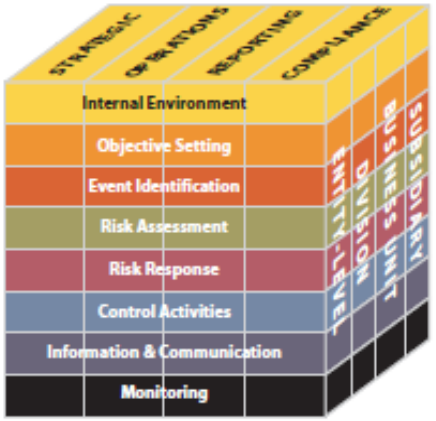
RISK FRAMEWORKS

COSO

Committee of Sponsoring Organizations of the Treadway Commission

2004



Risk examples

failure to manage ESG (environmental, social and governance)-related risks

Table 0.3: Examples of risk events and their consequences

Year	Company	Event	Business Impact
2018	Wells Fargo	The Federal Reserve found that Wells Fargo workers responded to the high pressure sales culture by creating as many as 3.5 million fake accounts. The bank also forced up to 570,000 customers into unneeded auto insurance.[5]	The punishment included a requirement to remove four board members and imposed a cap on the growth of the company until sufficient improvements are put in place[6]
2017	Uber	Multiple reported incidents pointed to a pervasive culture of alleged sexual harassment[7]	Reputational damage
2016	Samarco (Vale and BHP)	A dam collapse killed 19 people and sent iron ore mining debris through the southeast region of Brazil[8]	USD $6.2 billion settlement[9]
2016	7-Eleven	Company workers were being paid less than the legal minimum wage[10]	At least USD $26 million in back pay to 680 workers[11]
2015	Volkswagen	Millions of cars were recalled worldwide after the company admitted to falsifying emissions tests[12]	USD $14.7 billion settlement[13]
2015	3M	NGO ForestEthics alleged that 3M suppliers provided products from endangered forests around the world[14]	Led 3M to revise its policy on pulp and paper sourcing to improve environmental and social practices in more than 70 countries with 5,000 suppliers[15]
2014	General Motors (GM)	A faulty ignition switch that caused airbags to fail in a crash prompted the recall of 1.6 million vehicles[16]	USD $35 million civil penalty after the National Highway Traffic Safety Administration determined GM delayed reporting the ignition switch defect[17]
2013	More than 25 brands including Primark, Benetton and Walmart	More than 1,100 workers were killed and 1,000 were injured in Bangladesh's Rana Plaza factory collapse[18]	USD $15 million of USD $40 million target raised by the International Labor Organization, a UN agency, to compensate impacted families[19]
2011	Automotive industry	Flooding in Thailand resulted in over 500 deaths and significant disruptions to supply chain networks, particularly in the automotive and technology industry sectors	The impact has been felt at the regional level, with the Thai central bank reducing its gross domestic product growth forecast for 2011 from 4.1% to 1.5%, and the Thai baht depreciating by about 3.9% in three months[20]
2010	BP	Oil spill in the Gulf of Mexico	BP paid USD $5.5 billion in Clean Water Act penalty and up to USD $8.8 billion in natural resource damages[21]
2000s	Mattel	Mattel experienced a number of product recalls, in 2007 recalled toys due to lead paint contamination	Recalled 967,000 toys[22]
1990s	Nike	Company paid its factory workers, including children, less than minimum wage and forced them to work overtime[23]	Reputational damage and loss of sales from protests at the Barcelona Olympics in 1992 and multiple exposés of labor practices[24]
1980s	Nestle	Infant Formula Action Coalition launched a boycott of Nestle for its marketing and sale of baby formula in emerging countries[25]	The boycott caught on in France, Finland, Norway, Ireland, Australia, Mexico, Sweden and the UK[26]
1970s	Ford	After the company learned its Pinto model was prone to fires, 1.9 million Pintos were recalled[27]	Initially one claimant was awarded USD $125 million in damages, which was later reduced to USD $3.5 million[28]

Risk examples

Risk Management cover the crucial processes that focuses on the survival, sustainability and objectives achieving of the company, anticipating risks and implementing the correct mitigation actions.

But how these processes and knowledge can be structured in a formal way inside the company?

COSO risk management framework

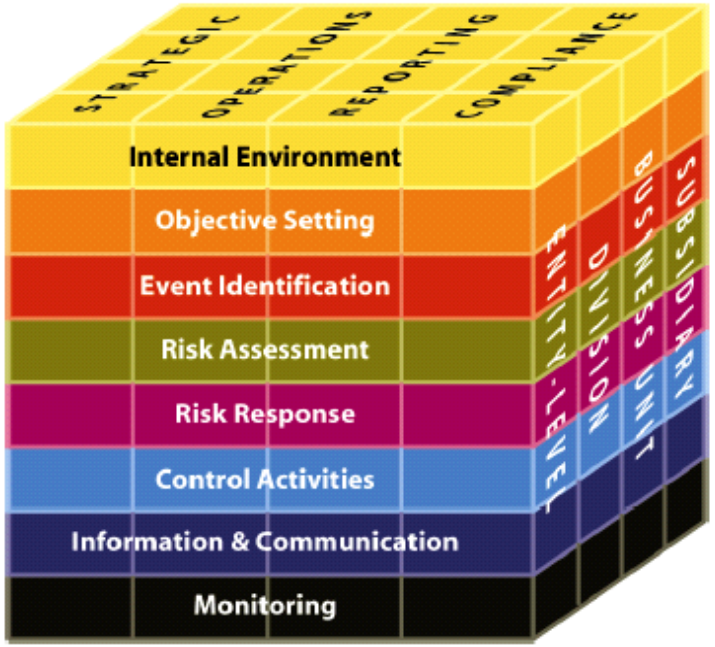
Until the very recent present, many enterprises or governmental agencies have not had a consistent **definition of the meaning of risk management** and what was necessary to establish an effective **risk management structure or framework.**

To help with this definition problem, the **Committee of Sponsoring Organizations of the Treadway Commission** (**COSO**) entity developed a risk management definition or framework definition called **COSO Enterprise Risk Management or COSO ERM** (1985). https://www.coso.org/Pages/default.aspx

This risk management framework, updated with COSO guidance and published in 2011, provides a structure and set of definitions to allow enterprises of all types and sizes to understand and better manage their risk environments.

COSO - What Is Enterprise Risk Management ?

According to COSO,1 Enterprise Risk Management (ERM) is "A process, effected by an entity's board of directors, management, and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, manage risk to be within its risk appetite, and to provide reasonable assurance regarding the achievement of entity objectives."



This enterprise risk management framework is geared to achieving an entity's objectives, set forth in four categories:

- *Strategic* – high-level goals, aligned with and supporting its mission
- *Operations* – effective and efficient use of its resources
- *Reporting* – reliability of reporting
- *Compliance* – compliance with applicable laws and regulations.

COSO risk management framework

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) is an accounting organization with a special focus in enterprise risk management (ERM).

They define Enterprise Risk Management (**ERM**) as **a process** designed to **identify potential events** that may **affect the organization and manage risk** to be within that organization's **risk appetite** in order to provide reasonable **assurance of accomplishing** the organization's **objectives**.

Risk identification and **mitigation** are a key component of an organization's ERM program.

COSO risk management framework

Figure 0.2: Principles according to COSO's ERM Framework[35]

GOVERNANCE & CULTURE

1. Exercises Board Risk Oversight
2. Establishes Operating Structures
3. Defines Desired Culture
4. Demonstrates Commitment to Core Values
5. Attracts, Develops and Retains Capable Individuals

STRATEGY & OBJECTIVE-SETTING

6. Analyzes Business Context
7. Defines Risk Appetite
8. Evaluates Alternative Strategies
9. Formulates Business Objectives

PERFORMANCE

10. Identifies Risk
11. Assesses Severity of Risk
12. Prioritizes Risks
13. Implements Risk Responses
14. Develops Portfolio View

REVIEW & REVISION

15. Assesses Substantial Change
16. Reviews Risk and Performance
17. Pursues Improvement in Enterprise Risk Management

INFORMATION, COMMUNICATION, & REPORTING

18. Leverages Information and Technology
19. Communicates Risk Information
20. Reports on Risk, Culture and Performance

COSO risk management framework

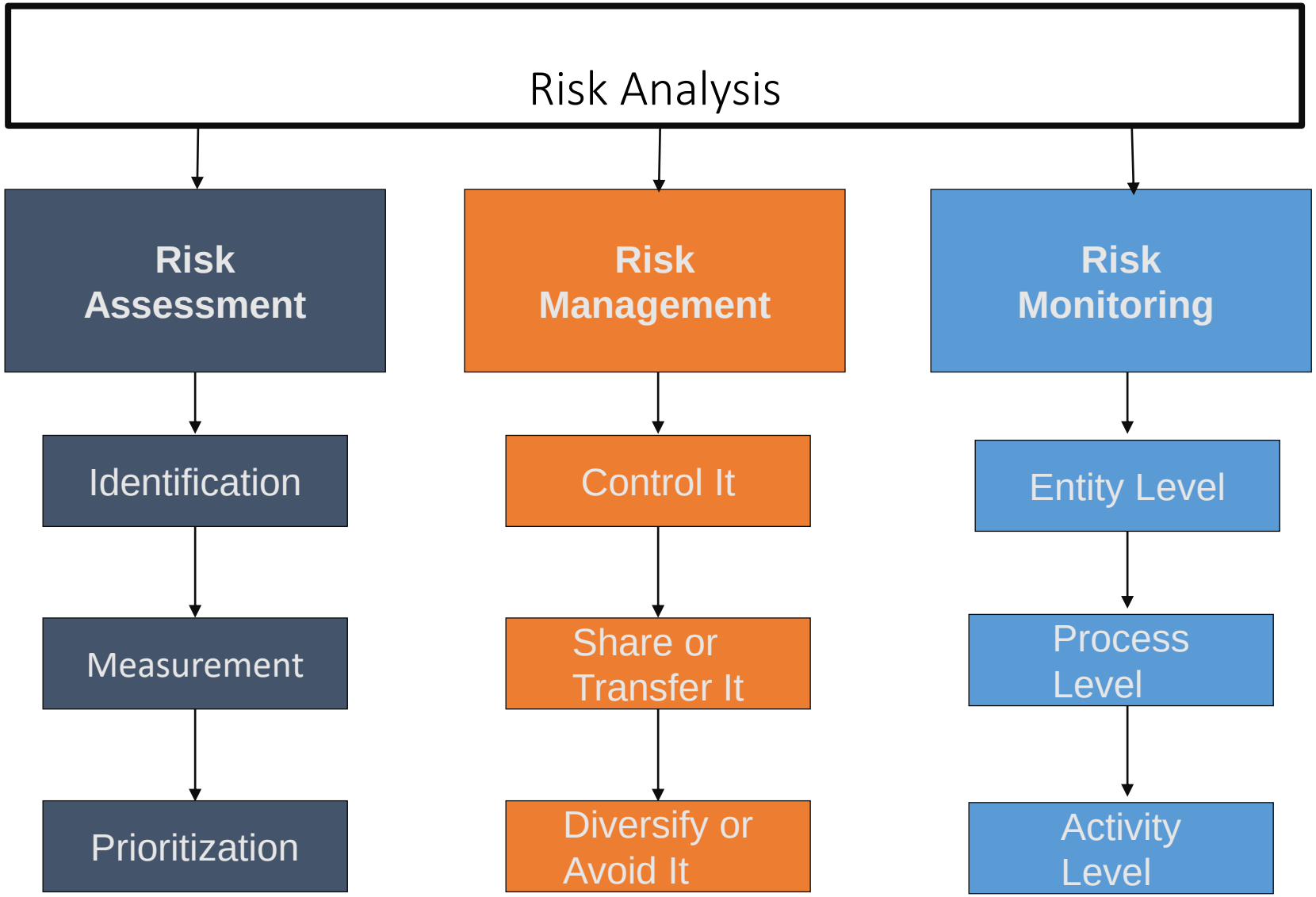
The **COSO** risk assessment process puts the responsibility on management to go through the steps **to assess whether a risk is significant** and then, if so, to take appropriate actions.

This **risk-assessment** process should be performed **at all levels and for virtually all activities within the enterprise**. The **COSO internal controls** framework describes risk assessment as a **main three-step process**:

1. Estimate the **significance of the risk**.
2. Assess the **likelihood or frequency** of the risk occurring.
3. Consider **how the risk should be managed** and assess what actions (e.g. mitigations) must be taken.

COSO Enterprise Risk Management, Robert Moeller, Wiley

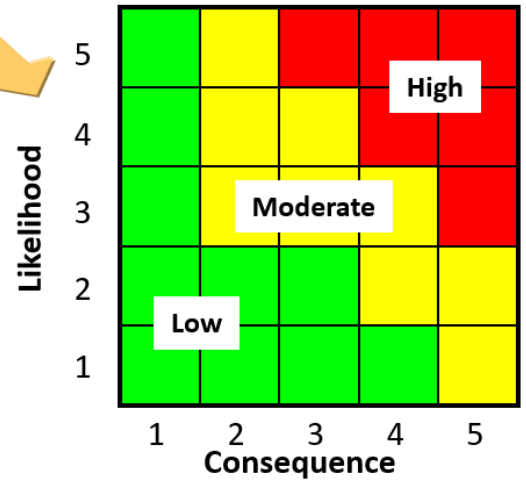
COSO risk management framework



COSO risk management framework

Example Risk Analysis Criteria

What is the likelihood the risk will occur?		
Level		**Current Plan, Approach and Processes...**
5	Near Certainty:	...Cannot avoid this type of risk; no known processes or workarounds are available
4	Highly Likely:	...Cannot avoid this risk, but a different approach might
3	Likely:	...May avoid this risk, but workarounds will be required
2	Low Likelihood:	...Have usually avoided this type of risk with minimal oversight in similar cases
1	Not Likely:	...Will effectively avoid this risk based on standard practices



Given the risk is realized, what would be the magnitude of the impact?					
Type \ Level	**1**	**2**	**3**	**4**	**5**
Technical	Minimal or no impact	Minor perf. shortfall, same approach retained	Moderate perf. shortfall, but workarounds available	Unacceptable, but workarounds available	Unacceptable; no alternatives exist
Schedule	Minimal or no impact	Additional activities required; able to meet key dates	Minor schedule slip; will miss need date	Program critical path affected	Cannot achieve key program milestone
Cost	Minimal or no impact	Budget increase or unit production cost increase <1%	Budget increase or unit production cost increase <5%	Budget increase or unit production cost increase <10%	Budget increase or unit production cost increase >10%

Consequence

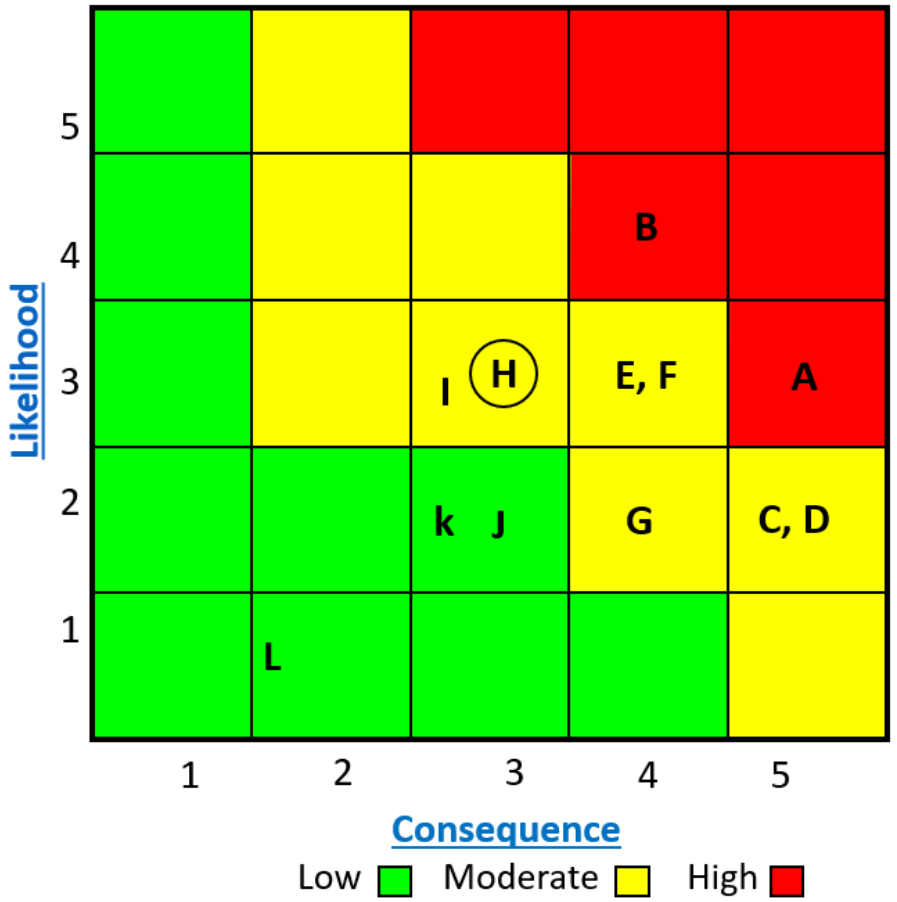
COSO risk management framework

Example

A	Environmental Issues	★
B	Health and Safety	★
C	FCPA	☆
D	Compliance Risk Management	☆
E	Training	☆
F	SOX	☆

G	Audit of Subcontractors	☆
H	Lobbying	☆
I	Import	☆
J	Staffing	☆

K	Labor Charging	☆
L	IT Security	☆



FCPA: *Foreign Corrupt Practices Act*

SOX: Sarbanes–Oxley Act

COSO risk management framework

Risk Management report example

Risk Management Report

1 Page: 1 of

Risk #: H

Title: Lobbying

Resp. Team: Legal & Contracts

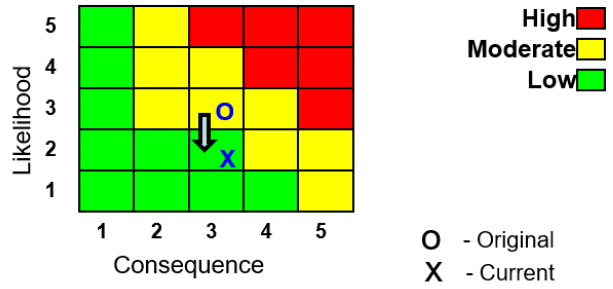
Owner: Jack Frost

Phone: 570.443.8425

Description:

Risk of a violation of U.S. lobbying laws/regulations.

Last Updated : 8/6/2016 Reviewed



Likelihood Rationale:

All lobbying is coordinated through the Corporate office. Only a few employees conduct any lobbying and it's at a very low level. Affected employees are aware of the procedure to report lobbying activity. Procurement and Accounts Payable suite of controls – see contract compliance risks / controls

Consequence Rationale:

A violation of law could subject the company to fines and cause harm to business or reputation. Lobbying cost not allowable on Government contracts

Visibility Level

- ☐ Entity
- ☒ Business
- ☒ Functional

Phase/Issue

- ☐ Candidate
- ☐ Open
- ☒ Closed

Risk Handling Strategy & Summary Rationale:

- ☐ Assume
- ☐ Transfer
- ☒ Mitigate
- ☐ Avoid

lobbying activity is reported to Corporate on a quarterly basis. Management communicates on a regular basis with the Corporate Lobbying Team and is on the Lobbying distribution e-mail list. Lobbying costs distributed through unique corporate accounts

Risk Category

- ☒ Cost
- ☐ Schedule
- ☐ Technical
- ☒ Contract

Handling Plan and Plan Status: G

Currently executing to plan.

COSO risk management framework

- **COSO internal controls** focus on an enterprise's daily activities,
- **COSO enterprise risk management** (ERM) focuses on activities that an enterprise and its managers may or may not do.

A manager is interested, for example, in the **controls** necessary to accumulate accounting transactions, to summarize them in a well-controlled manner, and to publish them as the financial results of the enterprise.

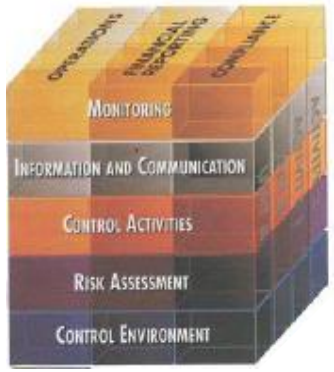
However, that same manager may be concerned about such **enterprise risks** as the financial impacts on the enterprise due to the launch of a new product, the reaction and actions of competitors, and overall market conditions for that new product launch. All of these do not involve the here and now of an internal controls framework but involve enterprise risk.

COSO Enterprise Risk Management, Robert Moeller, Wiley

COSO risk management framework

COSO Evolution

Internal Control - Integrated Framework



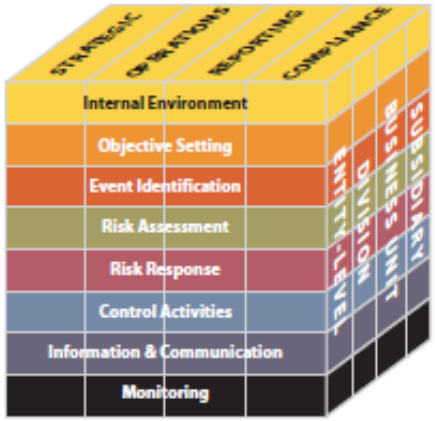
Internal Control - Integrated Framework (updated)

Draft 2017 ERM

1992 **2013** **2016**

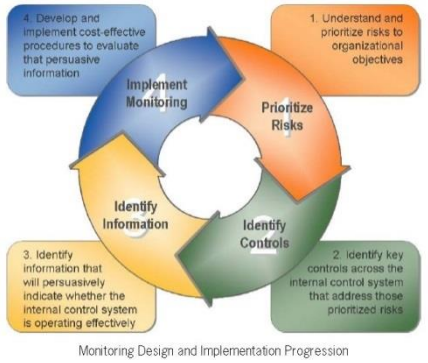
2004

Enterprise Risk Management (ERM) - Integrated Framework



2009

Guidance on Monitoring Internal Control Systems



Monitoring Design and Implementation Progression

COSO Enterprise Risk Management, Robert Moeller, Wiley

COSO risk management framework

Compliance standards first became particularly important at the beginning of this century with the corporate accounting fraud–related failure of the high-flying corporation **Enron** (*).

This led to the passage of the **Sarbanes-Oxley Act (SOx)** in the United States and a worldwide interest in enterprise **governance and compliance issues**.

These concerns became even more significant with the **worldwide financial recession** starting around 2008 (banks giving credit to customers had no serious rules).

Because of these incredible **compliance and governance failures**, frequently, **Risk management is included in a broader level** which includes **Governance, Risk, and Compliance** (**GRC**) issues!

COSO Enterprise Risk Management, Robert Moeller, Wiley

COSO risk management framework

Governance can be defined as: “The system by which entities are directed and controlled. It is concerned with structure and processes for decision making, accountability, control and behavior at the top of an entity.

Compliance is the act of complying with a command, desire, wish, order, or rule. It can also mean adhering to requirements, standards, or regulations. Both of these compliance definitions are important for your organization.

Governance, risk, and compliance – popularly known as **GRC** – is a set of processes and procedures to help organizations achieve business objectives, address uncertainty, and act with integrity. The basic purpose of GRC is to instill good business practices into everyday life.

COSO Enterprise Risk Management, Robert Moeller, Wiley

COSO risk management framework

Governance, Risk, and Compliance (**GRC**) is a relatively new corporate management system that integrates these three crucial functions into the processes of every department within an organization.

GRC is in part a response to the "silo mentality," as it has become disparagingly known. That is, each department within a company can become reluctant to share information or resources with any other department.

This is seen as reducing efficiency, damaging morale, and preventing the development of a positive company culture.

The overall purpose of GRC is to reduce risks and costs as well as duplication of effort. It is a strategy that requires company-wide cooperation to achieve results that meet internal guidelines and processes established for each of the three key functions.

COSO Enterprise Risk Management, Robert Moeller, Wiley

Enron bankruptcy

(*): **Enron** engaged in mark to market (MTM) accounting, with official US Securities and Exchange Commission (SEC) approval in 1992. This accounting method, based on the "fair value" of the company's assets, which may change as market conditions change was used by Enron to **overinflate the company's estimated profits and mislead investors**.

To **hide its mounting debt**, Enron used **special purpose vehicles** (SPVs: shell companies capitalized entirely by Enron stock) to borrow money on Enron's behalf

Enron's stock price reached a high of **US$90.75** per share in mid-2000. **After it was revealed that the company had been engaging in accounting fraud** - had, in fact, been **hiding billions of dollars in debt** via various accounting loopholes - **the company's shareholders filed a $40 billion lawsuit**. The **Arthur Andersen company** was found **guilty of crimes** in the firm's **auditing** of Enron and was **closed**.

Enron's stock price **drop to $1 per share** by the end of November 2001. On December 2, 2001, **Enron filed for bankruptcy**. Enron's was the **largest bankruptcy in US history**.
http://large.stanford.edu/courses/2018/ph240/smith1/

Sarbanes-Oxley Act (SOx)

Inserir matriz Galp

Since becoming a U.S. law in 2002, the Sarbanes-Oxley Act (SOx) has had a major impact on corporations whose securities are registered with the U.S. Securities and Exchange Commission (SEC). SOx has changed the financial reporting and public accounting regulatory landscape from one of self-regulation by external audit firms to quasi-governmental rules and has become a **worldwide standard**.

SOx now requires senior business executives **to assume personal responsibility for the documentation**, **review, and testing of their enterprise's internal controls**.

Although the act requires enterprises to follow the **COSO internal control rules**, COSO enterprise risk management (ERM) was released after SOx and was not specifically mentioned in that legislation

COSO Enterprise Risk Management, Robert Moeller, Wiley

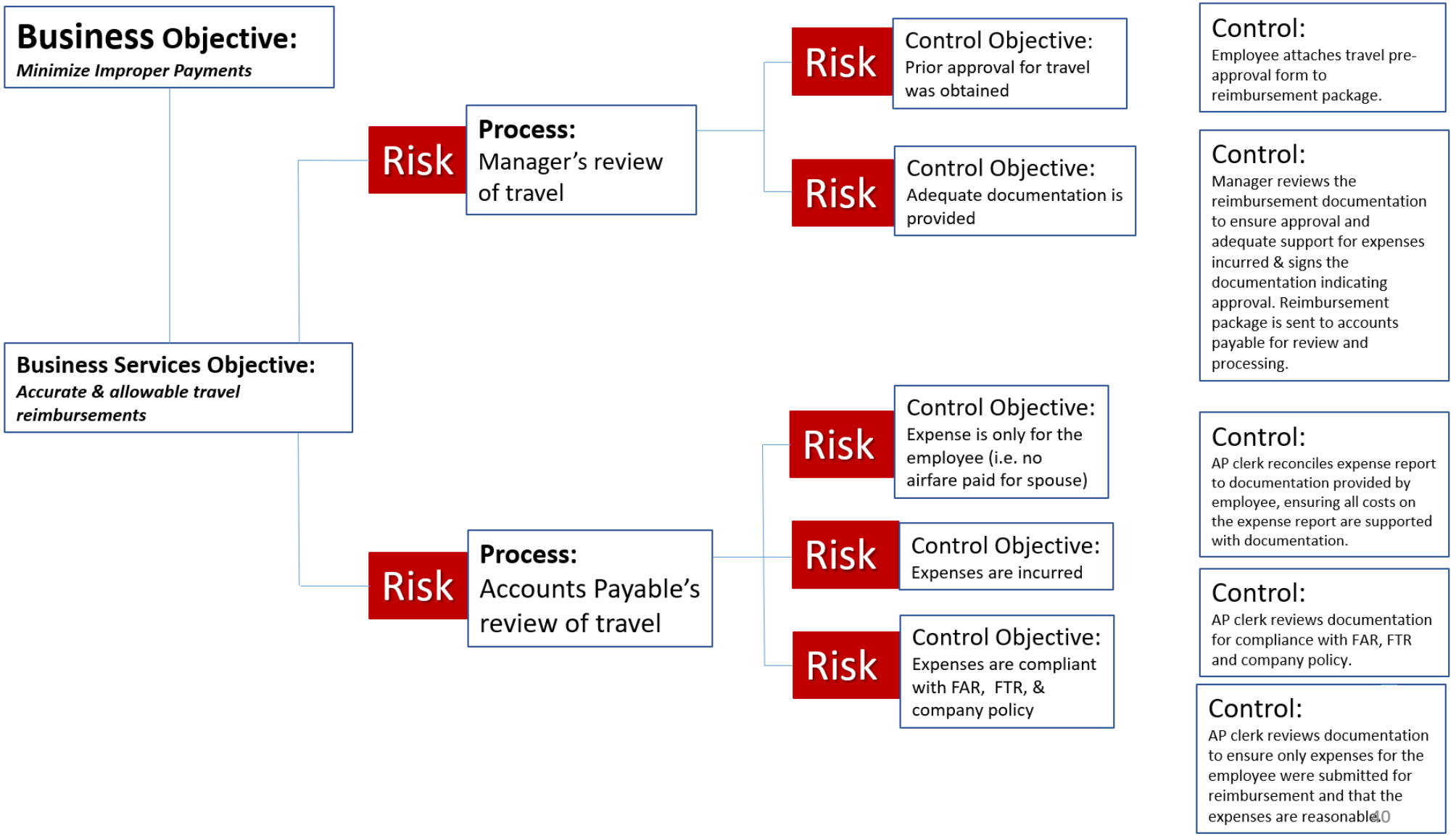
COSO internal control procedures

Many control activities under COSO **internal controls** are fairly easy to identify and test due to the accounting nature of many internal controls. They generally include the following internal control areas:

- **Separation of Duties**. Essentially, the person that initiates a transaction should not be the same person that authorizes that transaction.
- **Audit Trails**. Processes should be organized such that final results can be easily traced back to the transactions that created those results.
- **Security and Integrity**. Control processes should have appropriate control procedures such that only authorized persons can review or modify them.
- **Documentation**. Processes should be appropriately documented.

COSO Enterprise Risk Management, Robert Moeller, Wiley

COSO internal control procedures



COSO GRC

Enterprise Governance (the **G** of the GRC acronym) is an important theme to ensure the accountability of certain individuals in an enterprise through mechanisms that try to reduce or eliminate the conflicts that will exist between their overall goals and individual stakeholders' self-interest.

Enterprise Risk management (the **R** of the GRC acronym) is a process designed to identify potential events that may affect the organization, and manage risk to be within that organization's risk appetite in order to provide reasonable assurance of accomplishing the organization's objectives

Compliance (the **C** of the GRC acronym) is either a state of being in accordance with some established guidelines, specifications, or legislation, such as the Sarbanes-Oxley Act (SOx) or the process of becoming so.

COSO Enterprise Risk Management, Robert Moeller, Wiley

COSO GRC

Business professionals did not even hear about the now increasingly familiar **acronym GRC** until a few years after SOx.

Governance means taking care of business, making sure that things are done according to an enterprise's standards, regulations, and board of directors' decisions.

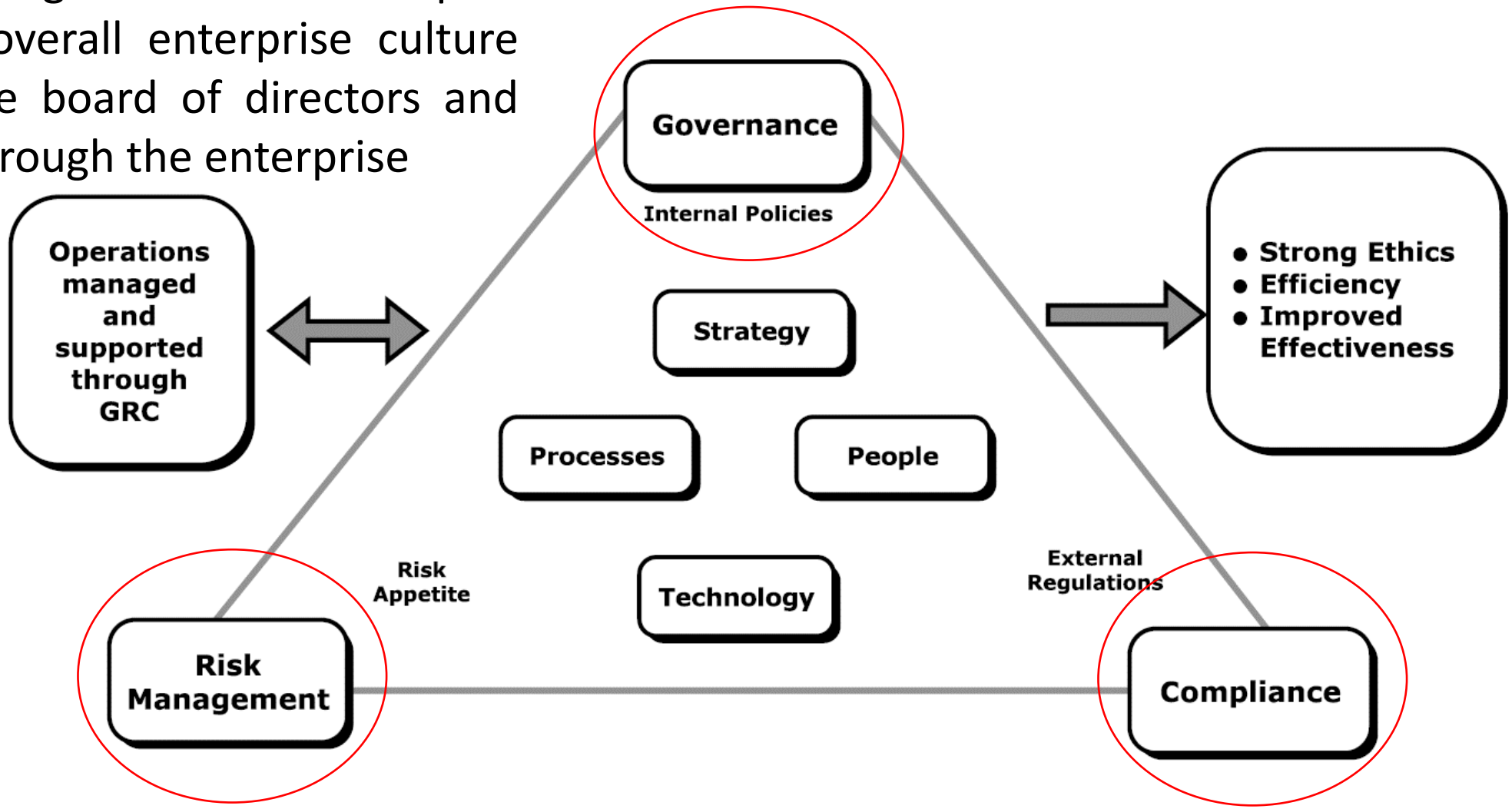
Risk becomes a way to help both protect existing asset value and create value by strategically expanding an enterprise or adding new products and services.

Compliance means follow the many laws and rules affecting businesses and citizens today. C can also include controls, meaning that it is important to put certain controls in place to ensure that compliance is happening.

COSO Enterprise Risk Management, Robert Moeller, Wiley

COSO GRC Governance Concepts

Risk management should be part of the overall enterprise culture from the board of directors and down through the enterprise



COSO Enterprise Risk Management, Robert Moeller, Wiley

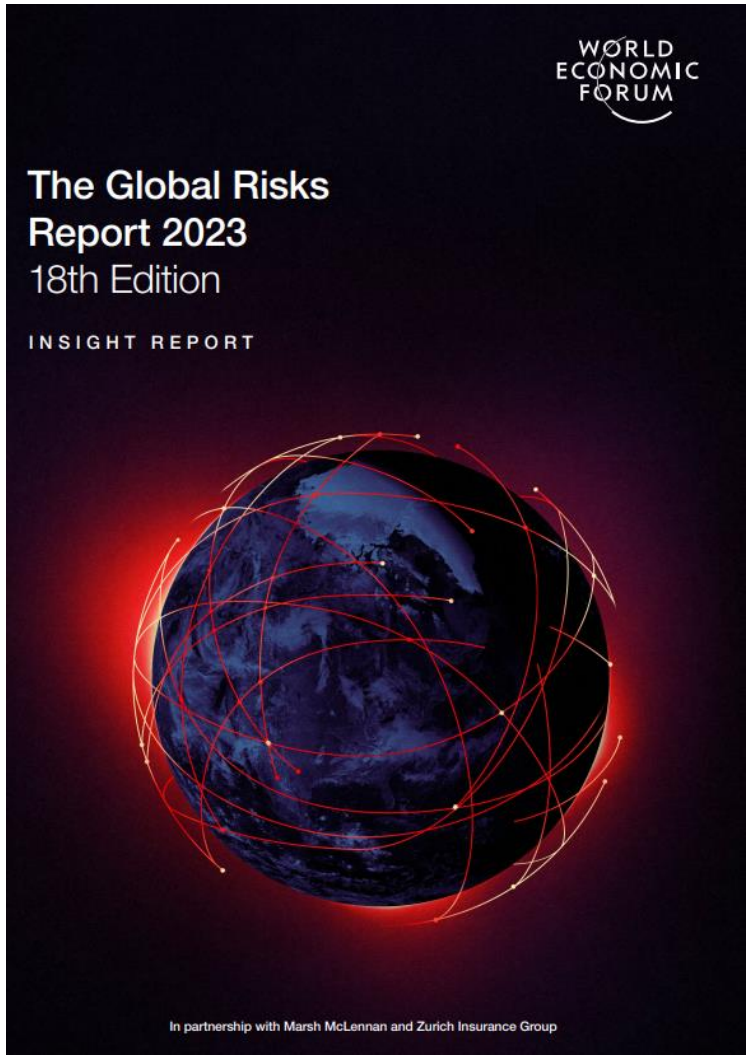
COSO GRC Governance Concepts

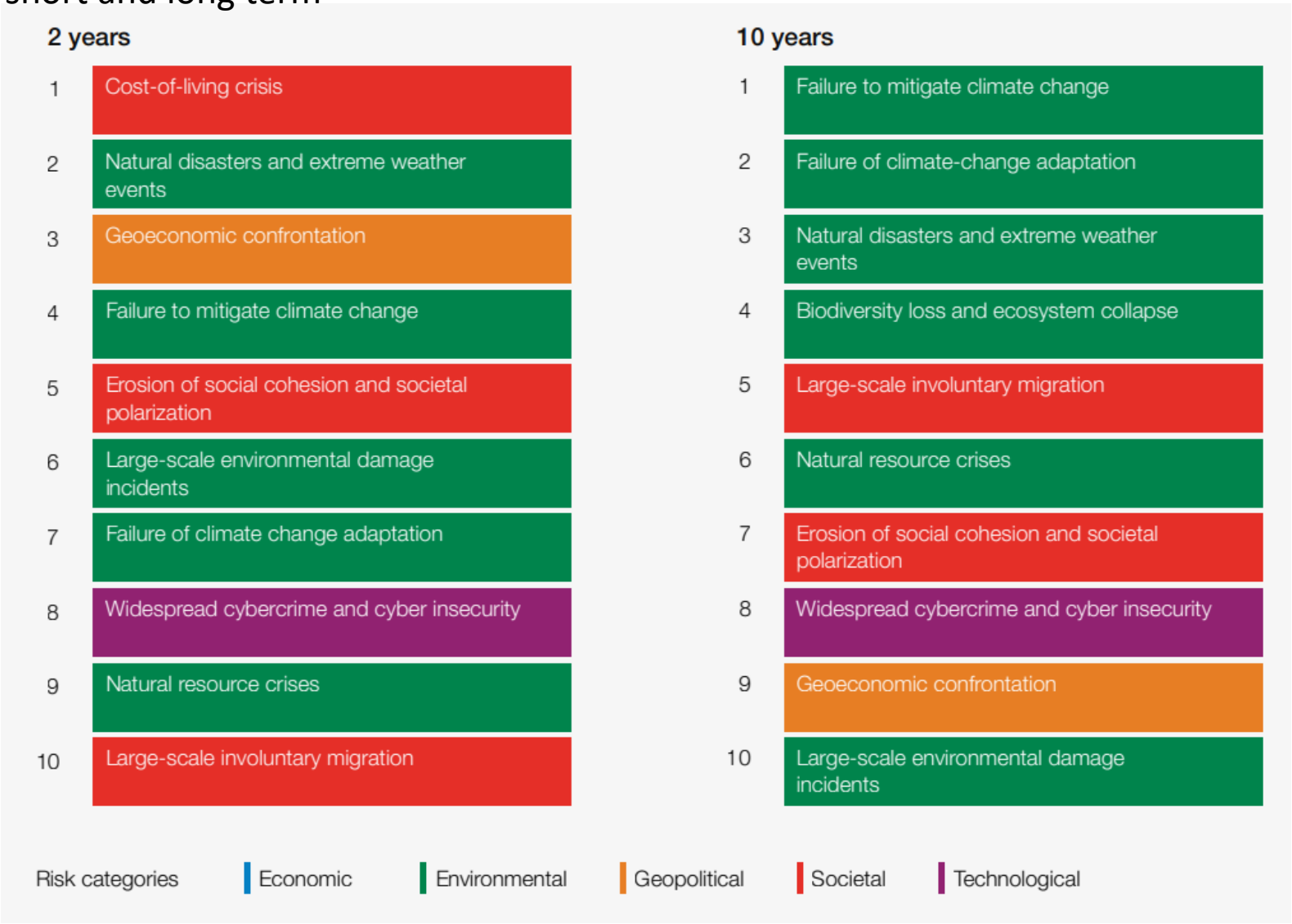
Next figure shows enterprise governance concepts with an executive group in the center and their interlocking and related responsibilities for establishing controls, a strategic framework, performance, and accountability

COSO Enterprise Risk Management, Robert Moeller, Wiley

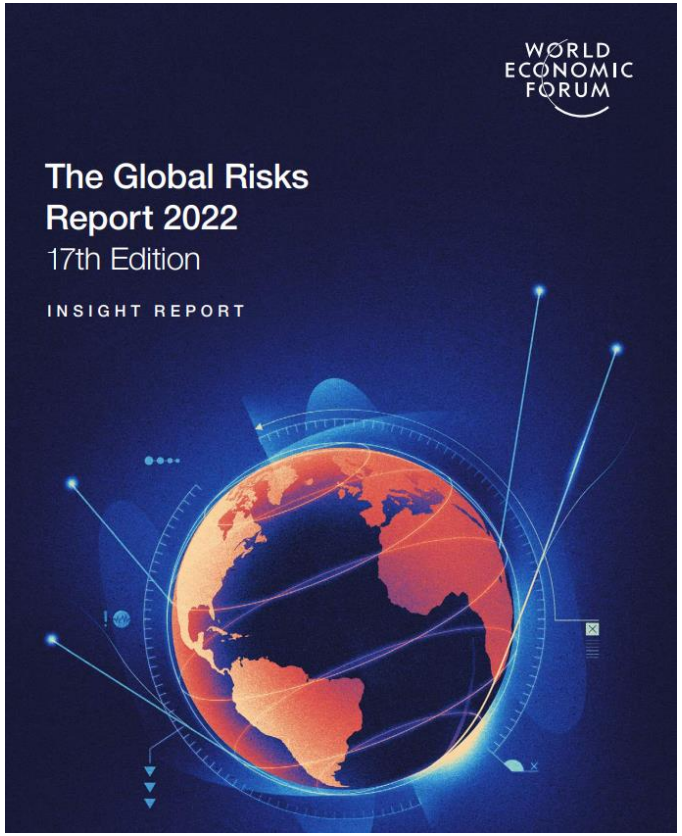
COSO GRC Governance Concepts

Global risks ranked by severity over the short and long term





2022 report



"Identify the most severe risks on a global scale over the next 10 years"

Economic | Environmental | Geopolitical | Societal | Technological

1st	Climate action failure	6th	Infectious diseases
2nd	Extreme weather	7th	Human environmental damage
3rd	Biodiversity loss	8th	Natural resource crises
4th	Social cohesion erosion	9th	Debt crises
5th	Livelihood crises	10th	Geoeconomic confrontation

Source: World Economic Forum Global Risks Perception Survey 2021-2022

COSO Enterprise Risk Management, Robert Moeller, Wiley

COSO GRC Risk Management Processes

These COSO GRC steps are common with other risk frameworks.

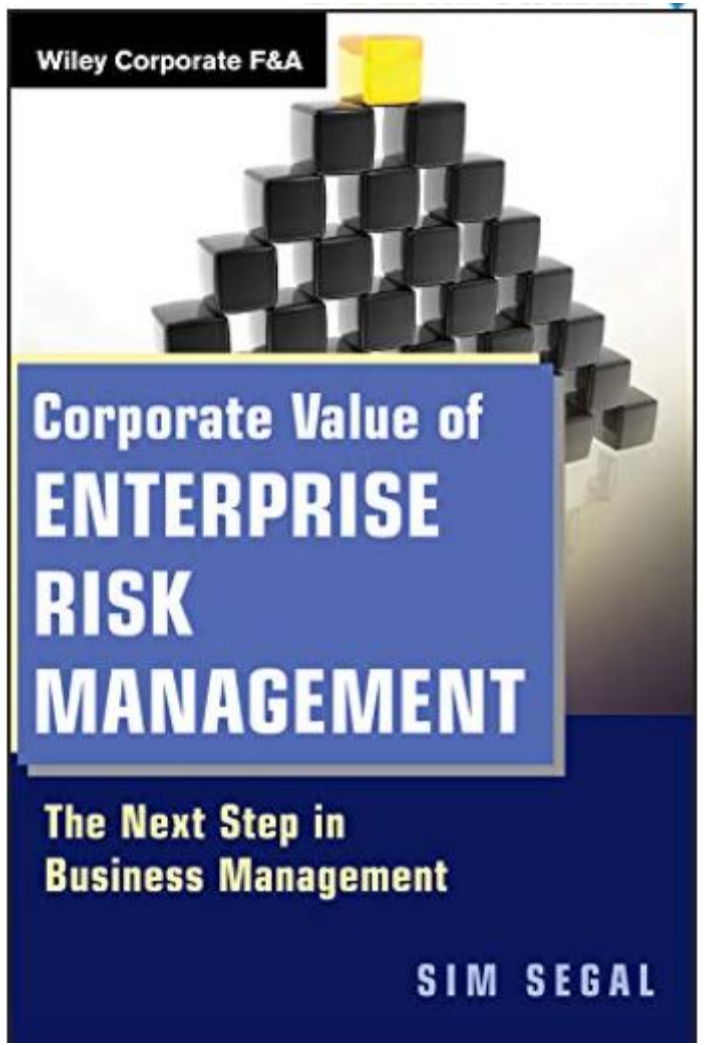
COSO Enterprise Risk Management, Robert Moeller, Wiley

COSO GRC Risk Management Processes

How much are you wiling to pay, as a percentage of your company profits to assure that your company is much more prepared to beat risks, survive them and achieve the objectives with a higher probability?

Your answer defines your understating and value of the risk management and your risk appetite.

Most of the times, managers do not understand well the value of the risk management and inherently the likelihood of the company incurring in dangerous situations is much higher.



COSO Enterprise Risk Management, Robert Moeller, Wiley

COSO GRC Risk Management Processes

Risk management should create **value** and be an integral part of organizational processes.

It should be part of **decision-making processes** and be tailored in a systematic and structured manner to explicitly **address the uncertainties an enterprise faces** based on the best available information.

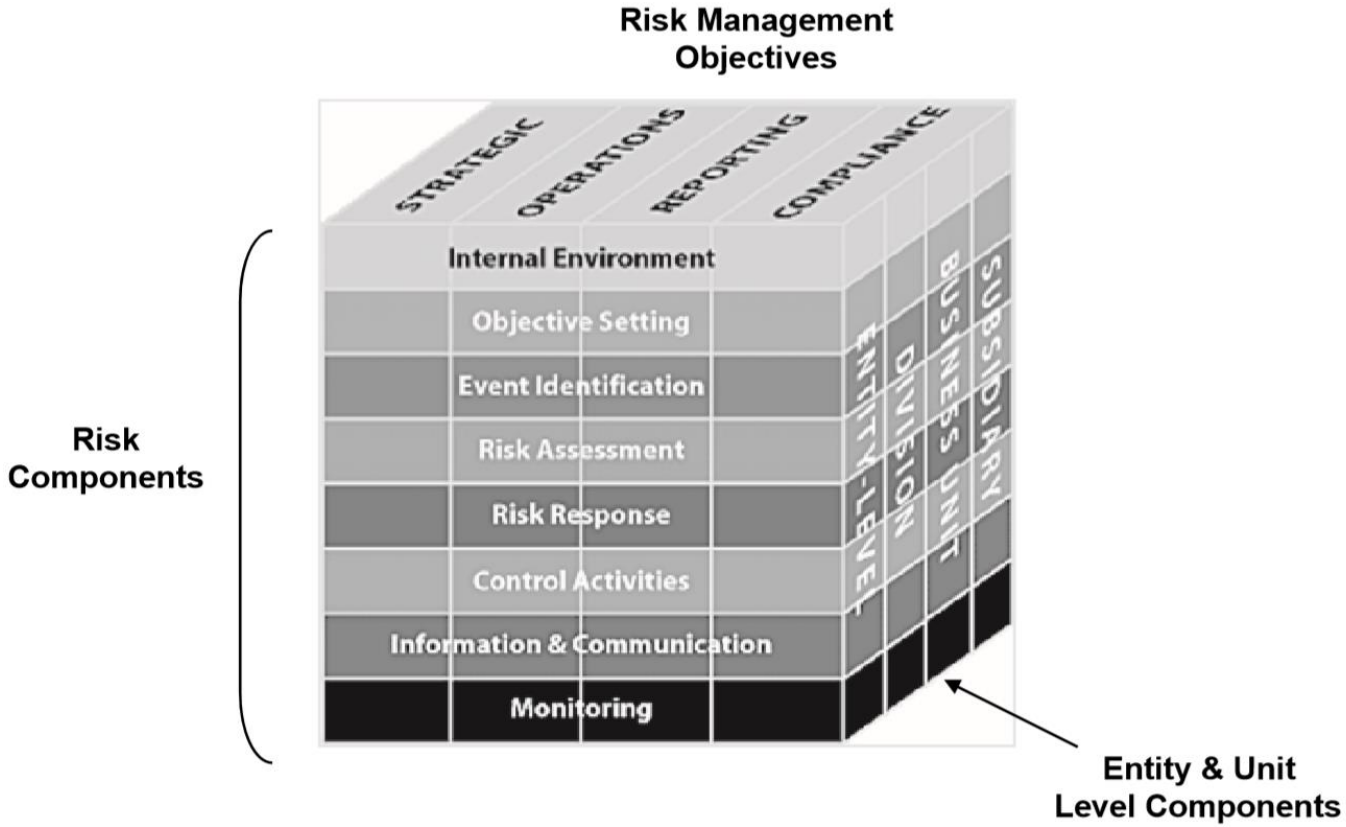
In addition, risk management processes should be dynamic, iterative, being **integrated at all levels in the company** and responsive to change with the capabilities of **continual improvements** and enhancements.

COSO Enterprise Risk Management, Robert Moeller, Wiley

COSO ERM framework cube

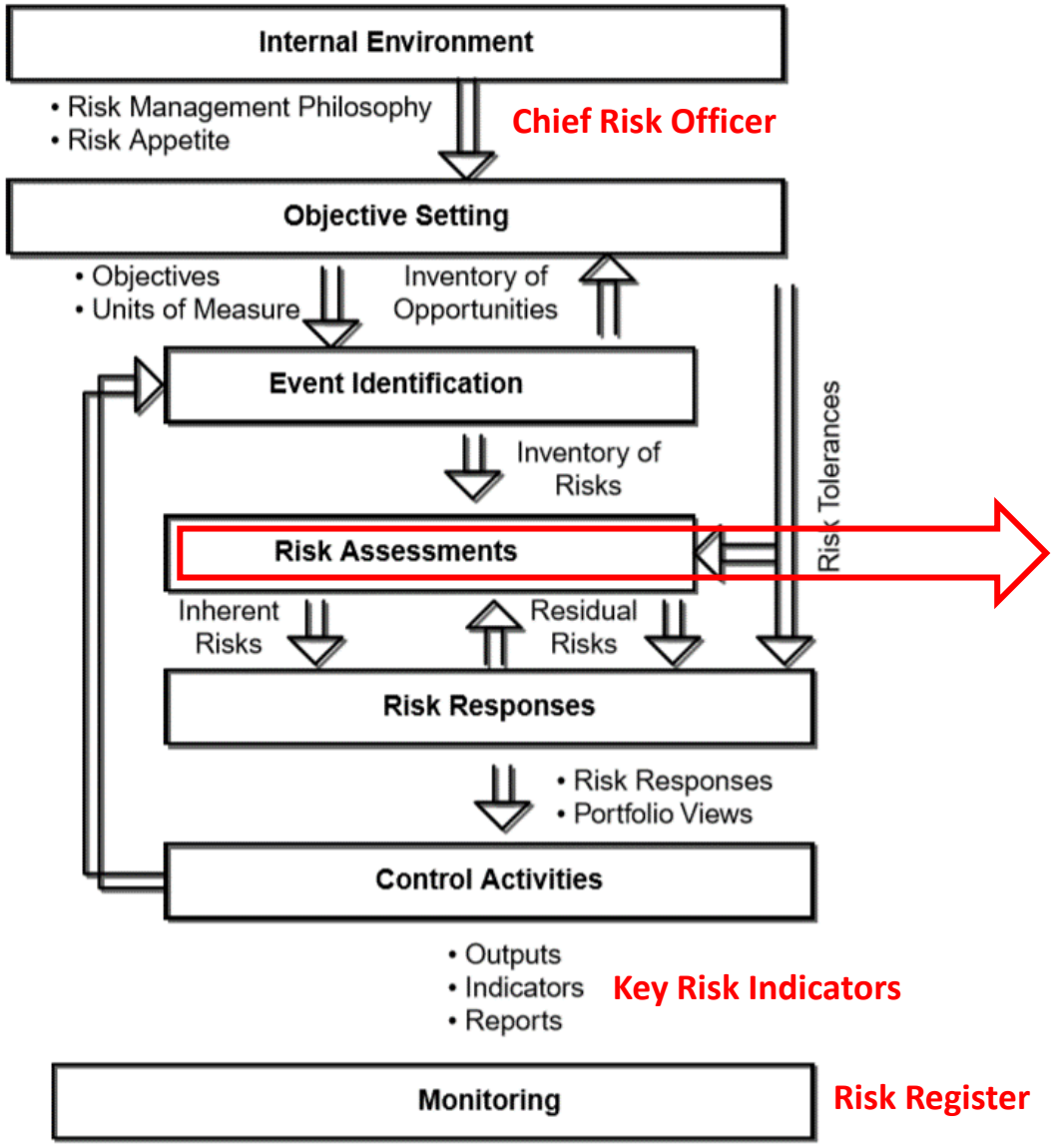
The COSO ERM framework is also a **three-dimensional cube** with the components of:

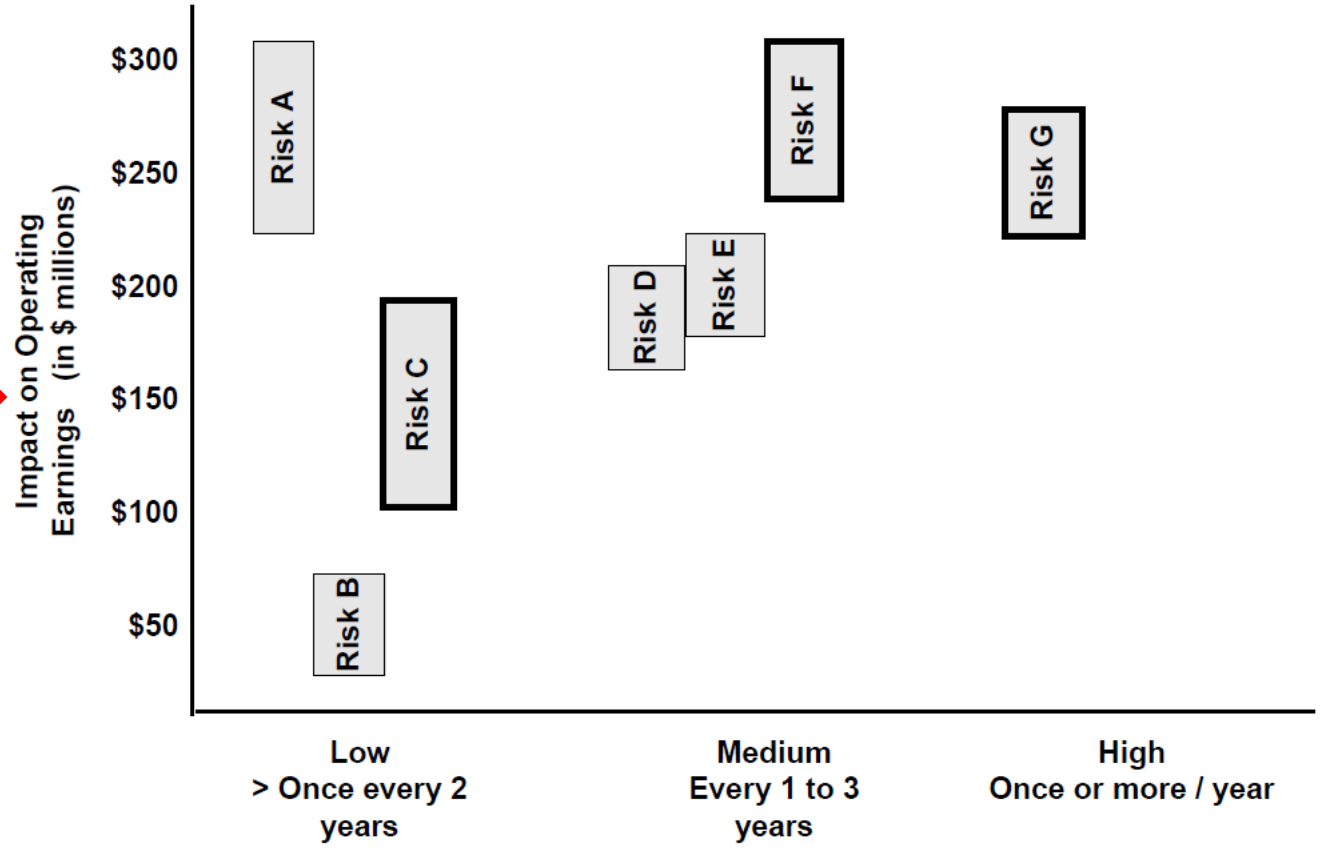
- Four vertical columns that represent the strategic **objectives** of enterprise risk.
- Eight horizontal rows or risk **components**.
- Multiple levels of the enterprise, from a ‘‘headquarters’’ **entity** level to individual subsidiaries



COSO Enterprise Risk Management, Robert Moeller, Wiley

COSO ERM Risk Components





COSO Enterprise Risk Management, Robert Moeller, Wiley

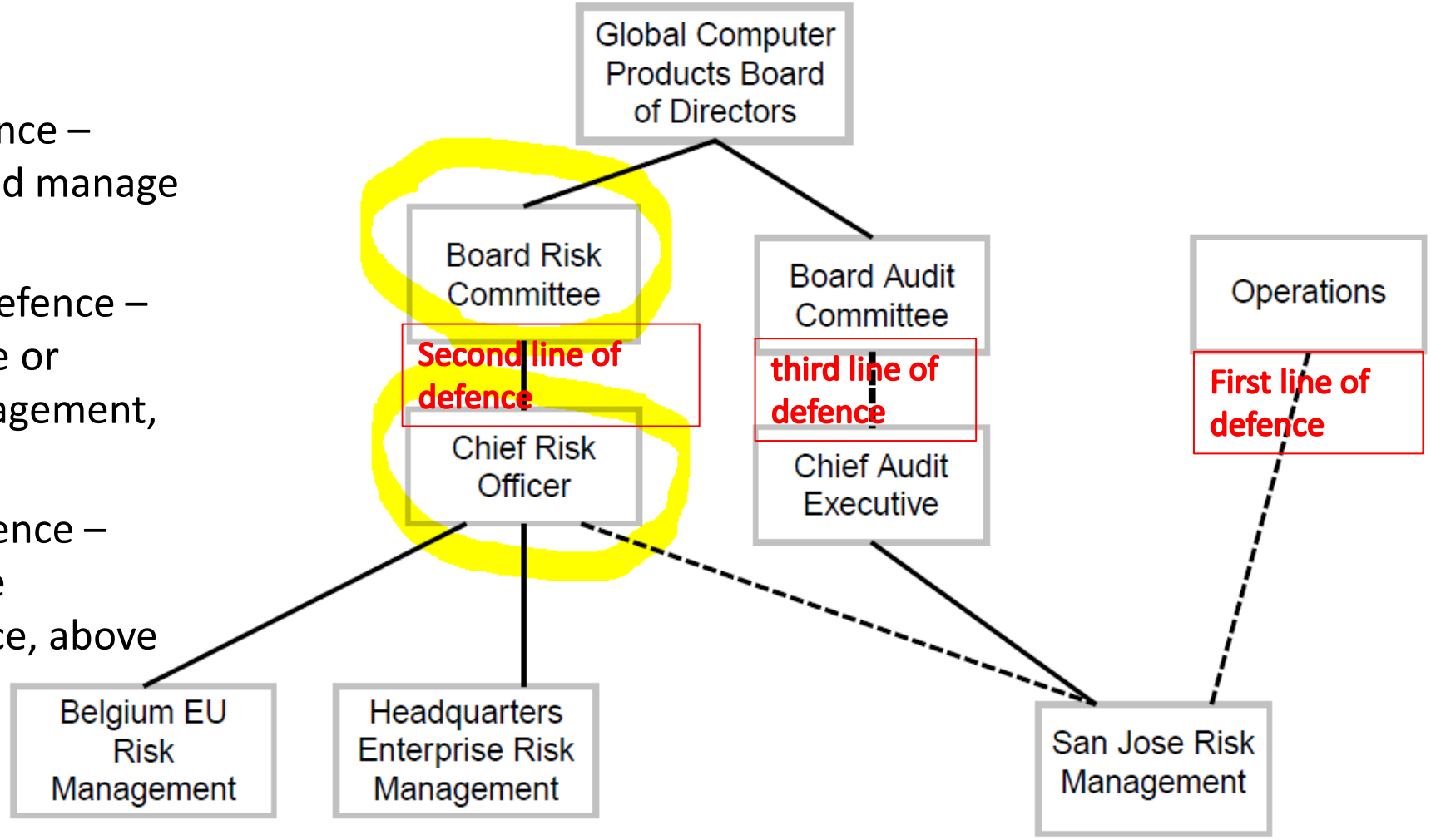
COSO and The Three Lines of Defence

The Three Lines of Defence (3LOD) Model

1.the first line of defence – functions that own and manage risk

2.the second line of defence – functions that oversee or specialise in risk management, compliance

3.the third line of defence – functions that provide independent assurance, above all internal audit



COSO Enterprise Risk Management, Robert Moeller, Wiley

Main differences between COSO and ISO 31000

ISO 31000 vs COSO

Structure

The length of the COSO is over 100 pages. ISO 31000 has 16 pages and can be read in less than an hour.

ISO 31000 also follows a more organized structure than COSO.

Geography

ISO 31000 is the official risk management standard in over 50 countries.

COSO was developed in the United States in partnership with PwC, a large accounting and consulting firm.

Audience

ISO 31000 is a more generic risk management standard. It was created for anyone interested in risk management.

COSO is focused on financial reporting.

ISO 31000 vs COSO

Focus

ISO 31000 focuses on risk and incorporating it everywhere in the organization.

COSO focuses more on general corporate governance.

Framework and Process

ISO 31000 clearly separates a framework and a process.

COSO combines the two concepts.

Risk Appetite

ISO 31000:2009 – no mention of risk appetite

ISO 31000: 2018 – brief mention, using different terminology

COSO – discusses risk appetite in great length

Some considerations on Risk Matrices

Some considerations on Risk Matrices

Risk matrices have been widely praised and adopted as simple, effective approaches to risk management. They provide a clear framework for systematic review of individual risks and portfolios of risks; convenient documentation for the rationale of risk rankings and priority setting.

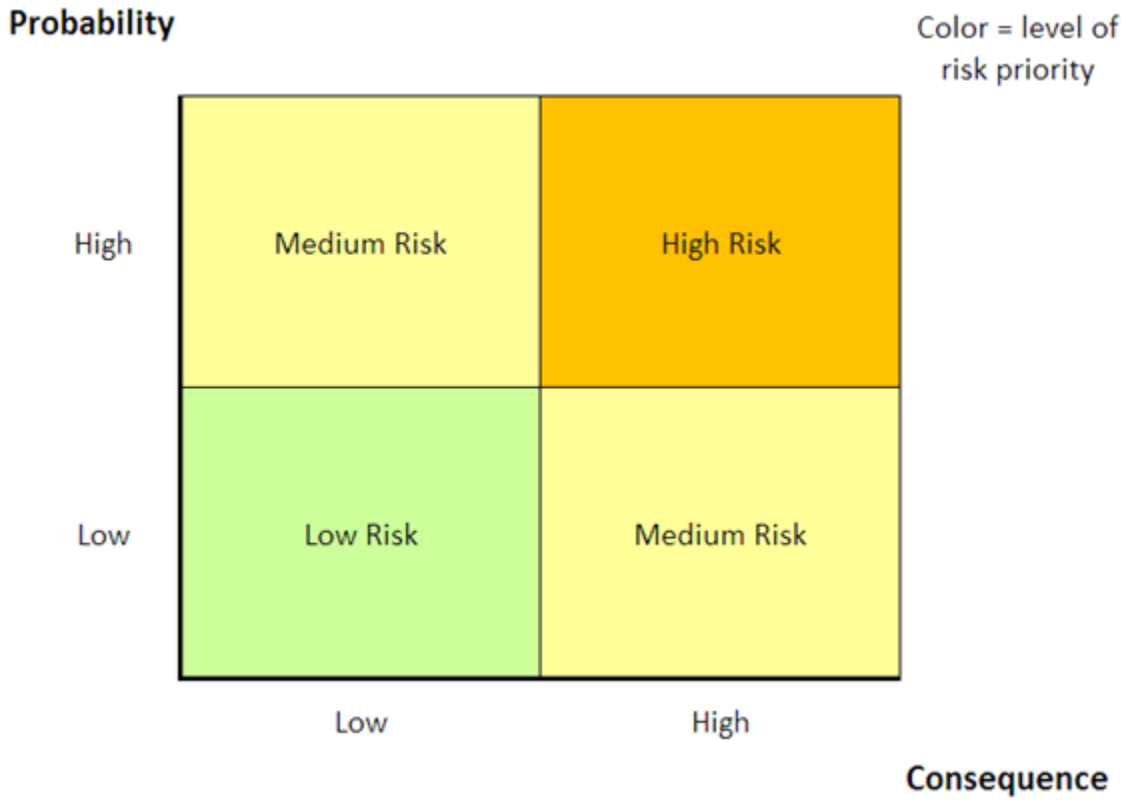
But… "risk" is not a measured attribute, but is derived from **frequency and severity** inputs through a priori specified formulas such as:

Risk = Frequency × Severity.

This article explores fundamental mathematical and logical limitations of risk matrices as sources of information for risk management decision making and priority setting.

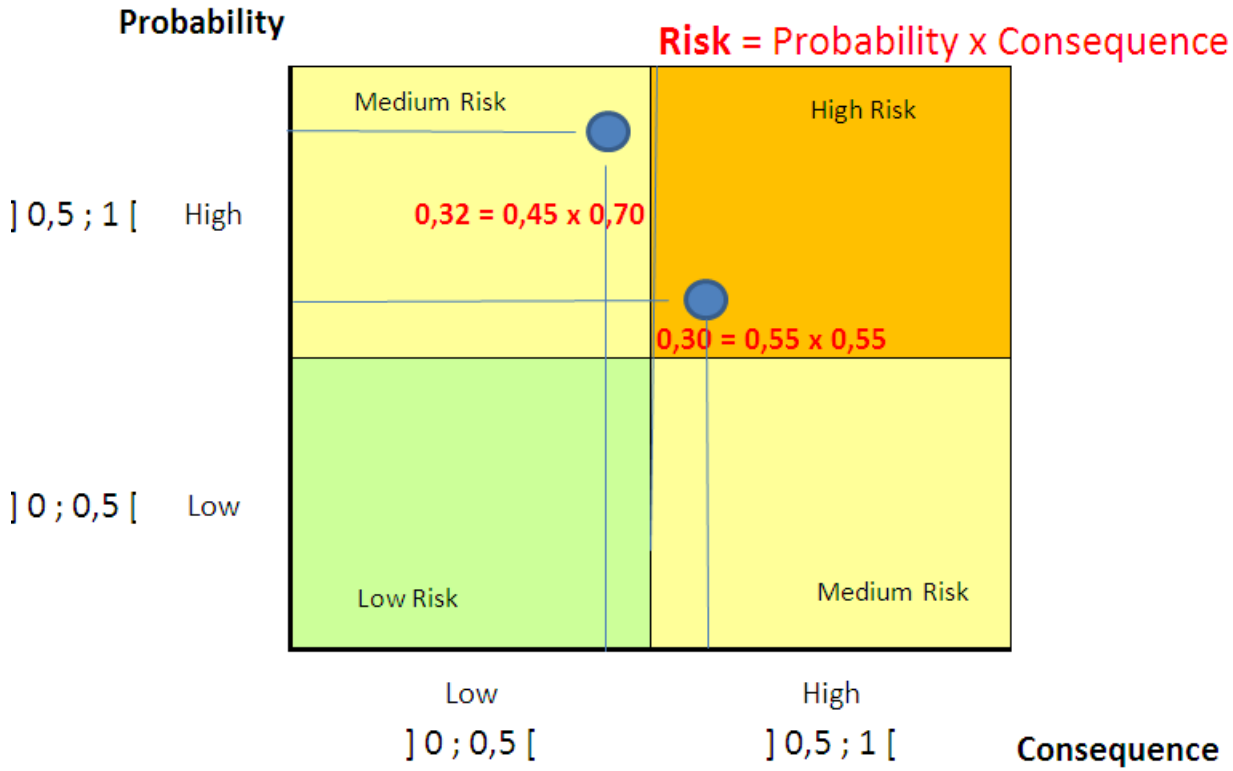
Some considerations on Risk Matrices

A Normative decision-analytic framework



Some considerations on Risk Matrices

The simplest case of a 2 × 2 risk matrix does suggest it is not necessarily true that risk matrices provide qualitatively useful information for setting risk priorities.



Some considerations on Risk Matrices

Logical compatibility of risk matrices with quantitative risks

Lemma 1. If a risk matrix satisfies weak consistency, then no red cell can share an edge with a green cell.

Lemma 2: If a risk matrix satisfies weak consistency and has at least two colors (“green” in the lower left cell and “red” in the upper right cell, if axes are oriented to show increasing frequency and severity), then no red cell can occur in the left column or in the bottom row of the risk matrix.

Definition of betweenness: A risk matrix satisfies the axiom of betweenness if every positively sloped line segment that lies in a green cell at its lower (left) end and in a red cell at its upper (right) end passes through at least one intermediate cell (meaning one that is neither green nor red) between them.

Some considerations on Risk Matrices

Logical compatibility of risk matrices with quantitative risks

Definition of consistent coloring:

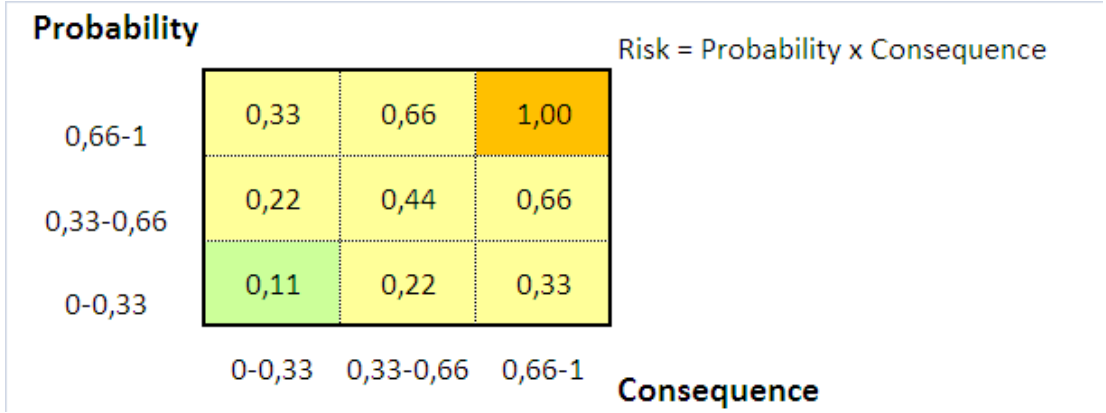
A cell is red if it contains points with quantitative risks at least as high as those in other red cells (and does not contain points with quantitative risk as small as those in any green cell).

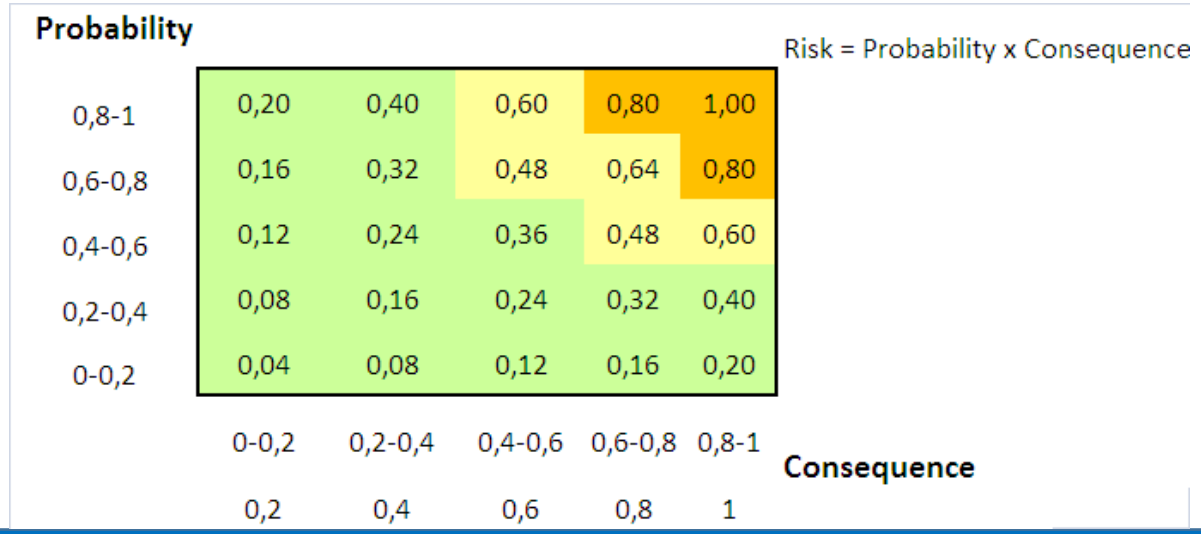
(2) A cell is colored green if it contains some points with risks at least as small as those in other green cells (and does not contain points with quantitative risks as high as those in any red cell).

(3) A cell is colored an intermediate color (neither red nor green) only if either (a) it lies between a red cell and a green cell; or (b) it contains points with quantitative risks lower than those in some red cells and also points with quantitative risks higher than those in some green cells.

Some considerations on Risk Matrices

Logical compatibility of risk matrices with quantitative risks





Some considerations on Risk Matrices

Logical compatibility of risk matrices with quantitative risks

Probability

Risk = Probability x Consequence

	0-0,33	0,33-0,66	0,66-1
0,66-1	0,33	0,66	1,00
0,33-0,66	0,22	0,44	0,66
0-0,33	0,11	0,22	0,33

Consequence

Probability

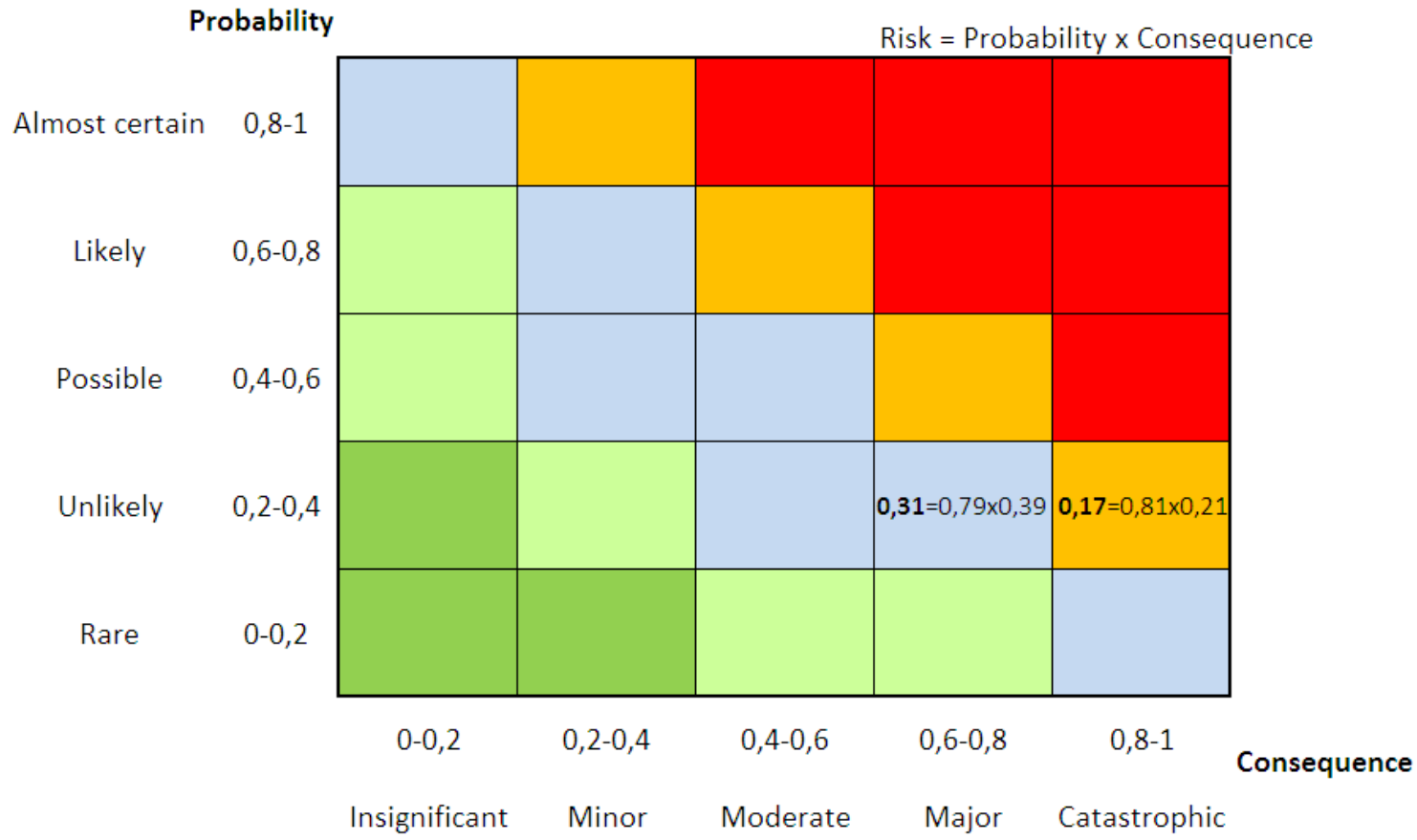
Risk = Probability x Consequence

	0-0,2	0,2-0,4	0,4-0,6	0,6-0,8	0,8-1
0,8-1	0,20	0,40	0,60	0,80	1,00
0,6-0,8	0,16	0,32	0,48	0,64	0,80
0,4-0,6	0,12	0,24	0,36	0,48	0,60
0,2-0,4	0,08	0,16	0,24	0,32	0,40
0-0,2	0,04	0,08	0,12	0,16	0,20

Consequence

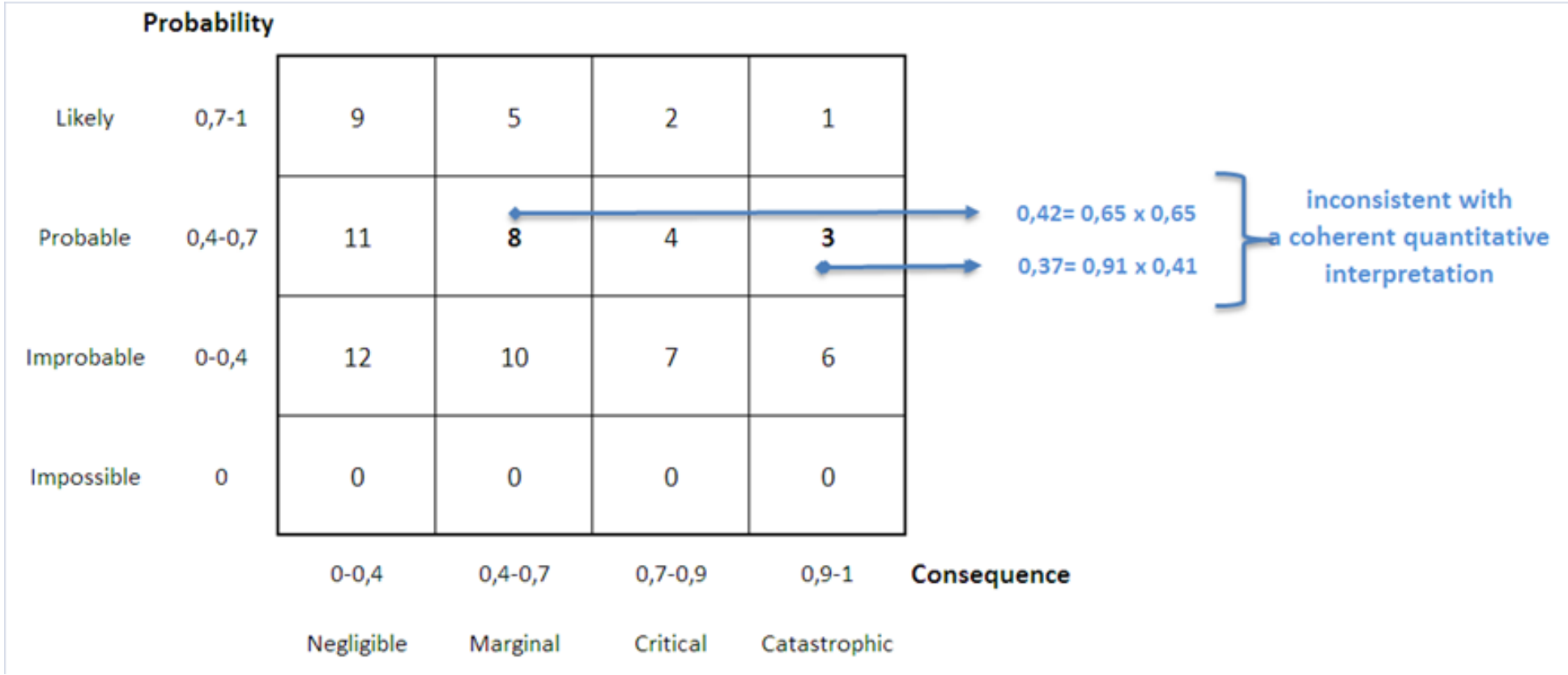
Some considerations on Risk Matrices

Risk matrices with too many colors or levels give spurious resolution



Some considerations on Risk Matrices

There's 13 priority levels as possible outputs, Anything that is in the box labeled “1” is the highest priority.



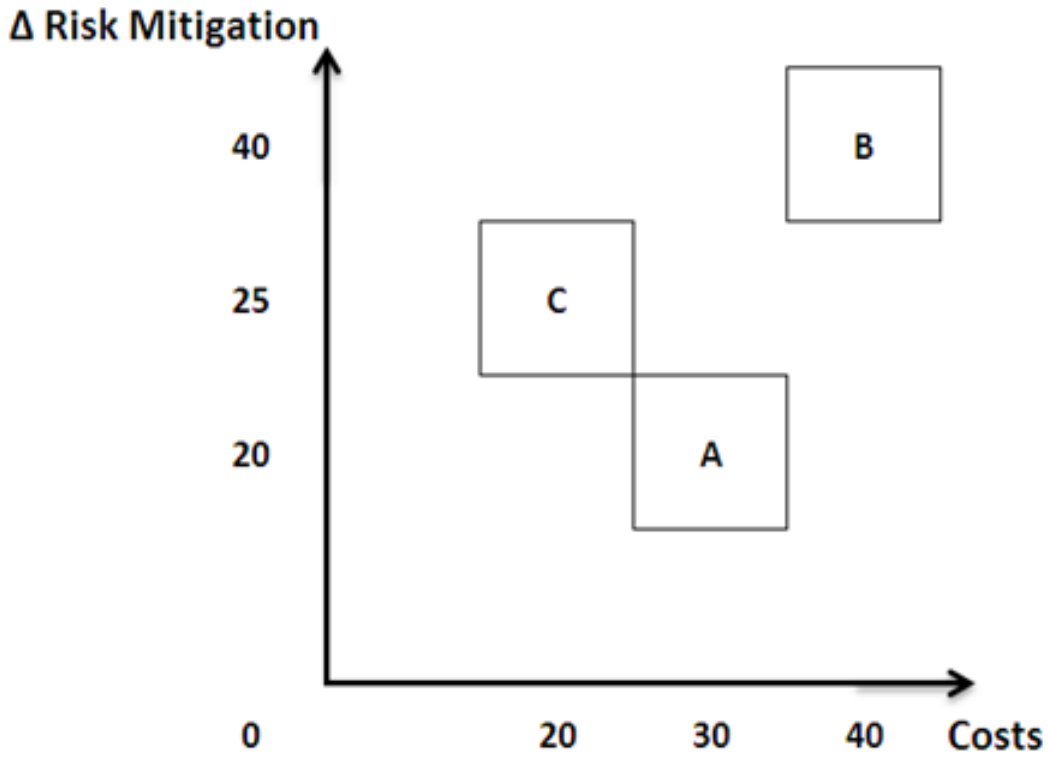
Some considerations on Risk Matrices

A risk manager has identified the following three risk reduction opportunities:

A. reduces risk from 100 to 80. It costs $30:

B. reduces risk from 50 to 10. It costs $40.

C. reduces risk from 25 to 0. It costs $20.



How should a risk matrix categorize A, B, C to support the goal of achieving the largest risk reduction from allocation of limited funds?

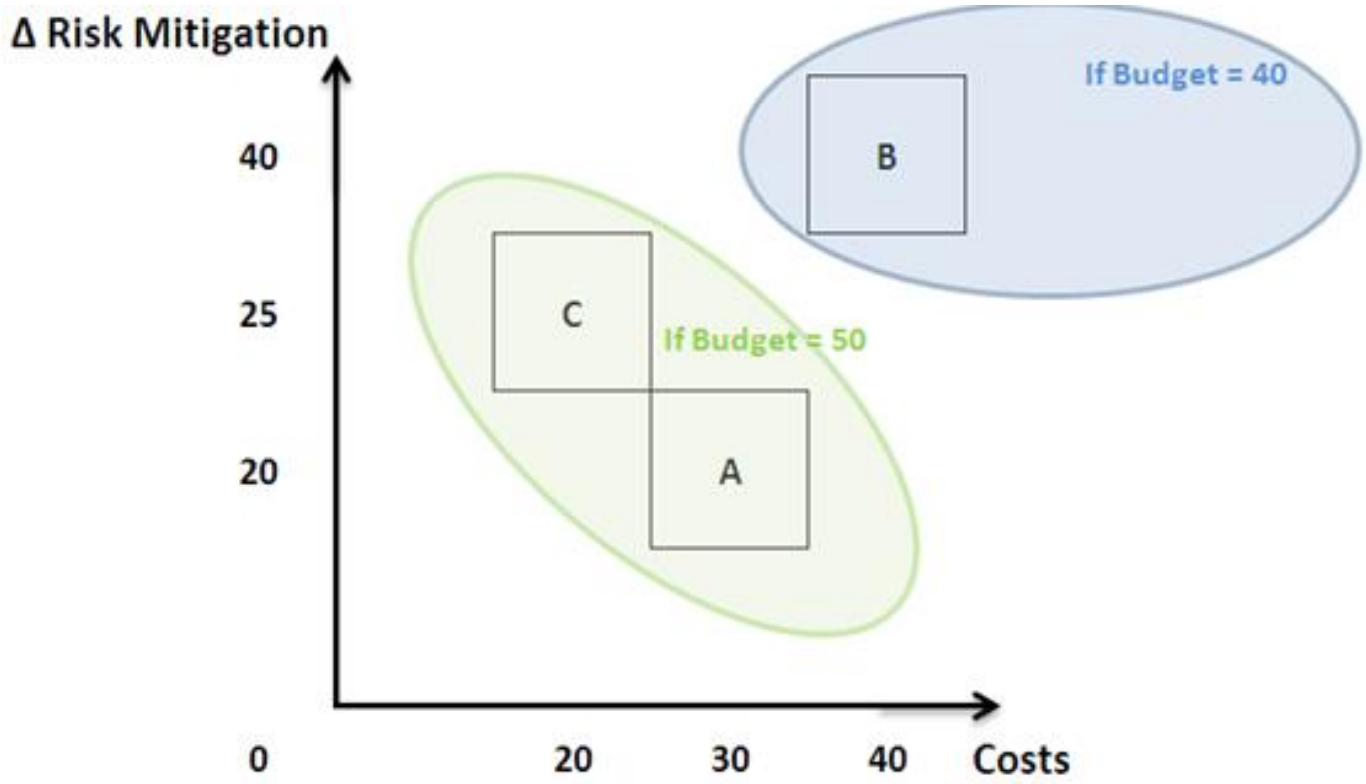
The answer: depends on the budget!

Some considerations on Risk Matrices

For a budget of $40, the largest feasible risk reduction is achieved by funding B, so the best priority order puts B first.

If the budget is $50, then funding A and C achieves the greatest risk reduction, so B should be ranked last.

At $60, the best investment is to fund B and C, so now A should be ranked last..



Some considerations on Risk Matrices

In short, no categorization or rank-ordering of A, B, and C, optimizes resource allocation independent of the budget.

Calculating optimal risk management resource allocations requires quantitative information beyond what a risk matrix provides, for example, about budget constraints and about interactions among countermeasures.

In general, risk rankings calculated from frequency and severity do not suffice to guide effective risk management resource allocation decisions.

Some considerations on Risk Matrices

For a decision maker with an exponential utility function, the certainty equivalent (CE) value of a prospect with normally distributed consequences is $CE(X) = E(X) - k \times Var(X)$,

where:

k is a parameter reflecting subjective risk aversion (k = 0.5 × coefficient of risk aversion);

E(X) is the mean of prospect X;

Var(X) is its variance;

CE(X) is its certainty-equivalent value (i.e., the deterministic value that is considered equivalent in value to the uncertain prospect)

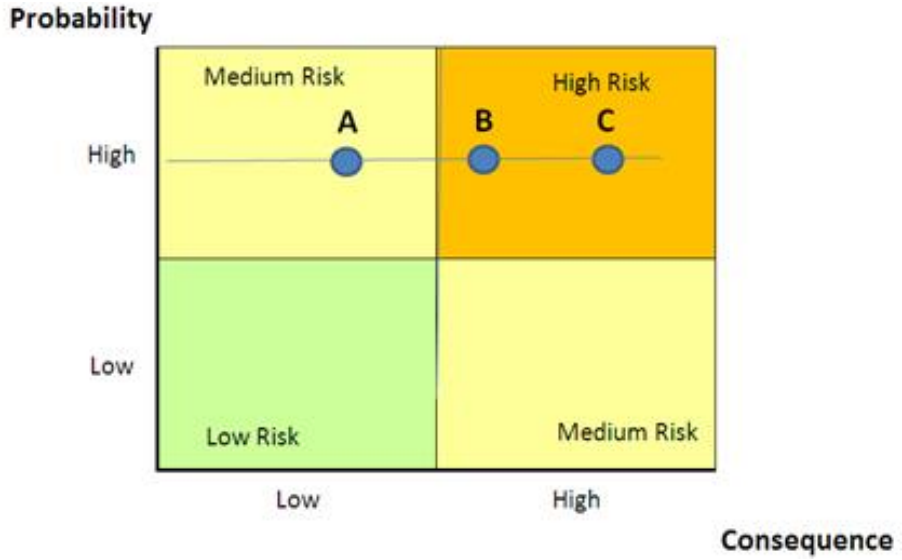
Some considerations on Risk Matrices

Consider three events, A, B, and C, with identical probabilities or frequencies and having normally distributed consequences (on some outcome scale) with respective means of 1, 2, and 3 and respective variances of 0, 1, and 2. The certainty equivalents of prospects A, B, and C are:

$$CE(A) = 1 ; \qquad CE(B) = 2 - k ; \qquad CE(C) = 3 - 2k$$

For a **risk-neutral** decision maker with **k = 0**:

C > B > A



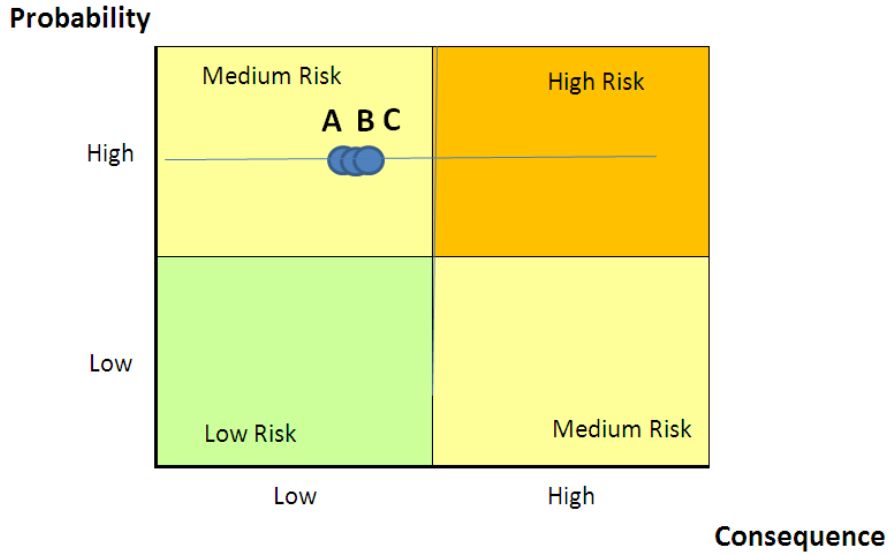
Some considerations on Risk Matrices

Consider three events, A, B, and C, with identical probabilities or frequencies and having normally distributed consequences (on some outcome scale) with respective means of 1, 2, and 3 and respective variances of 0, 1, and 2. The certainty equivalents of prospects A, B, and C are:

$$CE(A) = 1 \; ; \qquad CE(B) = 2 - k \; ; \qquad CE(C) = 3 - 2k$$

For a **risk-averse** decision maker with **k = 1**:

A = B = C



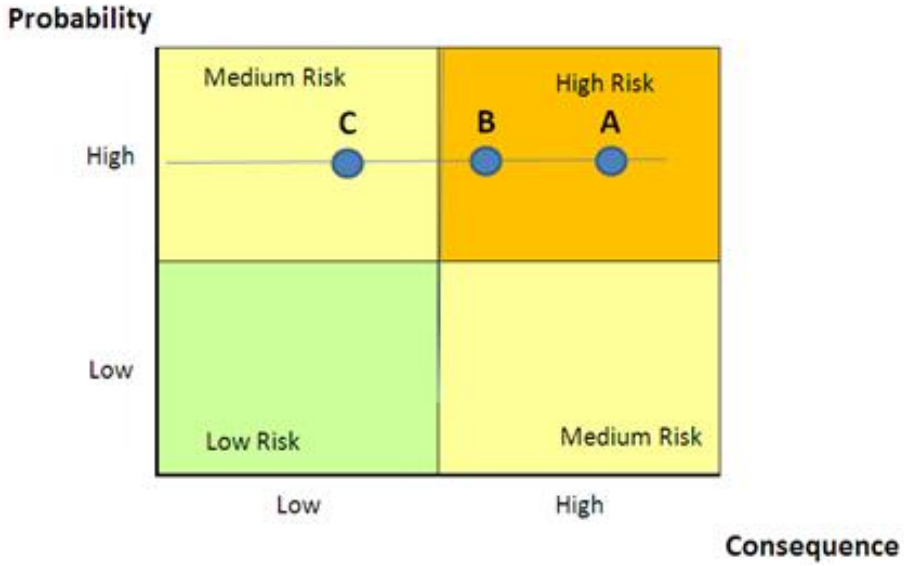
Some considerations on Risk Matrices

Consider three events, A, B, and C, with identical probabilities or frequencies and having normally distributed consequences (on some outcome scale) with respective means of 1, 2, and 3 and respective variances of 0, 1, and 2. The certainty equivalents of prospects A, B, and C are:

$$CE(A) = 1 ; \qquad CE(B) = 2 - k ; \qquad CE(C) = 3 - 2k$$

For a **more risk-averse** decision maker with **k = 2**:

$$A > B > C$$

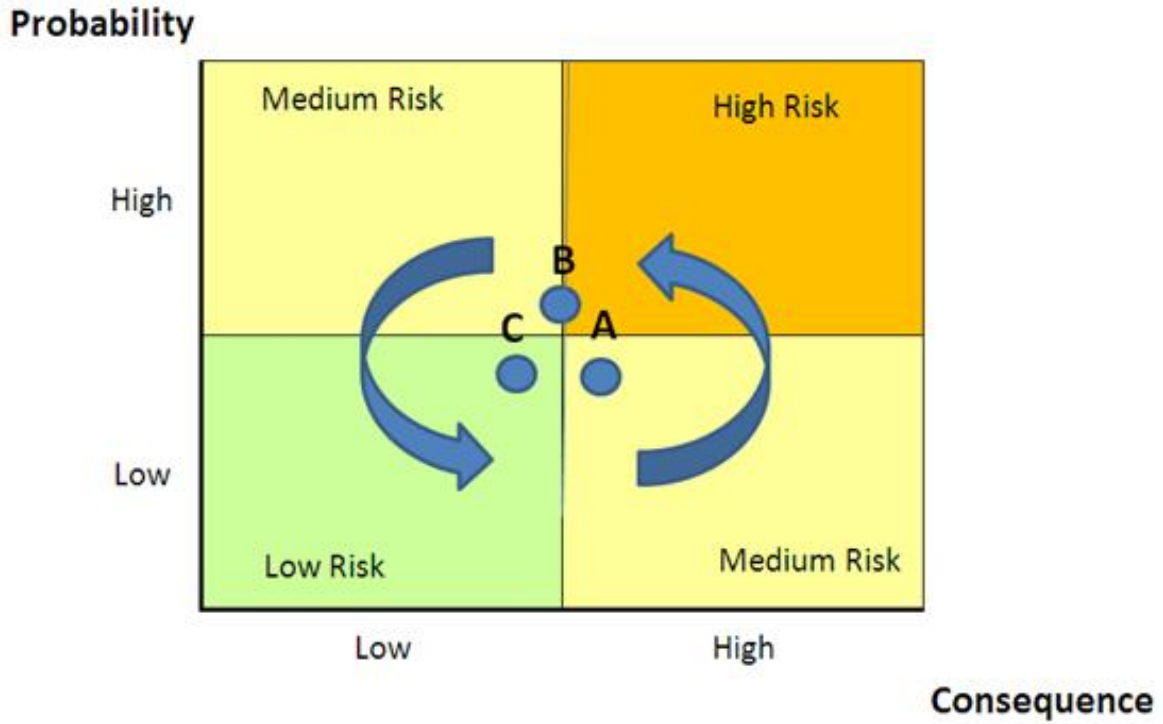


Some considerations on Risk Matrices

Risk matrices typically do not specify or record the risk attitudes of those who use them.

Users with different risk attitudes might have opposite orderings, as in this example.

As a result there is no objective way to classify the relative severities of such prospects with uncertain consequences



Some considerations on Risk Matrices

How should one rate the severity of a consequence that consists of 1 death and 1 severe injury compared to that of a consequence of 0 deaths but 50 severe injuries? The answer is not obvious from the example below!

Severity Level	Characteristics
I Catastrophic	Death, system loss, or severe environmental damage
II Critical	Severe injury, severe occupational illness, major system or environmental damage
III Marginal	Minor injury, minor occupational illness, or minor system or environmental damage
IV Negligible	Less than minor injury, occupational illness, or less than minor system or environmental damage

Source: GAO (1998).

Some considerations on Risk Matrices

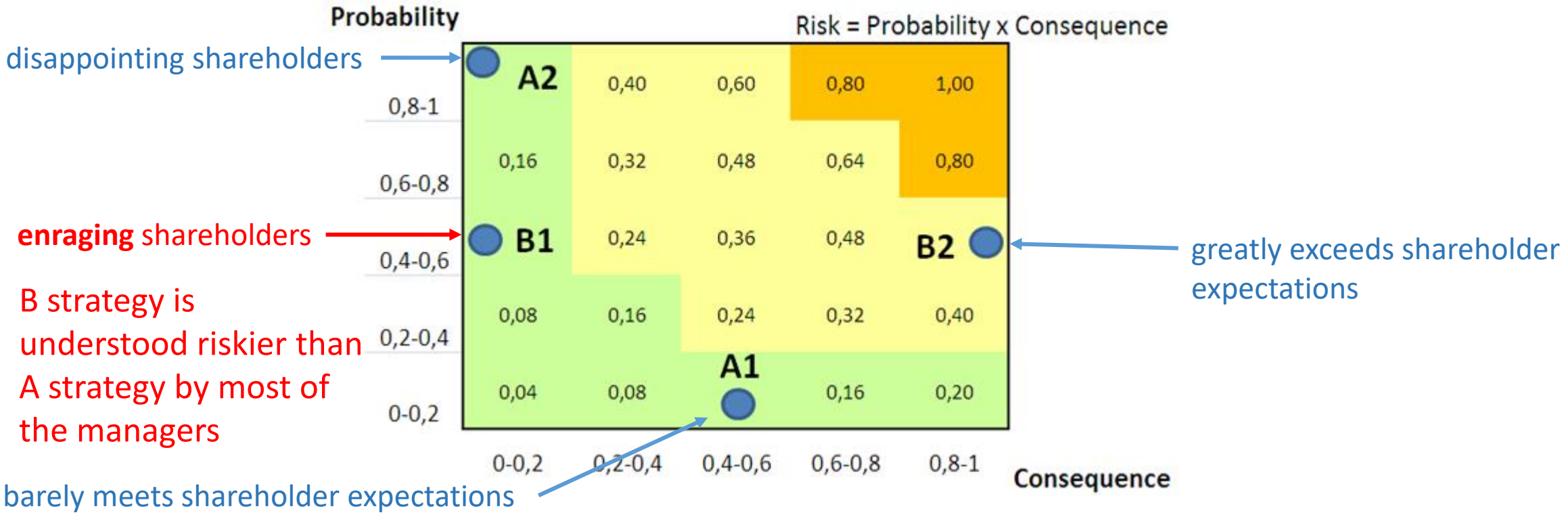
Suppose that a company must choose between the following two risky investment strategies:

- Strategy A has probability 0.1% of leading to a 1% growth rate that barely meets shareholder expectations (outcome **A1**); otherwise (probability 99.9%) shareholder value and growth will increase by a negligible amount (0.0001%), disappointing shareholders (outcome **A2**).
- Strategy B has probability 50% of causing 5% sustained growth that greatly exceeds shareholder expectations (outcome **B1**); otherwise, shareholder value and growth rate = 0%, enraging shareholders. (outcome **B2**).

Which strategy, A or B, better matches a responsible company's preferences (or "risk appetite") for risky strategic investments?

Some considerations on Risk Matrices

Implementing the discrete categorization criteria in the guidance could distract attention from the fact that most shareholders would gladly trade a negligible increase in adverse consequences for a large increase in the probability of a much better outcome.



Some considerations on Risk Matrices

Prospect theory is a theory of behavioral economics and behavioral finance that was developed by Daniel Kahneman and Amos Tversky in 1979. The theory was cited in the decision to award Kahneman the 2002 Nobel Memorial Prize in Economics.

Prospect theory stems from Loss aversion, where the observation is that agents asymmetrically feel losses greater than that of an equivalent gain. It centralizes around the idea that people conclude their utility from "gains" and "losses" relative to a certain reference point. This "reference point" is different for each person and relative to their individual situation. Thus, rather than making decisions like a rational agent (i.e using Expected utility theory and choosing the maximum value), decisions are made in relativity not in absolutes.

Some considerations on Risk Matrices

Consider two scenarios;

100% chance to gain $450 or 50% chance to gain $1000

100% chance to Lose $500 or 50% chance to lose $1100

Prospect theory suggests that;

- When faced with a risky choice leading to gains agents are risk averse, preferring the certain outcome with a lower expected utility. (concave value function)
- Agents will choose the certain $450 even though the expected utility of the risky gain is higher
- When faced with a risky choice leading to losses agents are risk seeking, preferring the outcome that has a lower expected utility but the potential to avoid losses. (convex value function)
- Agents will choose the 50% chance to lose $1100 even though the expected utility is lower, due to the chance that they lose nothing at all

Some considerations on Risk Matrices

In the terminology of multicriteria decision making, the discrete categorization of consequences and probabilities inherent in risk matrices can produce “non compensatory” (*) decision rules that do not reflect the risk trade-off preferences of real decisionmakers and stakeholders.

So, resuming, Risk matrices do not necessarily support good (e.g., better-than-random) risk management decisions and effective allocations of limited management attention and resources.

Research is needed to better characterize conditions under which they are most likely to be helpful or harmful in risk management decision making and that develops methods for designing them to maximize potential decision benefits and limit potential harm from using them.

(*): A **compensatory** decision-making strategy weighs the positive and negative attributes of the considered alternatives and allows for positive attributes to compensate for the negative ones.