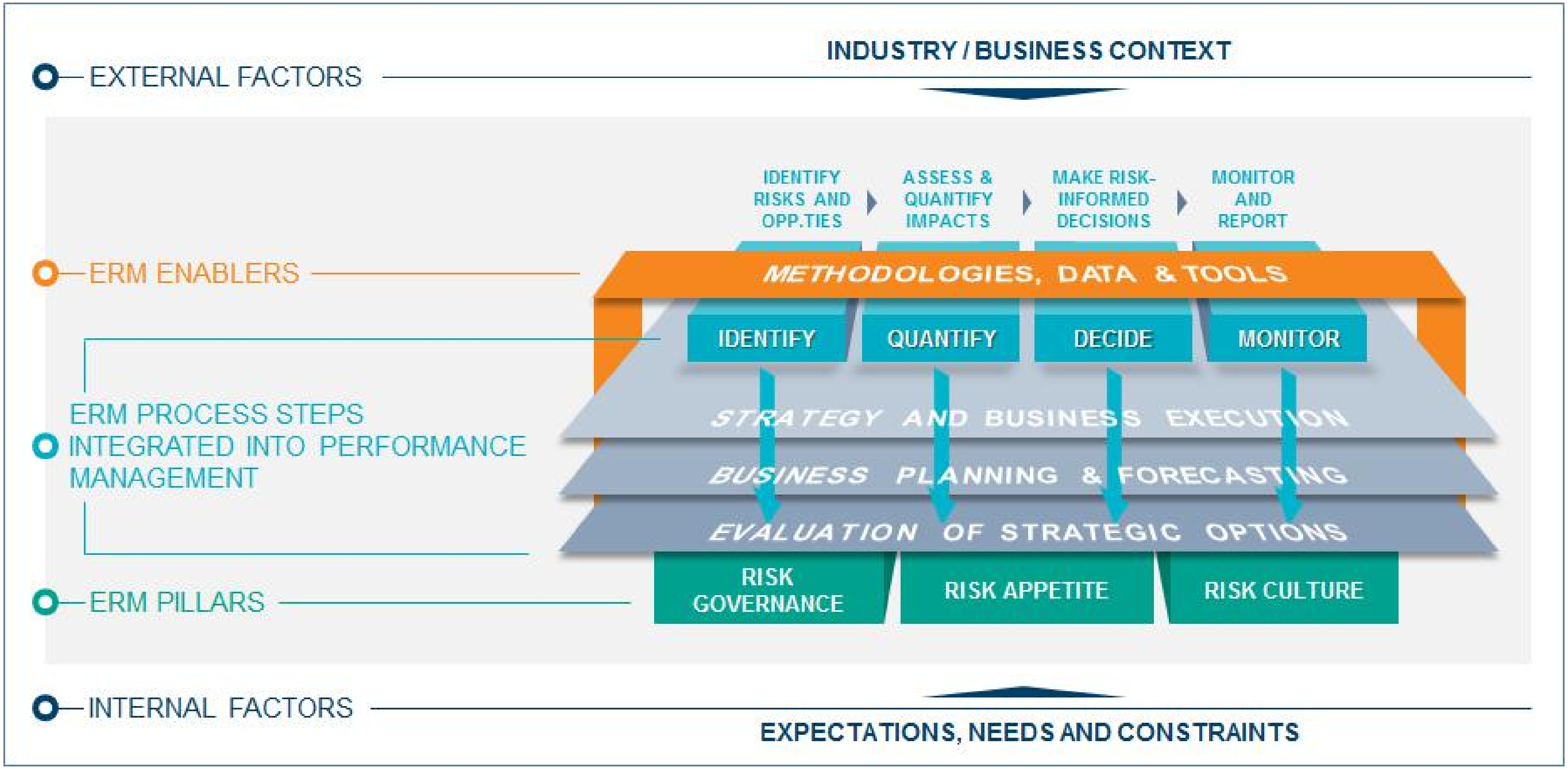
ERM FRAMEWORKS: COSO 2017

Risk management

- Creates and protects value
- Integral part of organizational processes
- Part of decision making
- Explicitly addresses uncertainty
- Systematic, structured and timely
- Based on the best information
- Tailored
- Takes human and cultural factors into account
- Transparent and inclusive
- Dynamic, iterative and responsive to change
- Facilitates continual improvement of the organisation



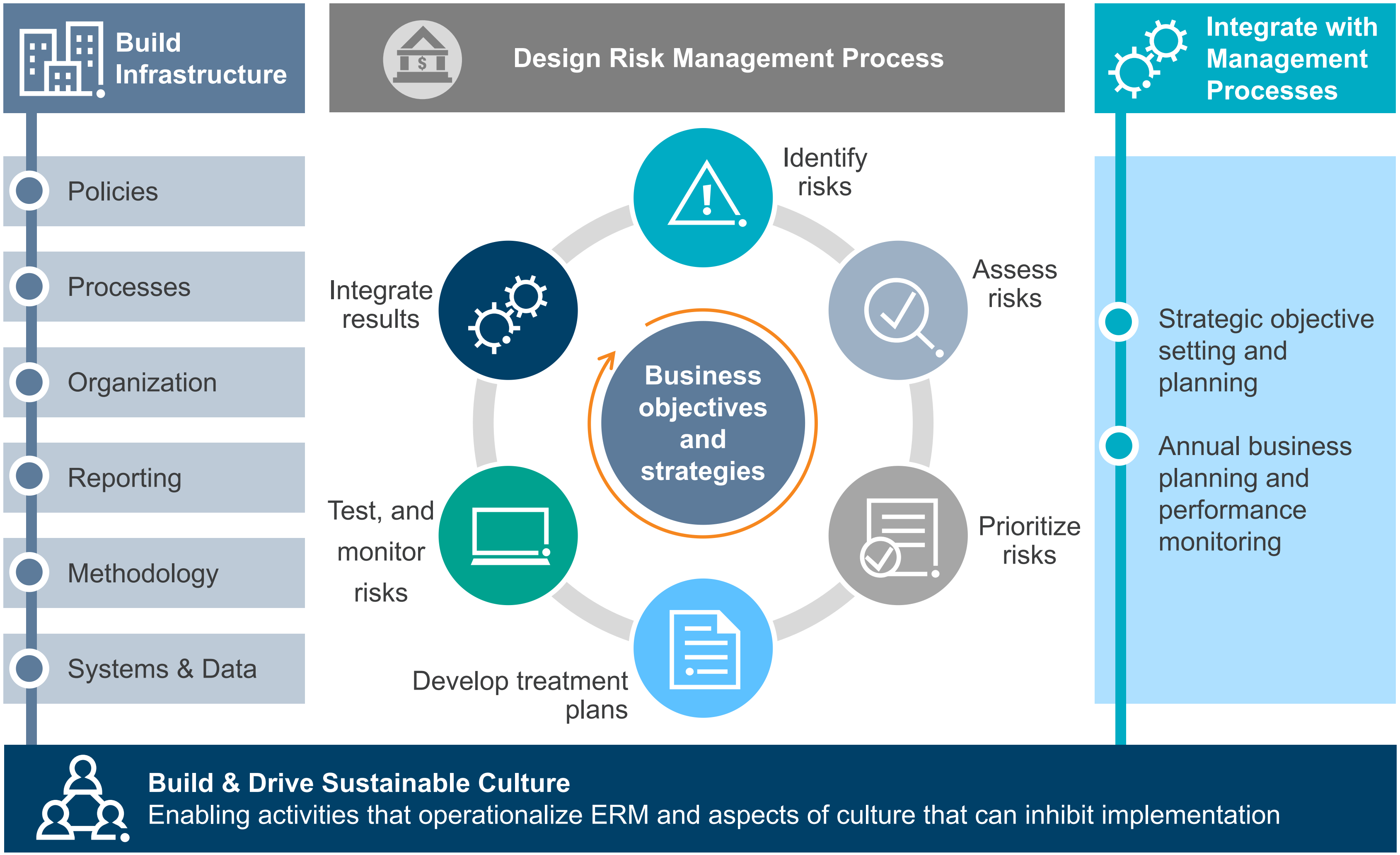
PROTIVITI ERM FRAMEWORK



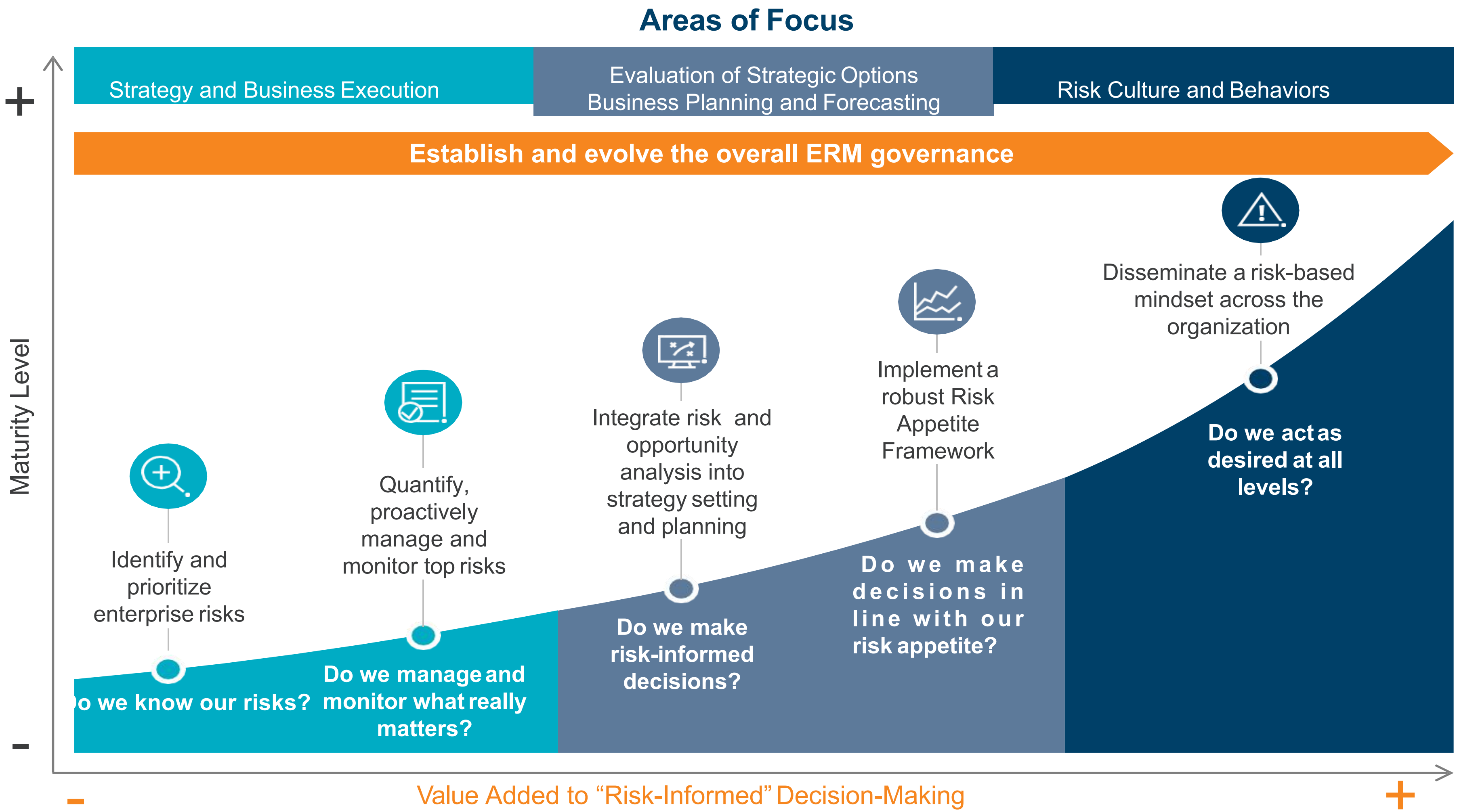
protiviti

PROTIVITI ERM METHODOLOGY

Protiviti's methodology is a judicious blend of recommended standards and field tested practical activities, aimed at building an effective proactive framework encompassing a universe of applicable business risks



CAPABILITY MATURITY ASSESSMENT: STARTING POINT FOR ERM



ERM FRAMEWORK CONSTITUENTS

1. Risk appetite and tolerance (RACM)

Define risk appetite/tolerance at an Enterprise and SBU level for guidance, evaluation and acceptance or risks

2. Risk Governance structure

Define key constituents of the governance structure (sponsors; decision makers; custodians and enablers

3. Risk Identification

- Risk identification techniques
- Risk capture into risk register

4. Risk analysis method

- Qualitative analysis - Impact/Likelihood matrix
- Quantitative analysis – Monte Carlo simulation

5. Risk Treatment

- Risk treatment strategy and process of risk mitigation

6. Risk monitoring and reporting

- Risk monitoring mechanism
- Risk reporting mechanism

protiviti

RISK APPETITE AND TOLERANCE

Risk Assessment Criteria Matrix (RACM) is a reflection of Company's risk appetite and tolerance, in the current context of business and economic environment.

1 Entity level RACM

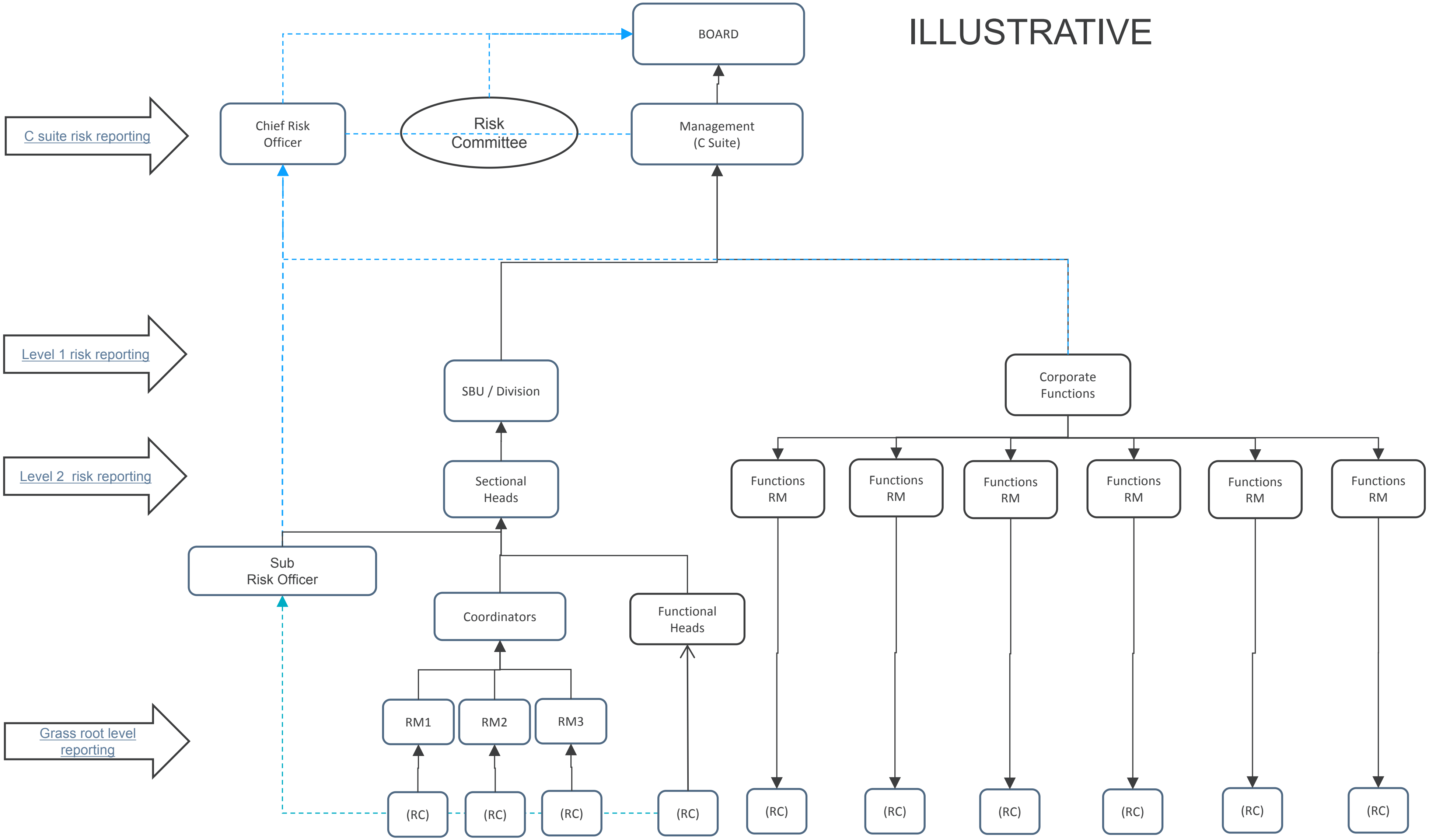
Entity level risk assessment criteria matrix may be based on key parameters like

- Strategic
- Operational
- Financial
- Legal, contractual, Compliance,
- Reputational.

IMPACT					LIKELIHOOD	
Scores & Rating	Financial / Materiality	Operational	Regulatory & Compliance	Reputational	Score Rating	Likelihood (within 3 year)
5 Critical	**Adverse impact on assets, annual revenues, costs or profit:** > USD 9.3 mln (~ 10% of 2012' projected Net Income after tax)	**Operational failures due to feed gas unavailability, technical, environmental, logistics, HR issues leading to production & delivery shortfall of** >3 cargoes.	**Regulatory non compliances leading to:** cancellation of license or entry in to other geography / country of major interest / exposures	**Bad publicity or damage to reputation:** Globally	5 Expected	50% to 100 %
4 Significant	USD 7 mln to USD 9.29 mln (~ 7.5 to 10% of projected Net Earnings)	3 cargoes.	Regulatory non compliances leading to cancellation & temporary ban on entry.	Regional (GCC) perspective	4 Highly likely	25 % to 50 %
3 High	USD 4.7 mln to USD 6.99 mln (~ 5 to 7.5% of projected Net Earnings.	2 cargoes.	Non compliances leading to major financial penalties.	Country perspective	3 Likely	10 % to 25 %
2 Moderate	USD 2.3 mln to USD 4.69 mln (~ 2.5 to 5% of projected Net Earnings)	1 cargo.	Non compliances leading to minor financial penalties.	Specific audience	2 Slightly	5% to 10 %
1 Low	<USD 2.3 mln (~ 2.5% of projected Net Earnings)	1cargo in 2 years	Non compliances leading to insignificant financial penalties.	Insignificant audience	1 Not Likely	0 to 5 %

RISK GOVERNANCE STRUCTURE

ILLUSTRATIVE



protiviti

RISK IDENTIFICATION TECHNIQUES

1. Questionnaires and risk surveys
2. Interviews and discussions
3. Financial statement analysis
4. Process flowcharts analysis
5. Analysis of business process drivers
6. Periodic MIS reports for the division (corporate, regions and projects) and review meetings
7. On a review of Internal and external audit reports
8. Update on several on-going matters and personal inspection
9. Loss histories / hazardous events

FORMATION OF RISK STATEMENT

Risk statement provides three-part structured “Risk Statement” ” : “As a result of <definite cause>, <uncertain event> may occur, which would lead to <effect on objective(s)>.”

Example :

- Incorrect item rate analysis (Fact=cause) at the tendering stage due to unrealistic assumptions (Uncertainty=risk) may lead to incorrect cost (Contingent possibility=effect) estimations for the project

- Overwhelming project compulsions (i.e. completion of project in stipulated time, cost and margins etc.) and pressures from the project manager (Fact=cause) may curb the assertiveness and independence of the quality manager at site (Uncertainty=risk) leading to compromise in quality enforcement (Contingent possibility=effect).

RISK ANALYSIS

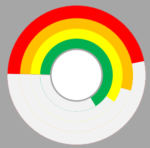
Risk Analysis involves clearly understanding of the risk sources, the potential impact/consequences and any treatments/controls that are currently in-place

Qualitative risk analysis – Impact / Likelihood rating matrix

Impact matrix

Impact matrix lists the standard definition of impact matrix based on various parameters like delay, shortfall of revenue etc. The rating of the impact is a scale from "1 to 5"

- Negligible
- Minor
- Moderate
- Significant
- Severe



Likelihood matrix

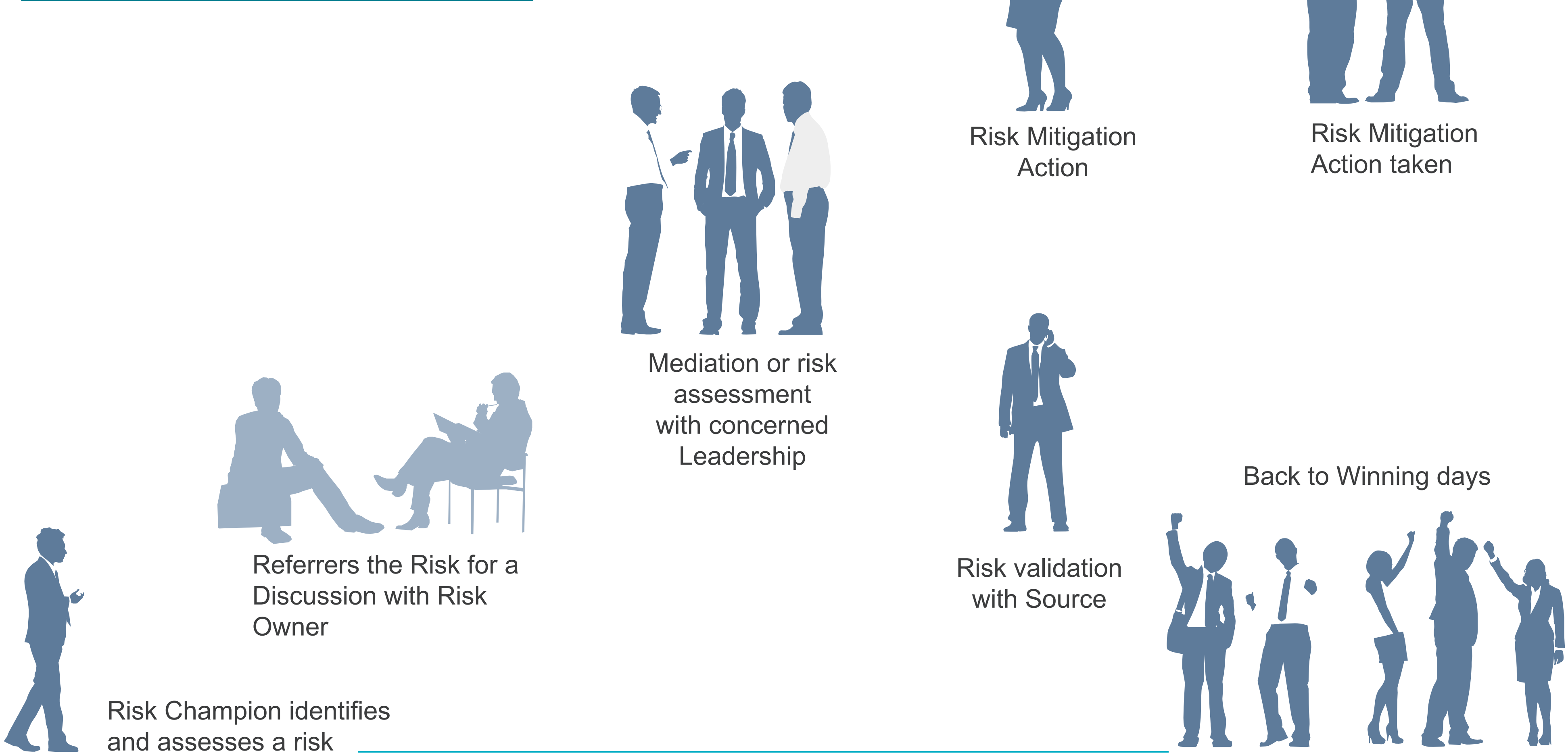
Likelihood matrix represent the probability of the impact to occur on the business activities in case the risk occurred. The rating of the probability is a scale from "1 to 5":

- Very unlikely
- Unlikely
- Possible
- Likely
- Very Likely

ENTERING THE RISKS INTO RISK REGISTER

RISK ANALYSIS

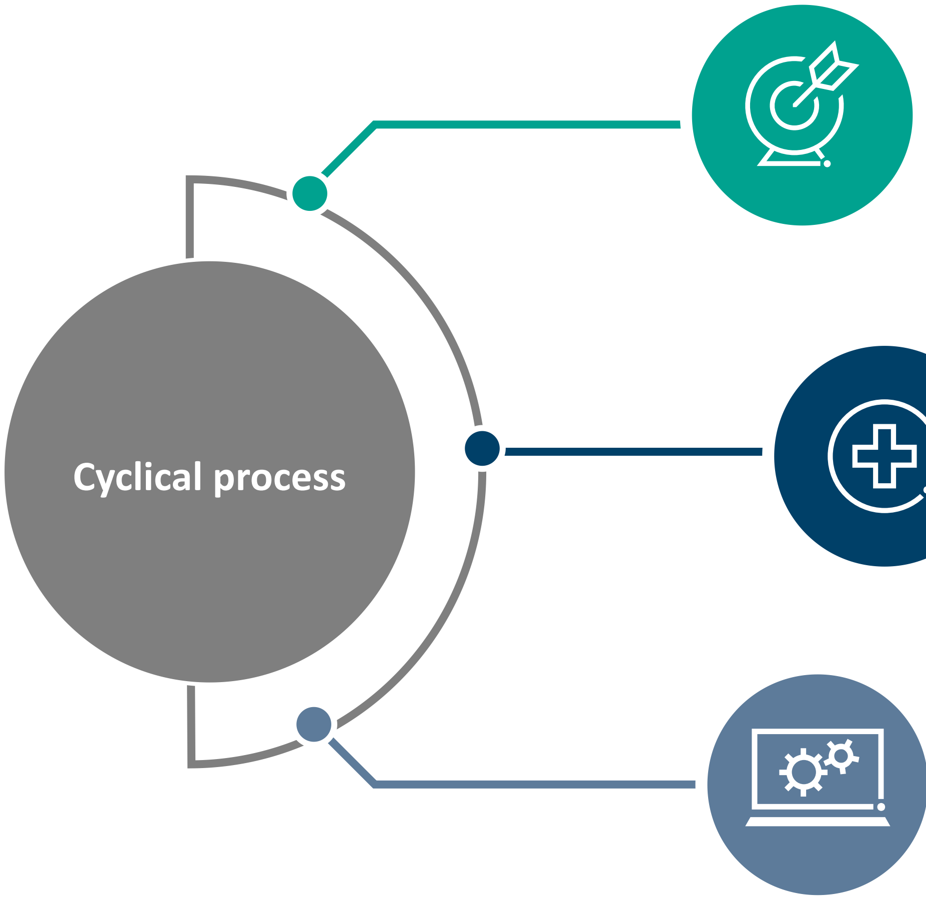
A culture of open dialogue and empowerment, at all levels, greatly benefits the risk management process. Organization wins.



protiviti

RISK TREATMENTS

Risk treatment involves selecting one or more options for modifying risks, and implementing those options



Risk Strategies
Retain
Reduce
Transfer
Avoid

Risk Treatment Process
Root cause analysis
Development of treatment plans

Effectiveness Tracking
Review of treatment by (Risk Officers)
Effectiveness tracking by pre define template

Suggested treatment plans implementation tracker

RISK TREATMENTS: PREREQUISITES

1. Every root cause should at least have one treatment plan

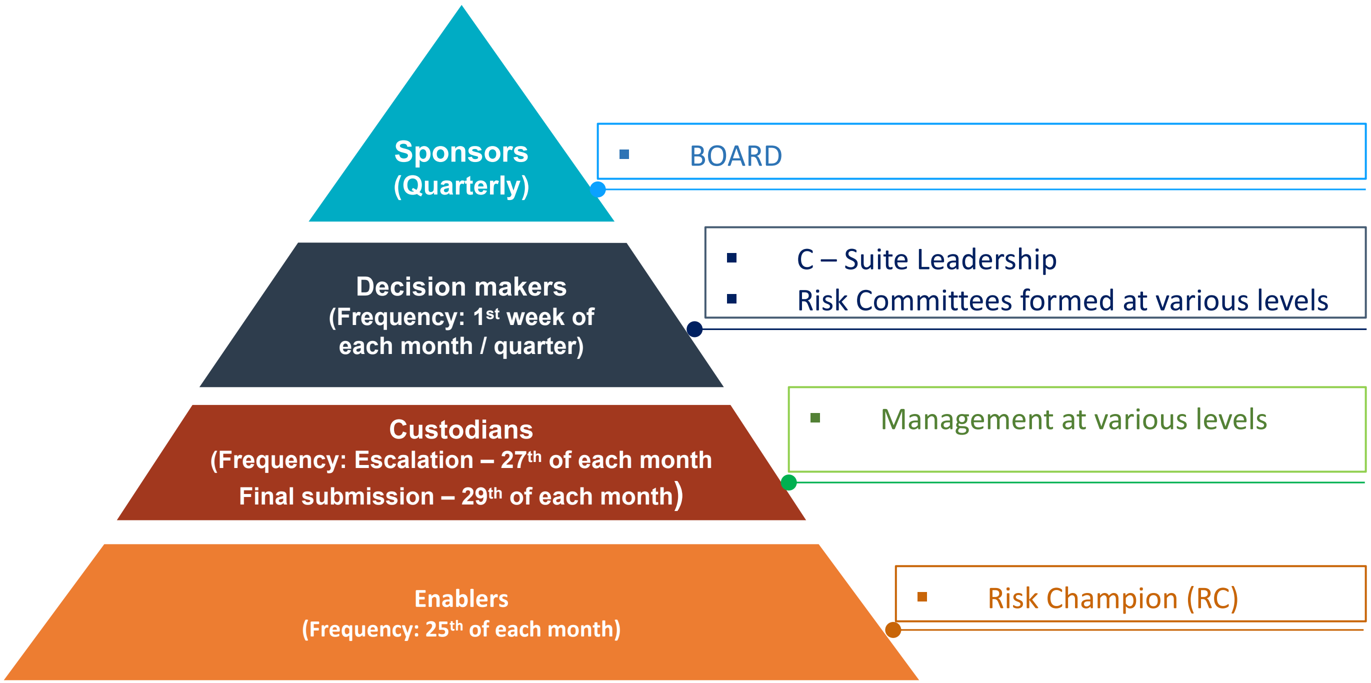
2. Treatment plans need to be modular in nature with clear cut action steps.

3. Treatment plans can be described at a concept level for lower risk ratings. However with higher rating, they need to be articulated with detailed action plan, sub tasks with dates for implementation

4. Pre articulated treatment plans must be validated to withstand the ‘test of time and current set of challenges and either be fine tuned or revamped to achieve the desired mitigation

5. Evert treatment plan should have a clear ownership and single point accountability

RISK MONITORING & REPORTING



Risk reporting involves key stakeholders to timely report the updated risk registers and related information based on the frequency defined for different levels

protiviti

KEY CHALLENGES IN ERM IMPLEMENTATION

- Failure to obtain "buy-in" and support from Executive Management / Allowing ERM to become a compliance program.
- Development of a centre of excellence for managing risk, drawing on the expertise of highly skilled individual risk managers
- Risk management not embed in day to day operations. Roles & responsibilities of participants not clearly defined
- Insufficient emphasis on defining information and reporting needs / Failure to integrate ERM into key management processes and performance management (i.e., metrics, scorecards, dashboards).
- Lack of planning and foresight in roll out a training, communication and sustenance programme for ERM
- Incentivizing ERM program for its success and sustenance

Face the Future with Confidence

protiviti®