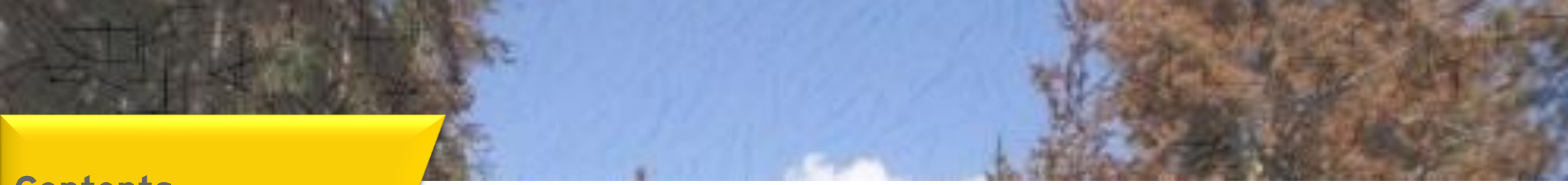
EY
Building a better working world

Enterprise Risk Management

2022



Contents

The present document is aimed to:

1. Give an overview of the Risk Management framework
2. Illustrate an ERM model

Context

The recent turmoil in the **international economic scenario** has increasingly revealed the **weaknesses** of **Risk Management** and **Internal Control Systems.** This scenario is characterized by:

Context	▸ Sudden **fluctuations** in demand ▸ **Volatility** of **financial markets** ▸ Strong **regulatory measures** of Supervisory Authorities ▸ **Financial collapses** of world-leading companies
Old Risk Governance Model	▸ **Risk governance** models were generally built around **regulatory compliance requirements**, and operate through a series of uncoordinated controls and systems
Evolution	The ability of each player to **comprehend and manage risks** is critical in order to **identify** and **exploit opportunities.** To formulate and implement **successful strategic decisions** within complex ecosystems, operators must therefore ensure that their **Risk Management Model** is efficient and constantly updated.

What is a risk?

Risk can be defined as:

- Any event or action that could influence the achievement of Company's objectives.

- This definition highlights risk as an **uncertainty of an outcome** which can relate to either a threat (downside) or an opportunity (upside).

Importance and Benefits of Enterprise Risk Management (ERM)

ERM is a framework of **systematic management practices** to assess and monitor risk

Systematic management practices:

- To improve the way that the risk is managed
- Supported and enabled by the appropriate risk management framework

1. Minimizing **threats**
2. Maximizing **opportunities**

EY

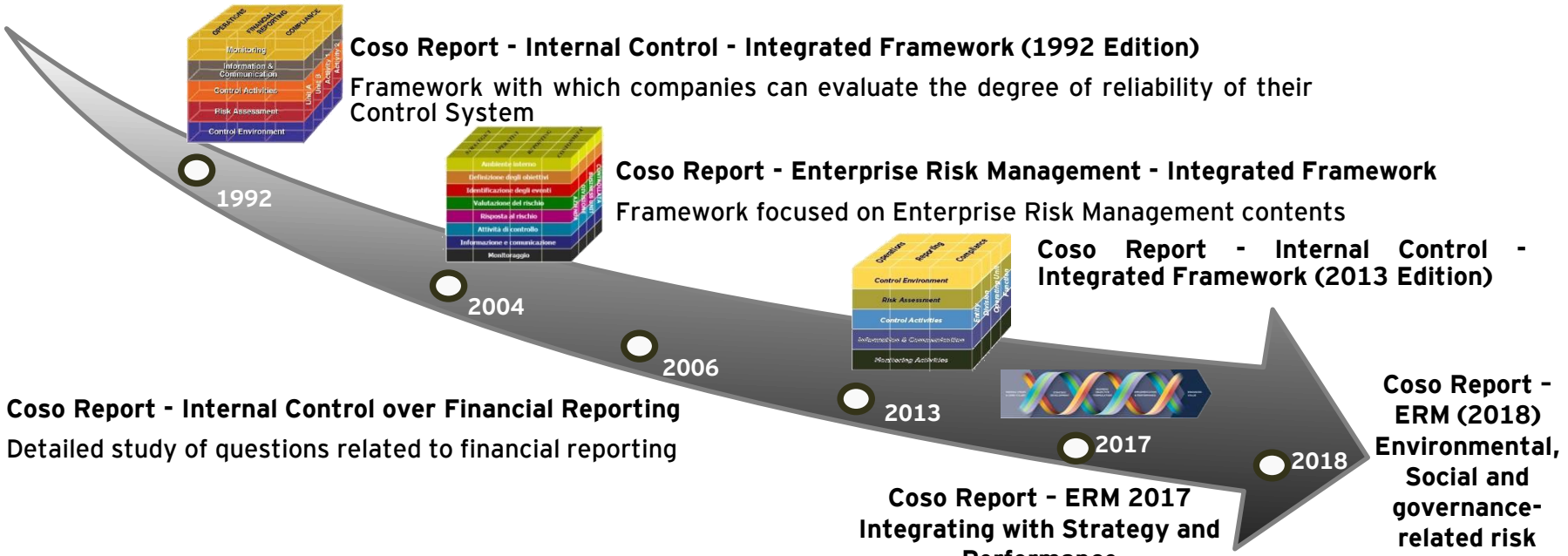
Risk Management
Regulatory framework

Below the main **normative requirements** for the definition and implementation of **Risk Management Models.**

International Organization for Standardization (the most important globally recognised organization for definition of technical standards) issued the following reports:

- **ISO 31000:2018, Risk management – Principles and guidelines and related standard**

Committee of Sponsoring Organizations of the Treadway Commission (worldwide organization for the development of frameworks and guidelines in the field of Enterprise Risk Management, Internal Audit and Anti-Fraud) issued the following reports:



Coso Report - Internal Control - Integrated Framework (1992 Edition)

Framework with which companies can evaluate the degree of reliability of their Control System

Coso Report - Enterprise Risk Management - Integrated Framework

Framework focused on Enterprise Risk Management contents

Coso Report - Internal Control - Integrated Framework (2013 Edition)

Coso Report - Internal Control over Financial Reporting

Detailed study of questions related to financial reporting

Coso Report – ERM 2017 Integrating with Strategy and Performance

Coso Report – ERM (2018) Environmental, Social and governance-related risk

Business Objectives

ERM is oriented to achieving an entity's objectives, set forth in four categories:

Strategic:

These objectives are high level and are aligned with an entity's mission.

Operational:

These objectives refer to the effective and efficient use of resources.

Financial:

These objectives surround an entity's need for financial sustainability.

Compliance:

These objectives refer to an entity's need to comply with applicable laws, regulations and procedures.

Risk Identification

Risk identification - Risk Universe

The results of **business targets** analysis and underlying risks are used to define the **Risk Universe** of the Company.

Risk Identification

Risks can be classified as follows:

Risk categories

COMPLIANCE

Legal or administrative sanctions, financial losses or reputational damage as a result of violations of laws, regulations or self-regulations.

FINANCIAL

These risks include Liquidity risk, Credit risk, risks of financial markets, risks relating to the accuracy and integrity of communications to the market and generally risks associated with **Financial Management.** Accuracy of Financial information communicated externally and within the company.

OPERATIONS

Risks that derive from **inadequacy or malfunction of business processes**, because of the ineffective and inefficient use of resources.

STRATEGIC

Threats to the current competitive position of the Company and the **achievement of strategic objectives**, resulting from operating context, inadequate or untimely decision making in relation to the competitive and dynamic business context, exposure to exogenous factors.

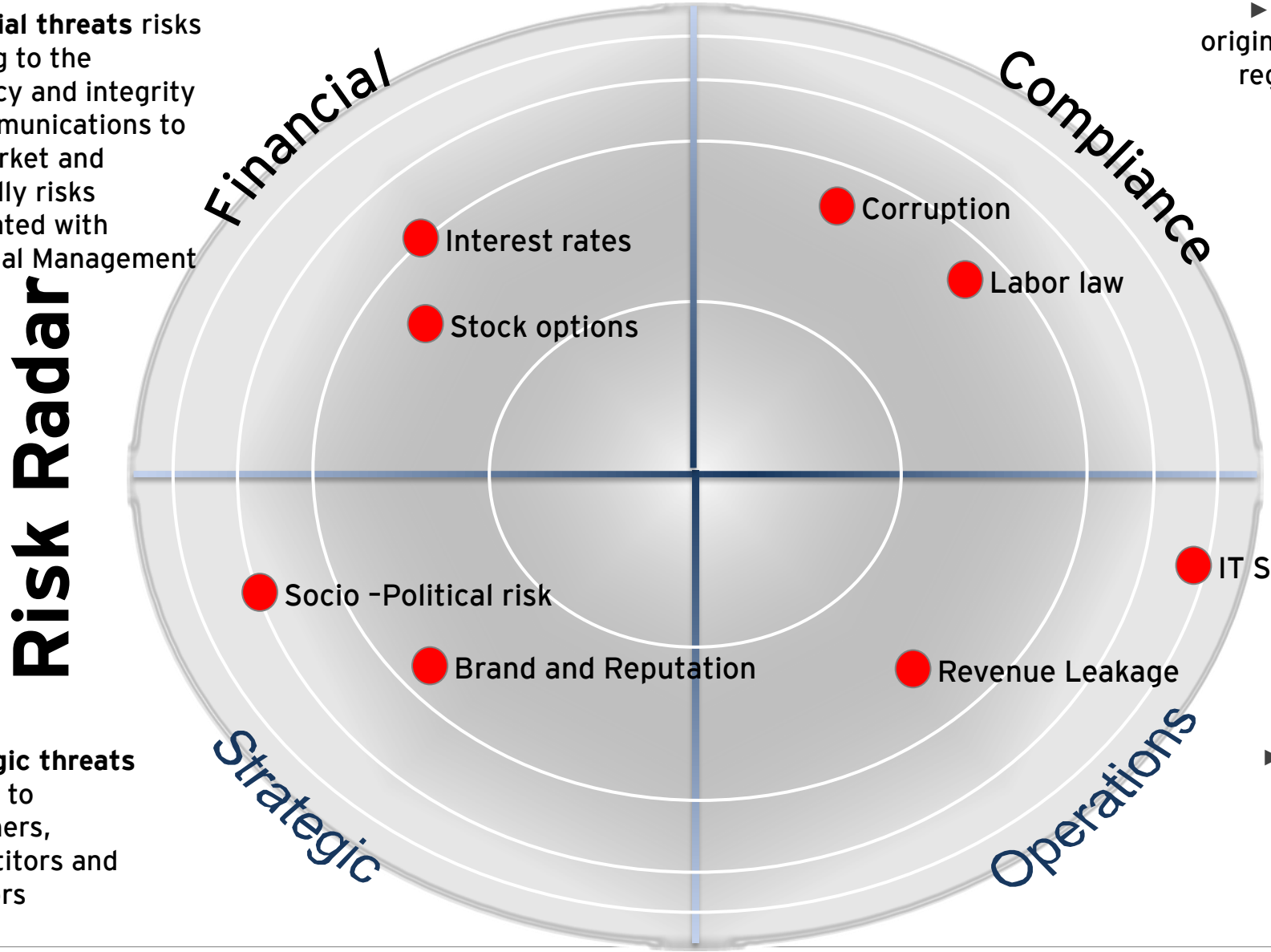
EY

Risk Radar

Below is an example of Risk Radar

- **Financial threats** risks relating to the accuracy and integrity of communications to the market and generally risks associated with Financial Management

- **Compliance threats** originating in politics, law, regulation or corporate governance



- **Strategic threats** related to customers, competitors and investors

- **Operational threats** impacting the processes, systems, people and overall value chain of a business

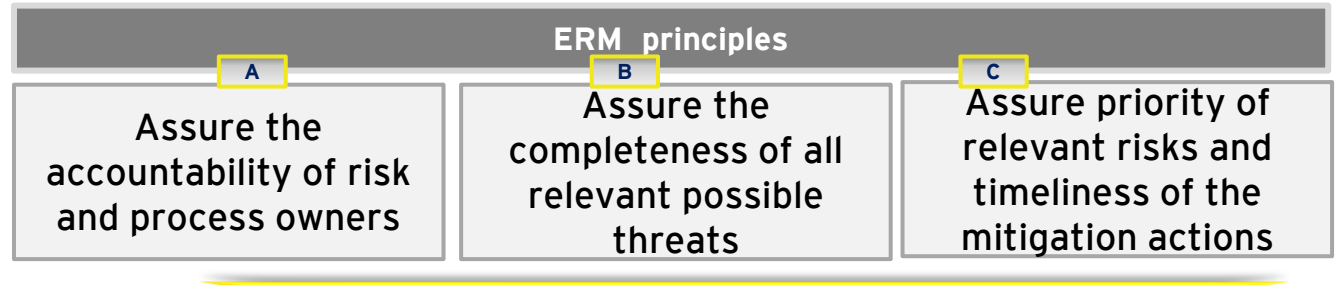
Exercise

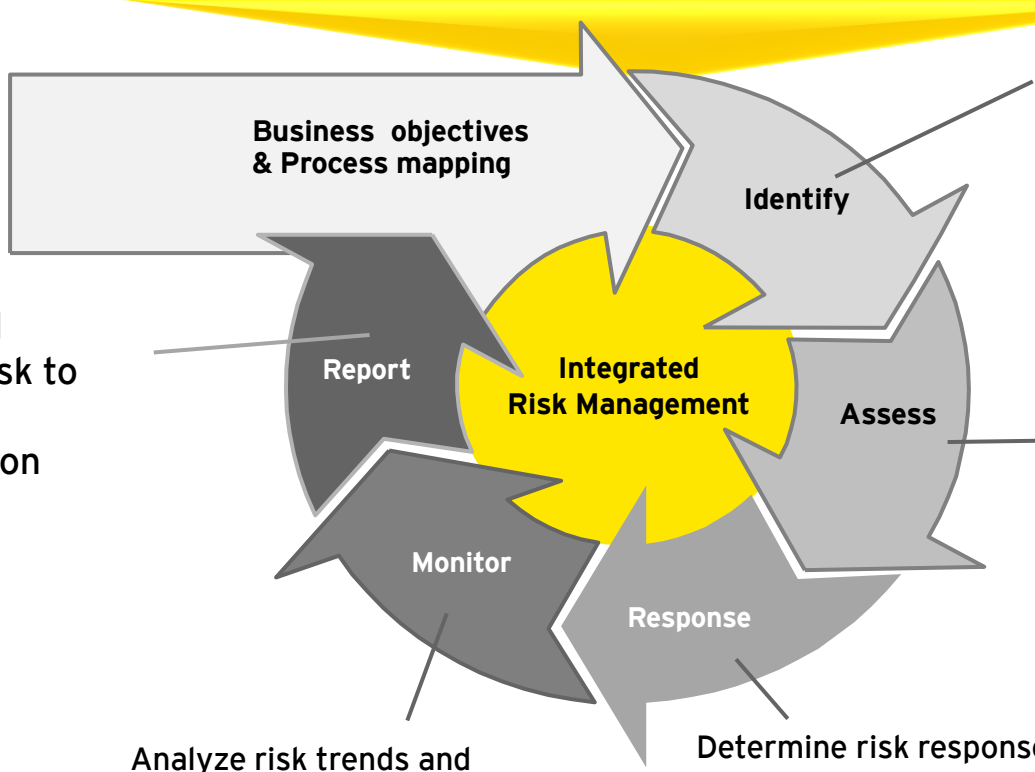
Categorize the following risks by source

		Risk category
Event 1	UnGuard Delivery is located downtown adjacent to a federal building in a major U.S. city. Yesterday, a **terrorist car bomb exploded** just outside the federal building, **completely destroying** both the federal building and UnGuard's headquarters. Virtually **all of UnGuard's top management**, including its top 25 salespeople, **were killed in the blast**. It was unusual for such a concentration of key employees to be present at UnGuard's headquarters, but they were hosting a special event in their largest meeting room, which was closest to the location of the bomb.	**Operational** ▪ **Disaster**
Event 2	The **stock market went down 25%** and has remained there for the past year. Aside from the fact that Shop-and-Spend had 100% of their assets in equities, **business is down. People are not shopping as much lately.** The gloomy economic projections have not improved since the day they were announced by the government the morning of the market crash. People have less disposable income.	**Strategic** ▪ **Economic** **Financial** ▪ **Market**

Risk Management
ERM Model

Below the **Enterprise Risk Management cycle:**





Identify potential risks by performing analysis of internal and external exposures

Assess identified risks against risk rating criteria

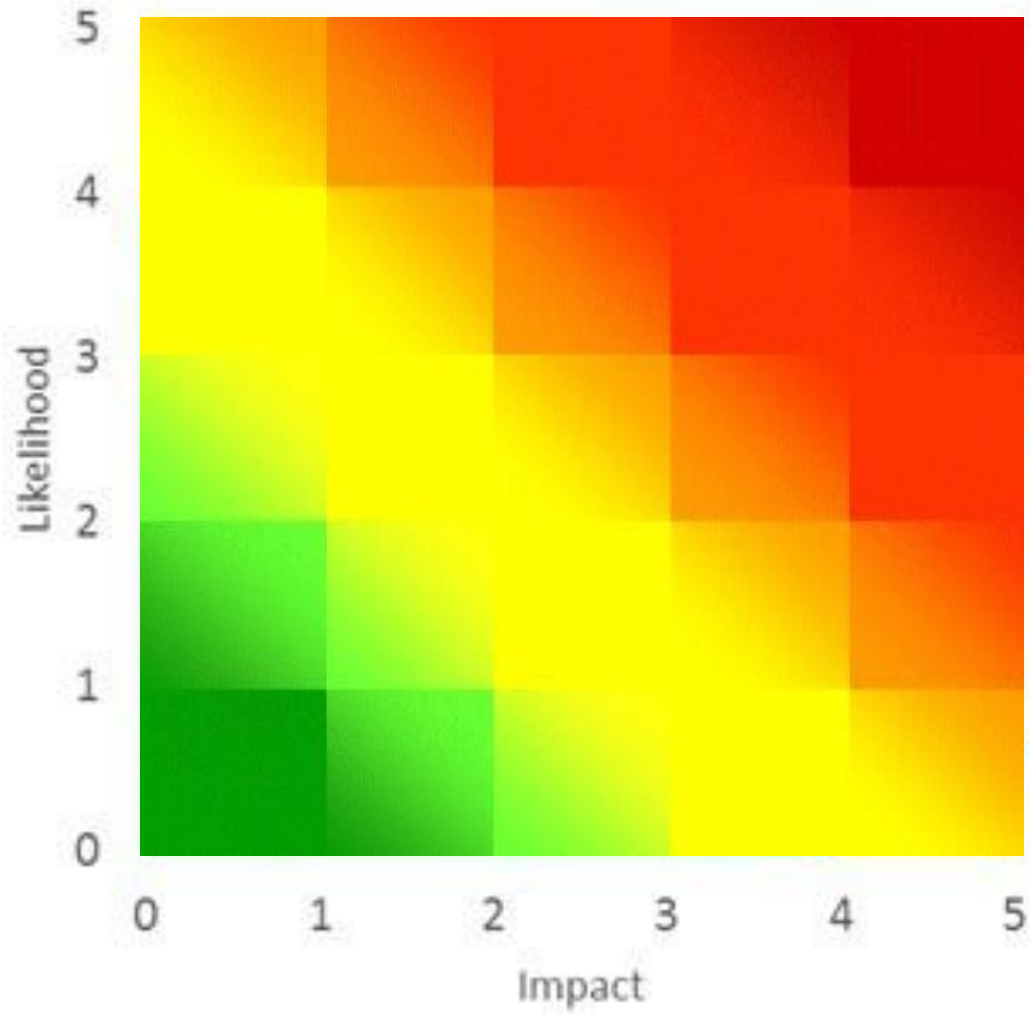
Determine risk response and perform risk treatment; remediation or acceptance

Analyze risk trends and monitor status of risk mitigation plans

Provide holistic and targeted views of risk to support efficient management decision making

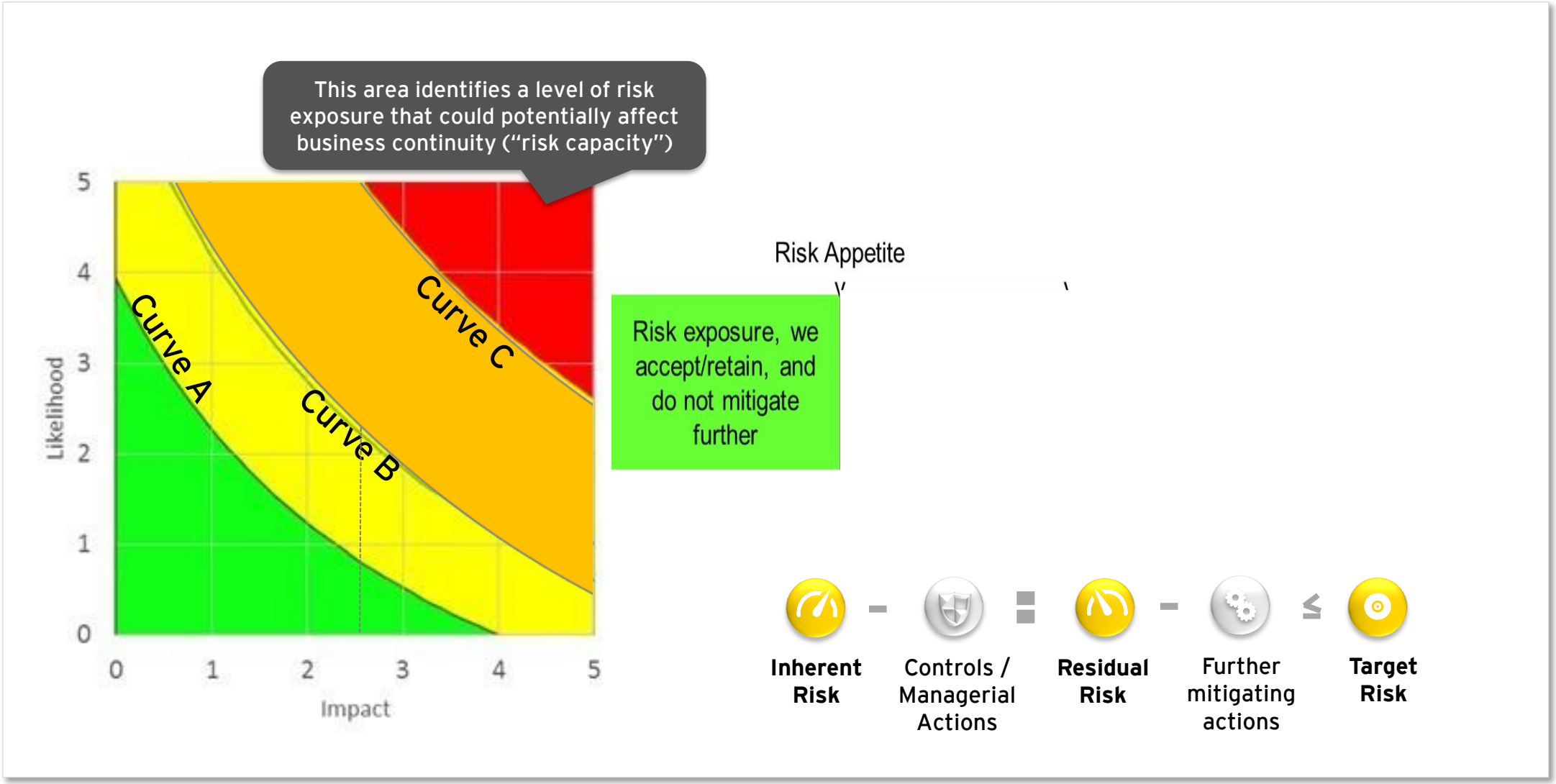
Risk Assessment
5x5 matrix

The assessment of risk, based on the product of likelihood and impact, allows to place the same on a 5 x 5 risk matrix, classifying it as "High", "Medium", “Low".



Risk Assessment
Risk Appetite and Risk Tolerance

The following figure shows the curves of Risk Appetite and Risk Tolerance in function of which the values of Risk are measured, in order to determine the need to implement additional mitigation actions to achieve the Target Risk.



Risk Assessment
Inherent risk

Below an example of **parameters and drivers** for the likelihood and impact evaluation in order to determine inherent risk level.

Parameters and evaluation drivers

LIKELIHOOD	VERY LIKELY (5)	LIKELY (4)	MODERATE (3)	UNLIKELY (2)	REMOTE (1)
Uncertain context	It is expected that the event / risk will occur **frequently during the coming year**	It is expected that the event / risk will occur **several times during the coming year**	It is expected … event / ri… **sometimes** o… **the comi…**	It is expected that the …ent / risk will occur …**uring the**	It is expected that the event / risk will not occur **frequently during the next 3 years**
Predictable context	The event / risk occurred **very frequently during the last year**	The event / risk occurred **several times during the last year**	The ev… **sometimes** occ… **during the last year**		…k did not occur **…last**
Measurable context	The event / risk occurs in **more than 50%** of cases	The event / risk occurs between **the 20% and 50% of cases**	The event / risk occurs between **5% and 20% of cases**	The event / risk o… between **1% and 5% of cases**	…curs in less t… **…cases**

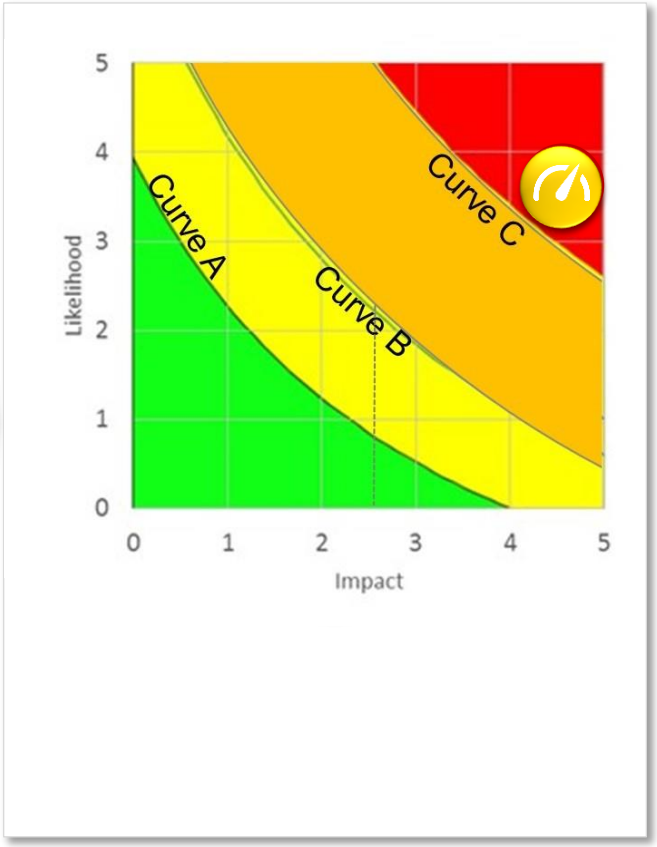
IMPACT		VERY HIGH (5)	HIGH (4)	MEDIUM (3)	LOW (2)	NEGLIGIBLE (1)
Economic		…	….	Potential damage caused by the event between **1,5% and 2,5%** of FCF	Potential damage caused by the event between **0,5% and 1,5%** of FCF	Potential damage caused by the event **lower than 0,5%** of FCF
Qualitative Drivers	**Operational**	Threat to **business continuity**. **Very negative** impact on the achievement of objectives. **…**	Impact over **5-6** business processes. **Negative** impact on goals achievement. **..**	Impact over … proc… **Medium** impact o… achievement. **…**		**…ligible** impact on …ment. …on …
	Reputation	**Very high** potential impact on the image and on the **national and international** reputation	**High** potential impact on the image and on the **national and international** reputation	**Moderate** potential impact on the image and on the **national and international** reputation (for example, relevance in the **national level press**)	**Low** potential impact on the image and on the reputation in Italy (for example, relevance in the **national level press**)	**Negligible** potential impact on the image and on the reputation
	Compliance	High potential **administrative sanctions and criminal penalties** for companies and individuals	High potential **administrative sanctions**	**Medium sized** potential administrative sanctions	**Small sized** potential administrative sanctions	**Negligible sized** potential administrative sanctions

Example

Example

$$R_I = L_I \times I_I$$

Inherent risk level



Risk Assessment
Identifying existing monitoring tasks

Controls and managerial actions can be evaluated according to the three layers described below:

Organization: in terms of roles and responsibilities, functional segregation of duties, powers of attorney and delegation of authority, expertise/skills, behaviors.

Processes: in terms of activities, controls and procedures (including directives, policies, guidelines and operating instructions).

Technology: in terms of Information Technology Systems, IT controls aimed at supporting business processes.

	Organization	Processes	Technology
Controls /Managerial actions totally adequate (0,80)*	• Organizational structure, roles and responsibilities **formally defined** and constantly updated • Staff with **appropriate skills** • Staff behavior **compliant** with laws and regulations	• Procedures that are **formalized, adequate** • Presence of documented control activities • Existence of a process of **continuous monitoring** • Presence of **adequate** information flows to support the decision-making	• Technology **properly implemented and maintained** • IT Controls **included and documented in the processe** • **Full** a… system capabilities to busines…
Controls /Managerial actions partially adequate (0,40)	• Organizational structure, roles and responsibilities **partially defined and updated** • … • ….	• Procedures on **consolidation /** formalization • Control activities **partially** documented • Existence of a monitoring process **at occurrence** • …	• Technology s… properly implemented, with p… **lways adequate** to the expectati… • … • **…**
Controls /Managerial actions to be adapted (0,05)	• Organizational structure, roles and responsibilities are **not defined** • …. • …	• **Not formalized** procedures • Control activities are **not documented** • **….** • ….	• Technology is not properly implemented, with inadequate performance **expectations** • … • **…**

Example

* The choice of the maximum value of 0,80 (and not 1) reflects the need to maintain the assessment consistent with the probabilistic concept of risk: as appropriate as the control can be, it never reduces the risk of 100%.

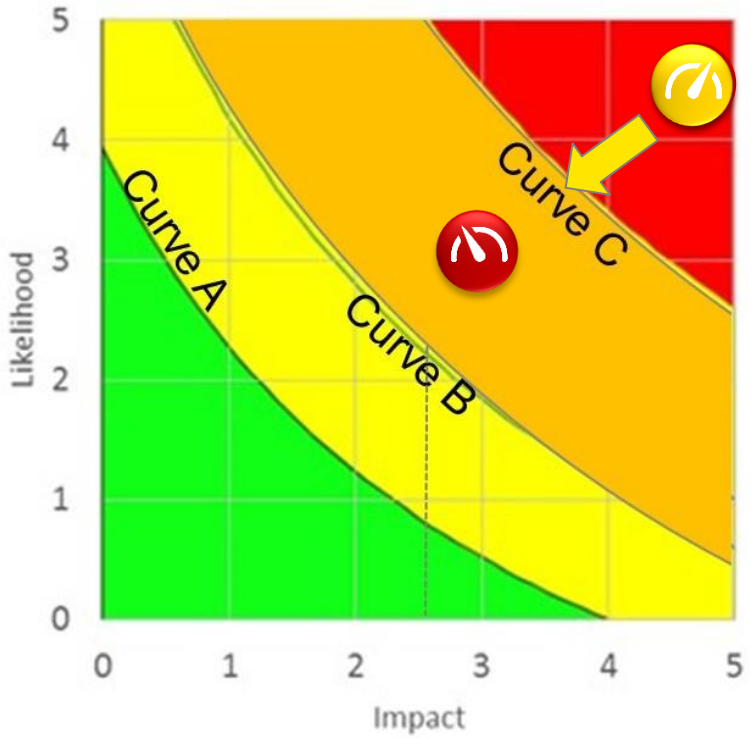
Risk Assessment
Residual risks

The assessment of Residual Risk is performed through a calculation algorithm that acquires as inputs the values of likelihood and Impact that characterize Inherent Risk and, based on the assessment of controls / mitigation actions in place, transforms in outputs the residual values of likelihood and impact through which calculating the Residual Risk:

$$R_R = L_{Residual} \times I_{Redisual}$$

The expected benefit from the implementation of all applicable controls / managerial actions results in a reduction of inherent impact (II) and/or inherent likelihood (LI) *(see annex 1):*

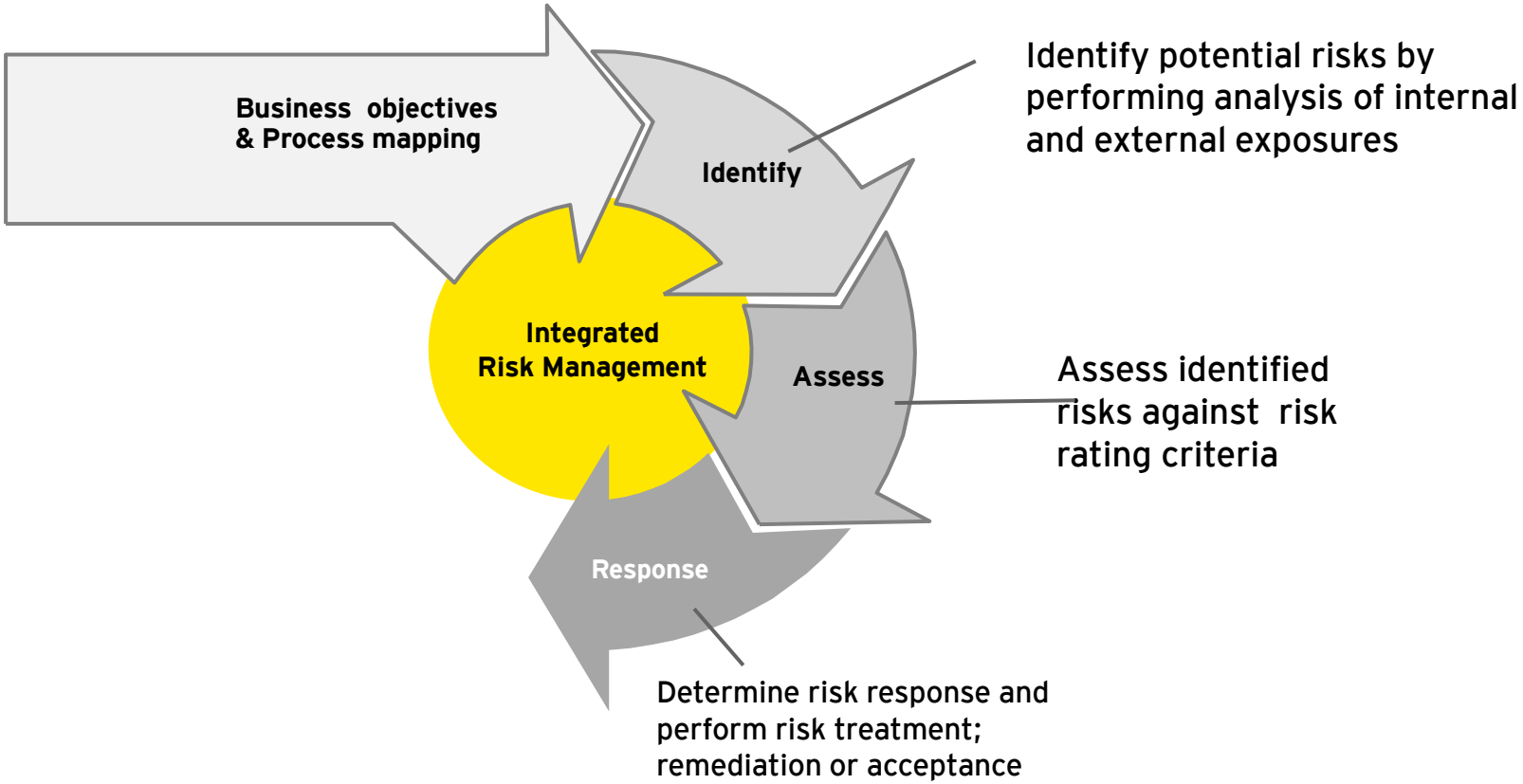
$$L_R = L_I - \Delta L$$
$$I_R = I_I - \Delta I$$



$$L_C = L_I - \Delta L = L_I - (L_I \times \alpha) = L_I \times (1 - \alpha)$$

Risk Management
ERM Model

Below the **Enterprise Risk Management cycle:**



Risk Response
Strategies

Once risks have been identified and assessed, all techniques to manage the risk fall into one or more of these four major categories

Accept 1

Accepting the risk means that while you have identified and analyzed it, you take no action. You simply accept that it might happen and decide to deal with it if it does.

Mitigate 2

Take mitigation actions that help reduce the likelihood of the occurrence or the severity of the impact.

Avoid 3

This includes not performing an activity that could carry risk. (e.g. by closing down a particular high-risk business area)
You can choose not to take on the risk by avoiding the actions that cause the risk.

Transfer 4

Transfer risks to an external agency (e.g. an insurance company)
Transference is a risk management strategy that isn't used very often and tends to be more common in projects where there are several parties. Essentially, you transfer the impact and management of the risk to someone else

Risk response is a cyclical process.
As circumstances are always changing, monitoring and review of the framework ensures continual improvement of the framework.

For Residual Risks higher than a threshold deemed acceptable, **further mitigation actions can be defined** in order to reach the desired level, **Target Risk**

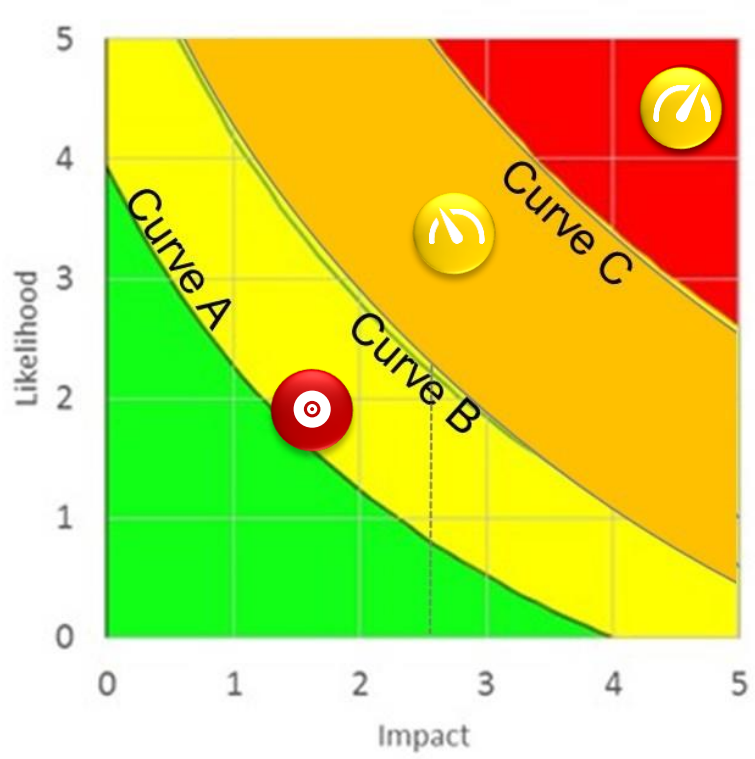
It is necessary to:

- **Define any further mitigation actions together with Risk Owner** and related timing of implementation
- **Assess** the adequacy of the set of controls (i.e. controls in place, to which adding the further mitigation actions).

Based on these considerations, the Target Risk is calculated as follows:

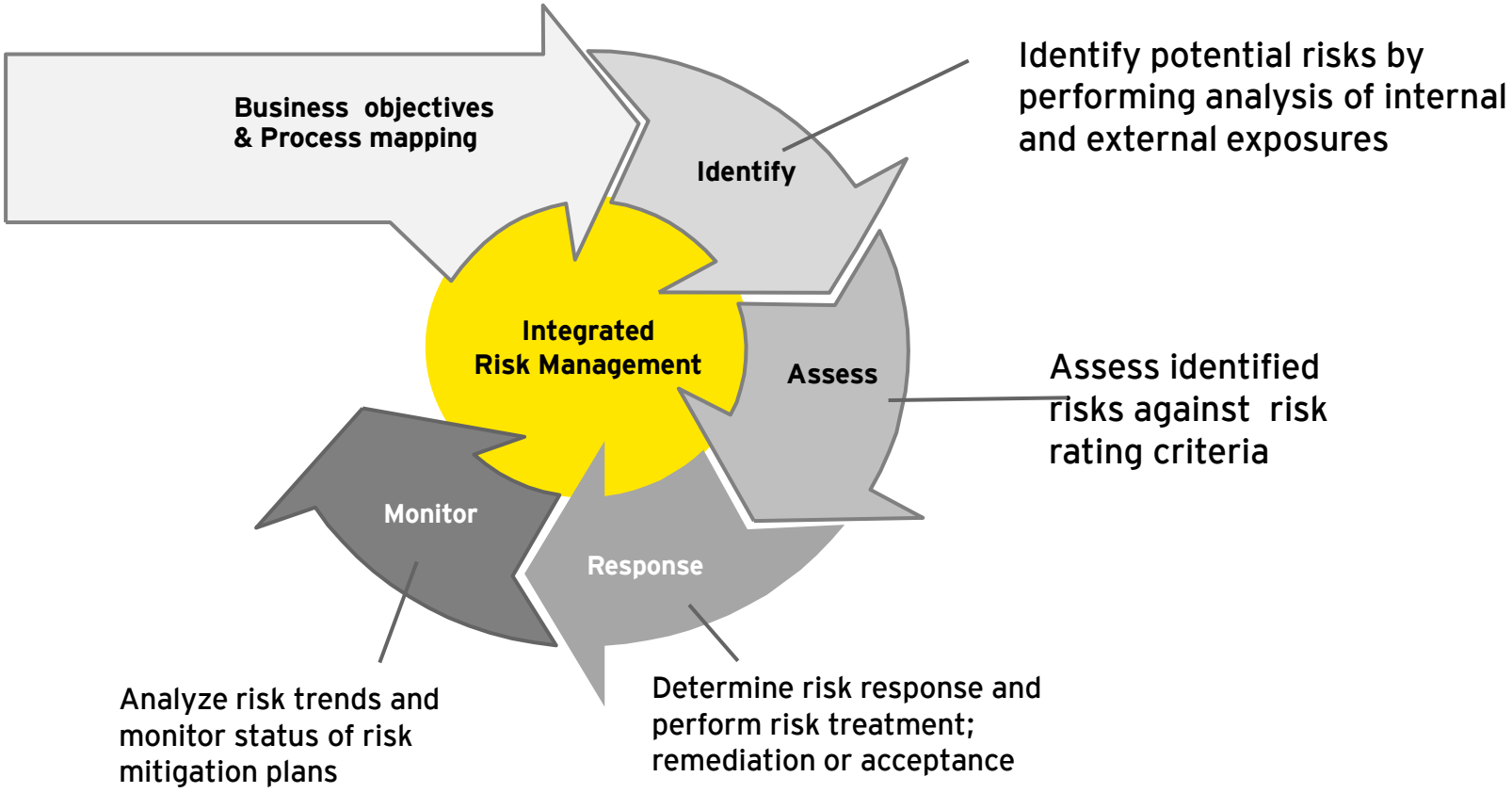
$$R_t = L_t \times I_t$$

in which L_t e I_P are calculated based on the same algorithm used for Residual Risk, applying the assessment of controls to Inherent Risk.



Risk Management
ERM Model

Below the **Enterprise Risk Management cycle:**



Risk Monitoring

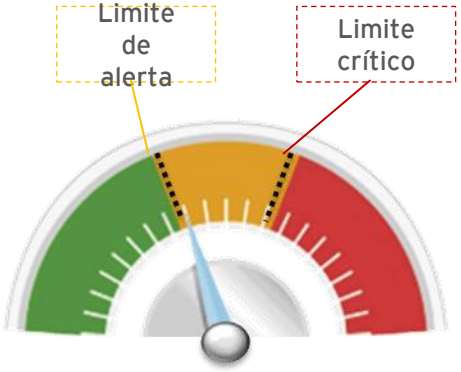
The monitoring process consists in keeping the evolution of risk under constant observation.
The KRIs monitoring allow to verify that the level of risk does not exceed the tolerance threshold, due to ineffective controls / action plans which would require intervention for their reinforcement.

The following monitoring activities should be performed for an effective KRI measurement:

1. Identification of the data set and calculation criteria;
2. Data elaboration / extraction;
3. Analysis of data;
4. Analysis of results and exceptions.

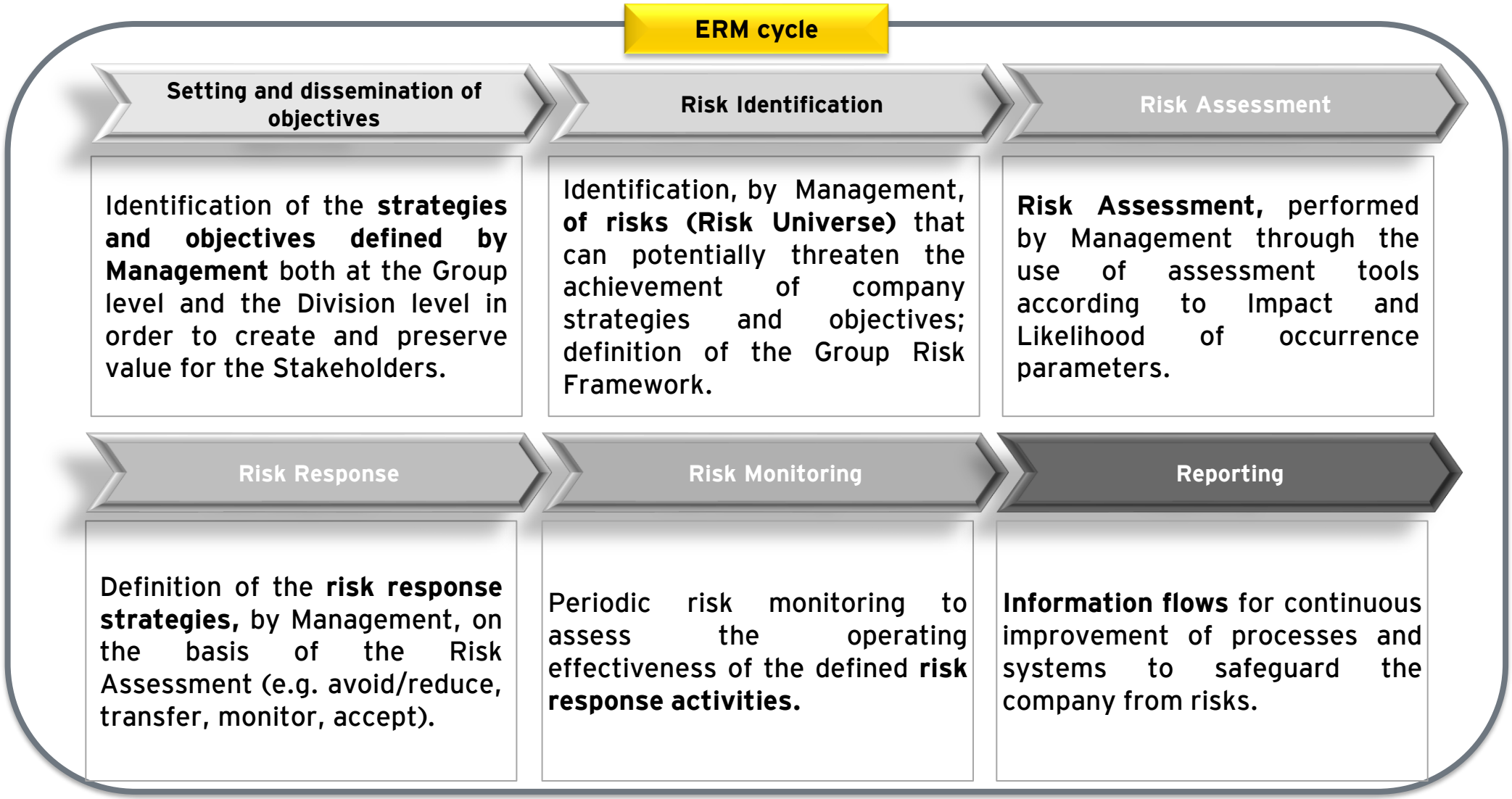
The KRI measurement should be compared to the following limits:

- "Critical" limit: the result of the indicator exceeds the established limit and should be considered particularly risky, based on the expectations and level of acceptability established;
- "Alert" threshold, above which the indicator should be carefully monitored because its level is higher than the one considered normal;
- Below the "alert" threshold, the value recorded is not considered significant, because is within the limit established.



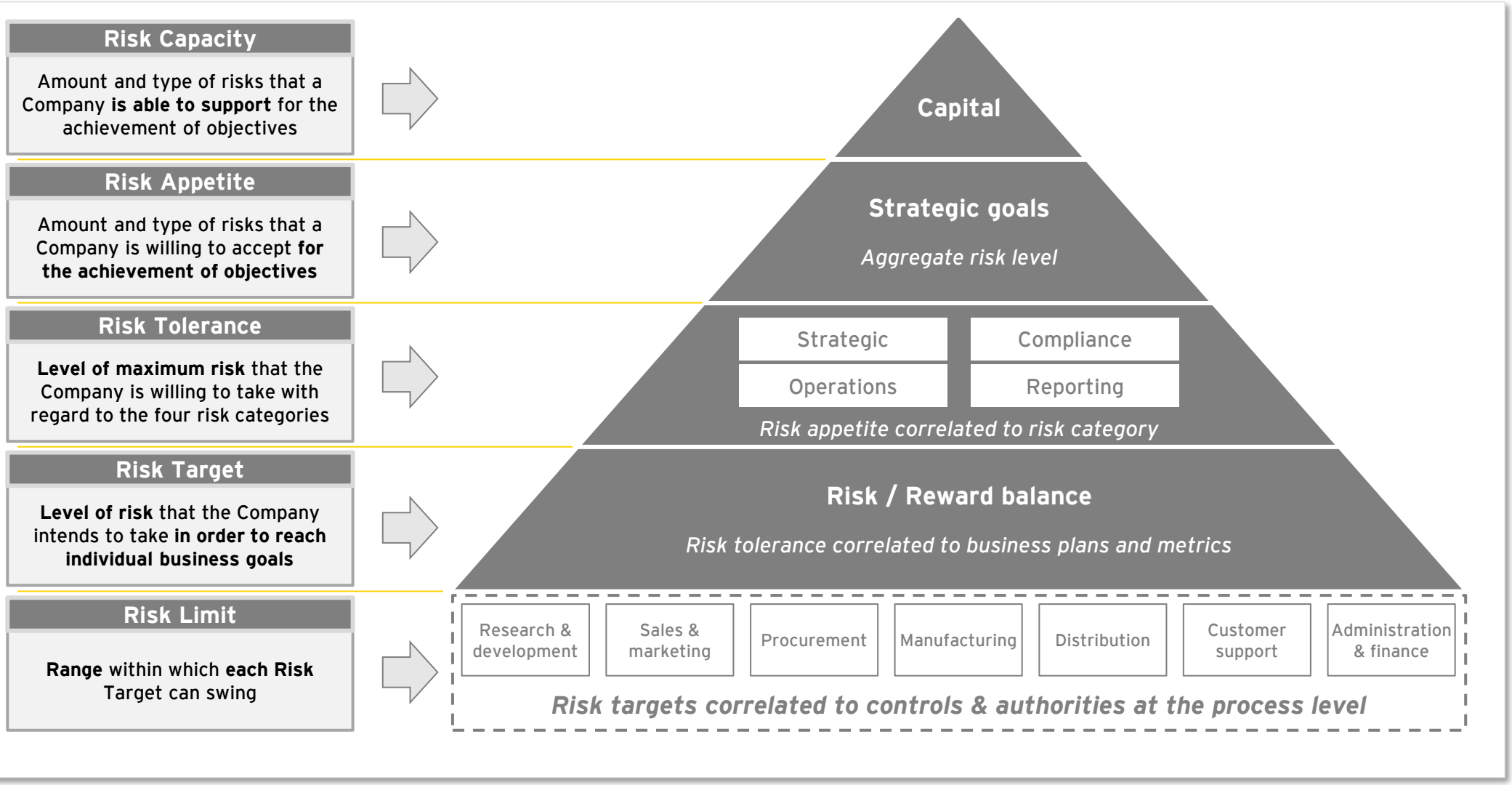
Any significant variation in relation to the value obtained from previous periods (historical analysis) should be analyzed. For example, if the indicator has improved, stabilized, or get worse compared to the current status.

Below is the **Risk Management cycle:**



Risk Management
Risk analysis and its impact - Risk levels

A good Risk Management System does not require the total elimination of risks, but a coherent and systematic management of them. At each stage of Company's life, it is necessary to know and evaluate the Risk Capacity, the Risk Appetite, the Risk Tolerance, the Risk Target and the Risk Limit.



"Risk comes from not knowing what you are doing"

Warren Buffett, economist

carlo.nicoletti@it.ey.com

Annexes

Annex 1
Residual Risk calculation

Following an example of the Residual Risk calculation algorithm that could be adopted:

$$R_R = L_R \times I_R$$

in which, the expected benefit from the implementation of all applicable controls / managerial actions results in a function of the reduction of inherent impact (ΔI) and/or inherent likelihood (ΔL)

$$L_R = L_I - \Delta L = L_I - (L_I \times \alpha) = L_I \times (1 - \alpha) \qquad I_R = I_I - \Delta I = I_I - (I_I \times \beta) = I_I \times (1 - \beta)$$

α and β are the coefficients of the adequacy of the set of controls and have a range of associable values between 0 e 0,80*.

$$\alpha = \left(\frac{A_{Organization} + A_{Processes} + A_{Technology}}{N_L}\right) \qquad \beta = \left(\frac{B_{Organization} + B_{Processes} + B_{Technology}}{N_I}\right)$$

Where:

- ***N*** = number of layers considered as **applicable for risk mitigation** (Organization, Processes, Technology), with effect in terms of likelihood reduction or with effect in terms impact reduction. *Nmax* = 3;
- ***A*** = assessment on the adequacy expressed by the evaluator for each class of controls for each layer, with effect in terms of likelihood reduction, considering them as **equivalent**;
- ***B*** = assessment of the adequacy expressed by the evaluator for each class of controls for each layer, with effect in terms impact reduction, considering them as **equivalent.**

Annex 2
Risk Assessment Methodologies

The following are, as an example, some techniques that can be used for risk assessment.

QUALITATIVE SCORING

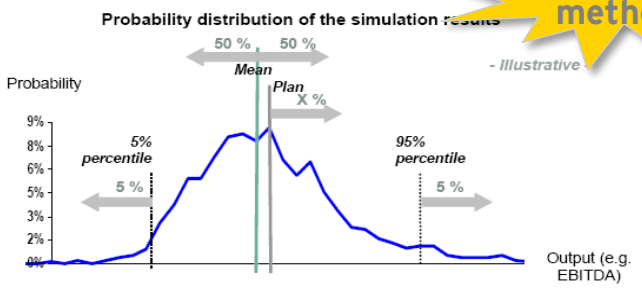
Qualitative methods

SCORE	RATING	FINANCIAL			OPERATIONS	COMPLIANCE			
		EBIT / EPS	Value	Disclosure	Scope	Legal/Regulatory	Repu…	…	…
5	Critical	> 25% EBIT / EPS	>25% Loss of Market Value	Fiscal Year Restatement	Enterprise-wide; Inability to continue normal business operations across all business units	Management Indictments Large Scale Class Actions Regulatory Sanctions	Lo… confidence in all stakeholder groups	… months)	…
4	Significant	> 20% EBIT / EPS	>20% Loss of Market Value	Fiscal Quarter Restatement	3 Business Units; Significant interruptions to business operations within 3 or more business units	Management Challenged Large Legal Liabilities Regulatory Fines	Loss of confidence by 3 or more stakeholder groups	Long Term Recovery (i.e., 12-24 months)	2 or more changes in senior leadership, financial restructuring, significant changes to strategic plan.
3	High	> 15% EBIT / EPS	>15% Loss of Market Value	Significant Deficiency	2 Business Unit(s); Moderate interruptions within 2 or more business unit(s).	Management Reviewed Legal Reserve Established Regulatory Investigation	Loss of confidence by 2 or more stakeholder groups	Mid-term Recovery (i.e., 6-12 months)	1 or more changes in senior leadership, significant changes to operating plans and execution.
2	Moderate	> 10% EBIT / EPS	>10% Loss of Market Value	Control Weakness	1 Business Unit; Interruptions restricted to 1 business unit.	Management Unaffected Minimal Liabilities Regulatory Attention	Loss of confidence limited to 1 stakeholder group	Short-term Recovery (i.e., less than 6 months)	Refinements or adjustments to operating plans and execution.
1	Low	> 5% EBIT / EPS	>5% Loss of Market Value	Additional Risk Disclosure	Limited interruptions within 1 business unit	Limited Liabilities or Regulatory Impact	Limited impact to 1 stakeholder group	Limited Recovery (i.e., less than 3 months)	Limited Adjustment Necessary

Qualitative application of risk assessment by assigning a severity score to impact and probability drivers, according to uniform and shared logics

OPERATIONAL VALUE@RISK (Net Risk evaluation)

Quantitative methods

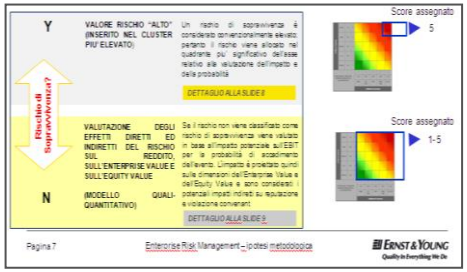


Application of the @Risk methodology for assessing the potential loss (through detection of time series or estimate of loss data). Methodology applicable to operational risk assessment

STOCK EXCHANGE MULTIPLES MODEL

Projection of impacts on EBIT - EV - EQV, with logic of stock exchange multiples (for listed companies)

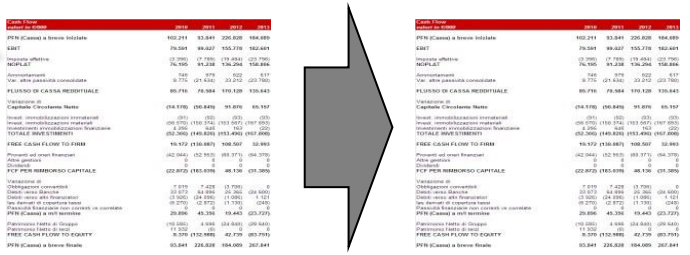
- CALCULATION OF EFFECTS ON EBIT
- PROJECTION ON ENTERPRISE VALUE (STOCK EXCHANGE MULTIPLES MODEL)
- EVALUATION AND CALCULATION OF EFFECTS ON NFP
- ESTIMATE OF INDIRECT IMPACT OF EQUITY VALUE RISK RESULTING FROM:
  - REPUTATIONAL DAMAGES
  - EFFECTS RESULTING FROM COVENANT VIOLATION



Mixed methods

CASH FLOW SCENARIOS MODEL

Analysis of the impact on cash flow ("worst scenario" approach)

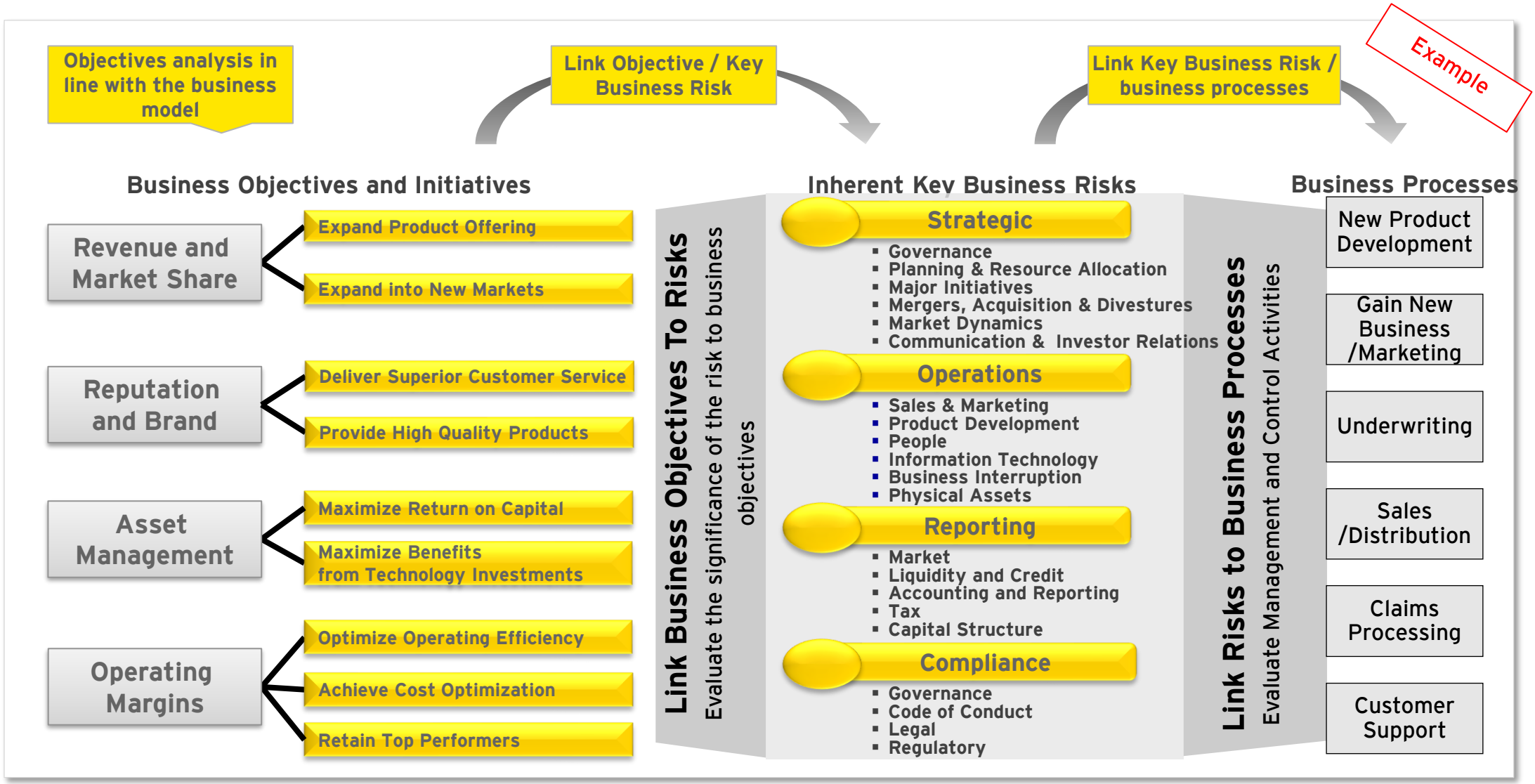


VA = C1 (1+i 1)
+
C2 (1+i 2)
+
C3 (1+i 3)
+
…

The projection of the impact on Net Profit, NFP and on the expected flows allows you to update the Expected Value of cash flows (e.g. Time horizon assumed Industrial Plan)

Annex 3
Business objectives and initiatives

The **Risk Identification Process** is closely related to the analysis of Company's **business targets.**




EY
Building a better
working world

Inherent Risk is

- Potential event that will adversely affect organization
- The risk after management takes action to reduce the impact or likelihood
- Risk when management has not taken action to reduce the impact or likelihood
- Potential event with low impact and likelihood

Which ISO standard is related to Risk management - Principles and guidelines?

- 14000 Environmental Management Systems
- 31000 Risk management -- Principles and guidelines
- 22301 Business Continuity Management
- None of above

Who is responsible for managing risks within a company?

- Risk Management function
- IT Security department
- Internal Audit
- Risk owner

Employee errors, or Systems failures. These are example of

- Compliance risks
- Financial risks
- Operational risks
- Preventive controls

What is the major challange in implementing ERM?

- Identifying executive sponsors of ERM
- Establishing a common risk glossary
- Implementing risk-ranking metholodogy
- All of above

The risk remaining after risk treatment, is called

- Inherent risk
- Risk monitored
- Residual risk
- Risk Assessment

Examples of Risk Response Strategies are

- Mitigate, Monitor, Control
- Mitigate, Transfer, Avoid, Accept
- Assess, Manage, Identify
- All of above

This is taking steps to eliminate risk

- Transferring
- Avoidance
- Reducing
- Assuming

Risks related to aspects of health and safety in the workplace, are example of

- Compliance risk
- Operational Risk
- Strategic Risk
- None of above

This is not an Effective Enterprise Risk Management

- Improve resource deployment
- Enhance enterprise resilience
- Identify and manage risk entity-wide
- Focus on Compliance Risks

Amount and type of risk that an organisation is willing to take in order to meet their OBJs

- Risk Tolerance
- Risk Appetite
- Risk Capacity
- Risk Response

A activity's role in risk management process can be

- no role
- Auditing the risk management process as part of the IA plan
- Managing and Coordinating risk management process; Monitoring Activities
- All of above

Which of the following is a factor affecting Risk?

- New personnel
- New Information System
- Rapid Growth
- all are correct

Which of the following are most directly designed to ensure that risks are contained?

- Risk Management process
- Control processes