

ENTERPRISE RISK MANAGEMENT

Ph. D. Özgür SATICI (CGAP)
Geo. Eng. (Msc. in Mining Eng. - MBA)

June 5, 2018, Joint Vienna Institute Vienna

Internal Audit Training of Trainers



CFRR >>

**Centre for Financial
Reporting Reform**



Co-funded by



**European
Union**



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Contents

1

- What is risk?

2

- What is risk management?

3

- How do we behave under certain risk circumstances?

4

- Why do we need to manage risks?

5

- Common frameworks and standards?

6

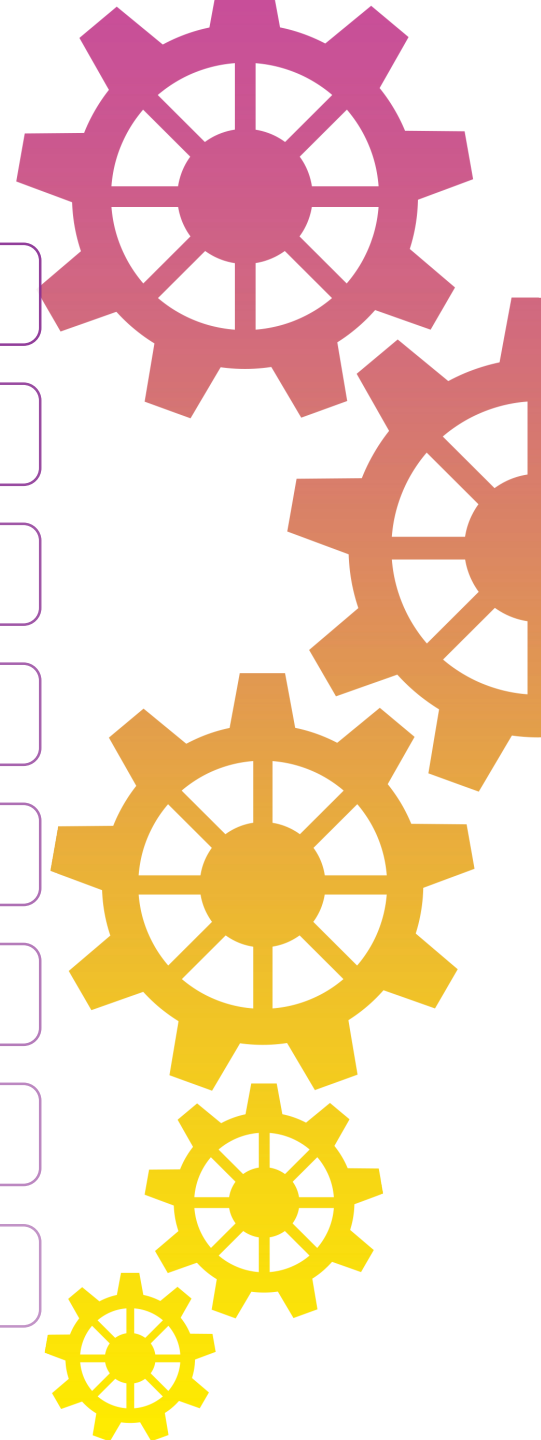
- COSO 2017 ERM Framework

7

- Situation in Turkey

8

- Questions



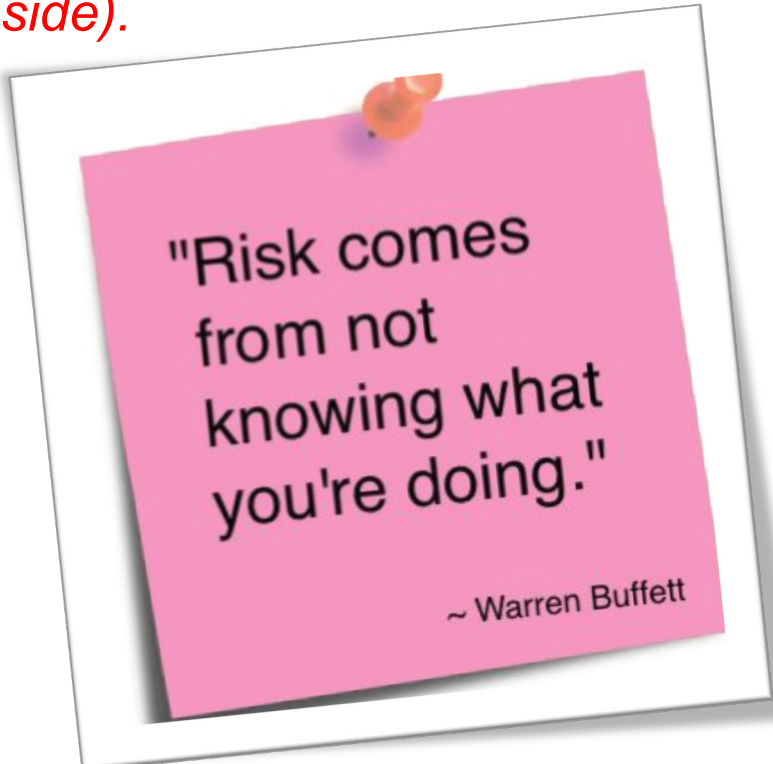
1

- What is risk?



• What is risk?

- *The most common concept in all definitions is the uncertainty of outcomes.*
- *Risk can be defined as the combination of the probability of an event and its consequences.*
- *In all types of undertaking, there is the potential for events and consequences that constitute opportunities for benefit (upside) or threats to success (downside).*



"Risk comes from not knowing what you're doing."

~ Warren Buffett

1

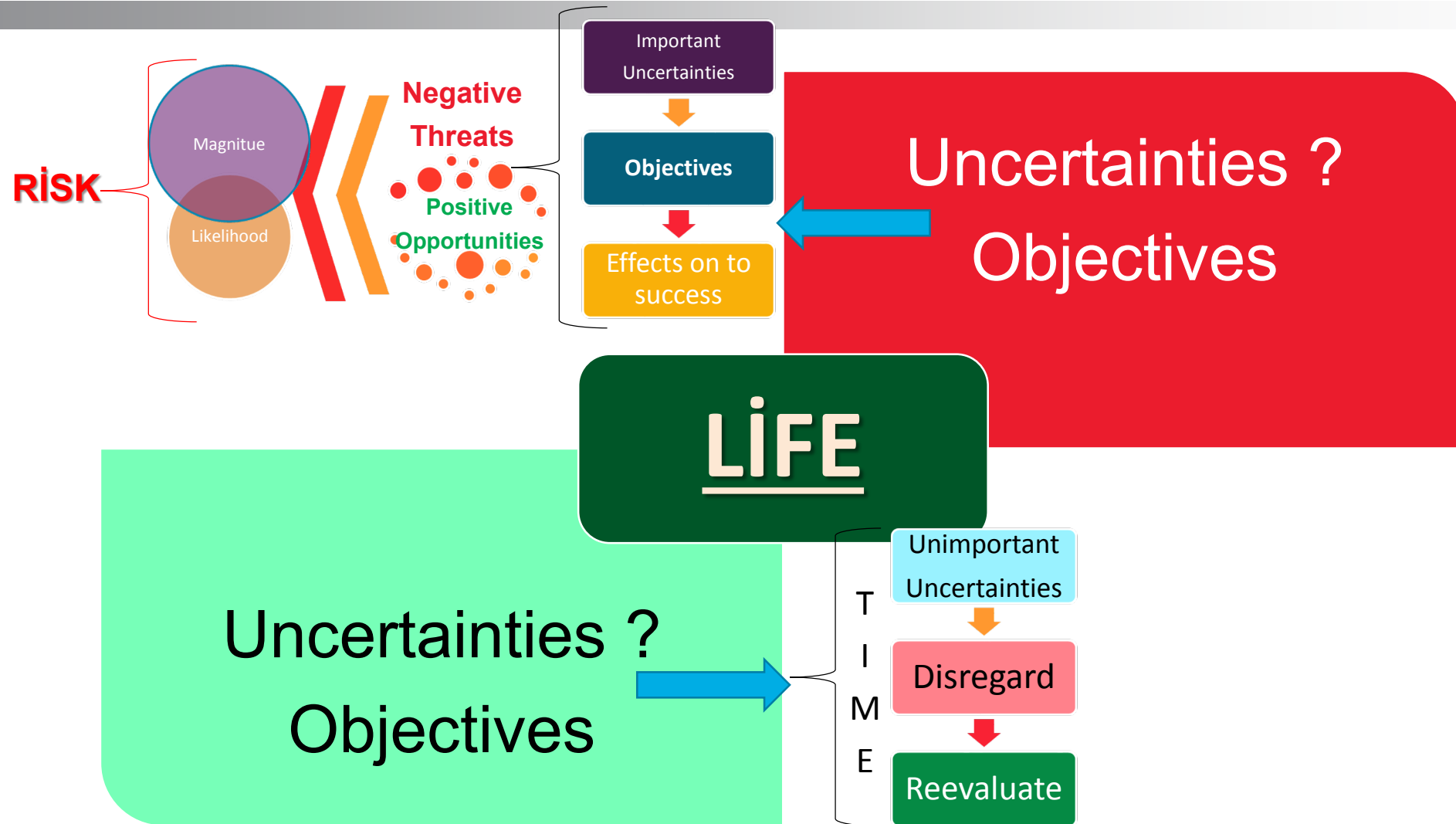
- What is risk?

Risk is everywhere and derives directly from unpredictability.



Risk is unavoidable but can be controlled!!!

- What is risk management?



- What is risk management?



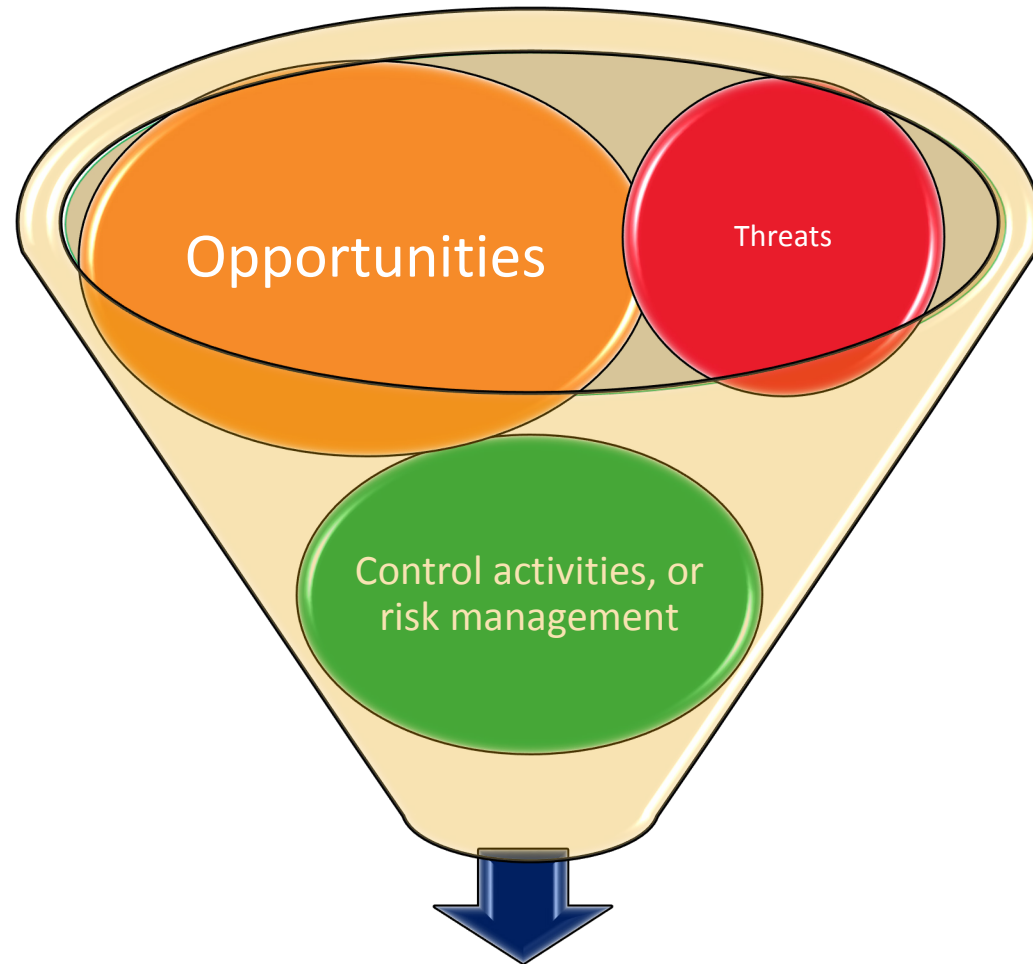
*Not all of the uncertainties
are risk, but all of the risks
are always uncertain.
This depends on how much
important that uncertainties
for us on our objectives.*



- What is risk management?

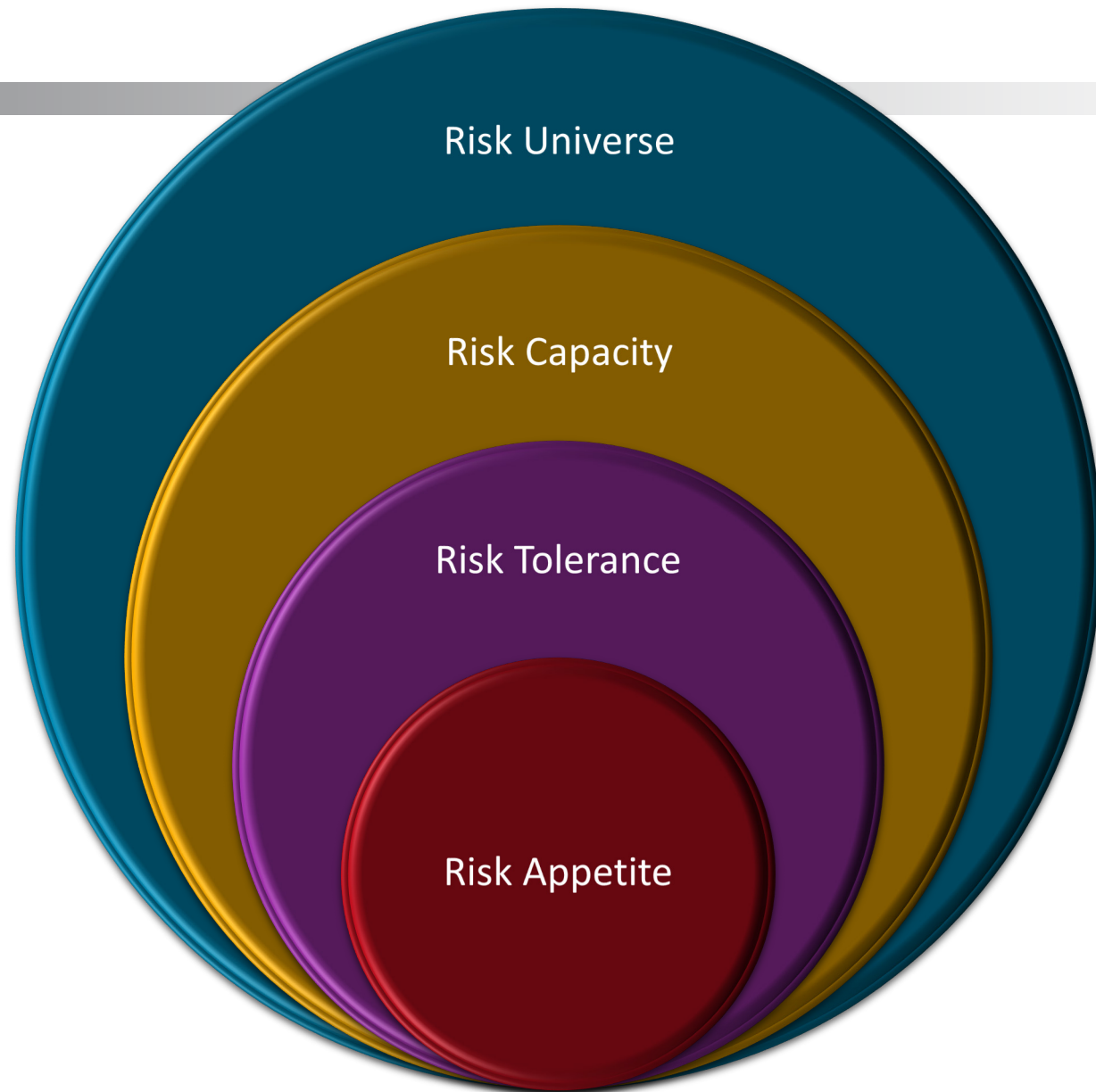


- What is risk management?



Objectives, outcomes, deviations





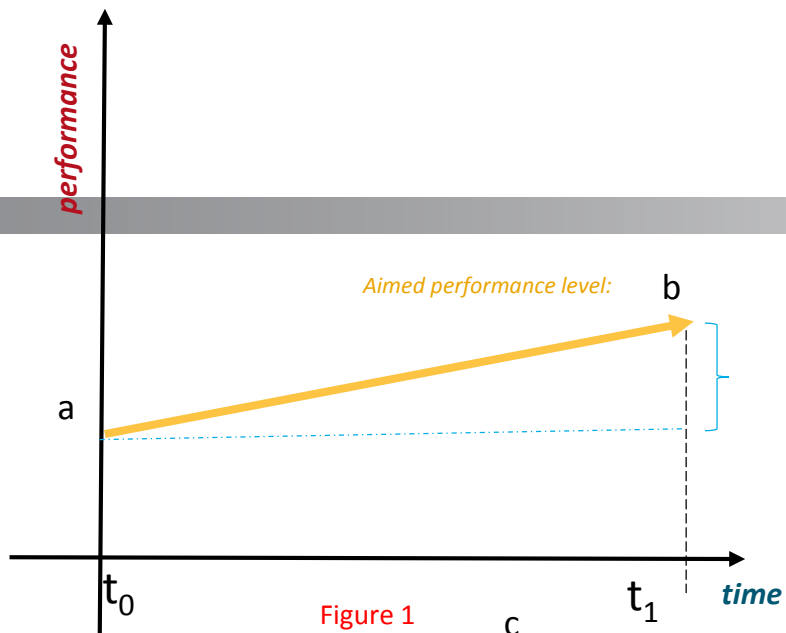


Figure 1

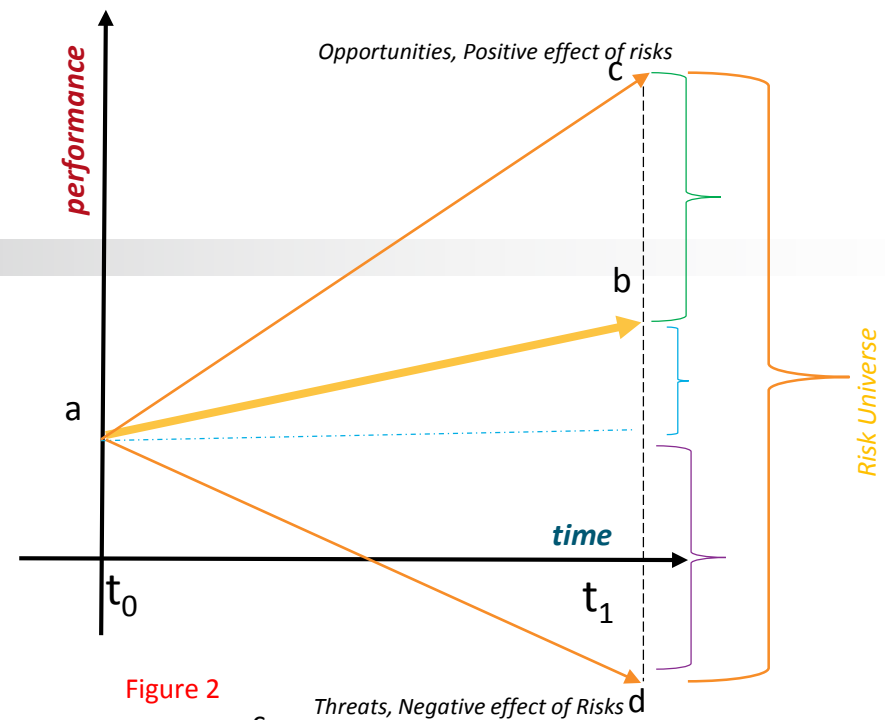


Figure 2

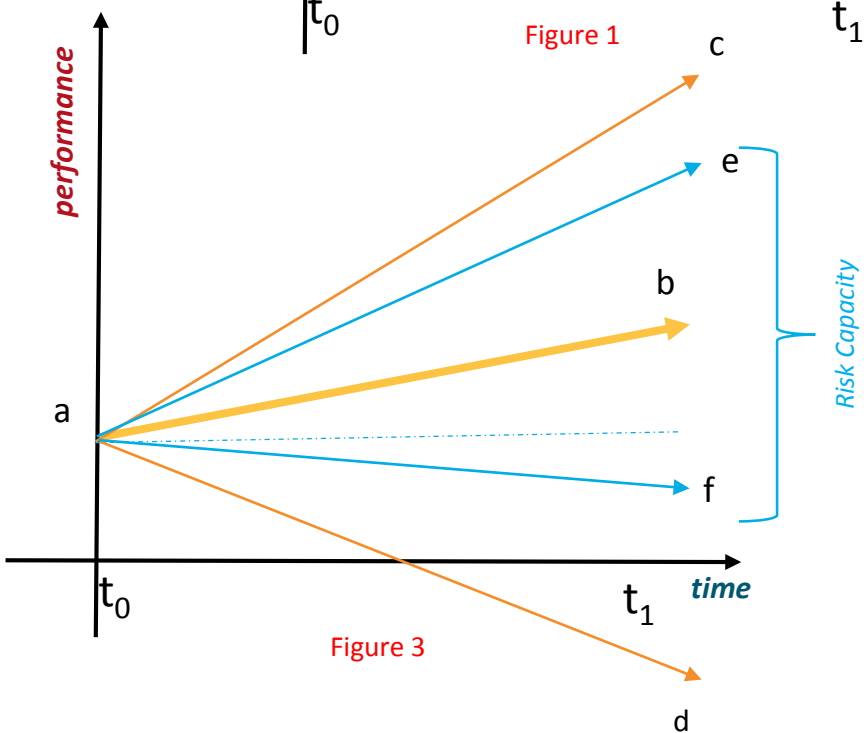


Figure 3

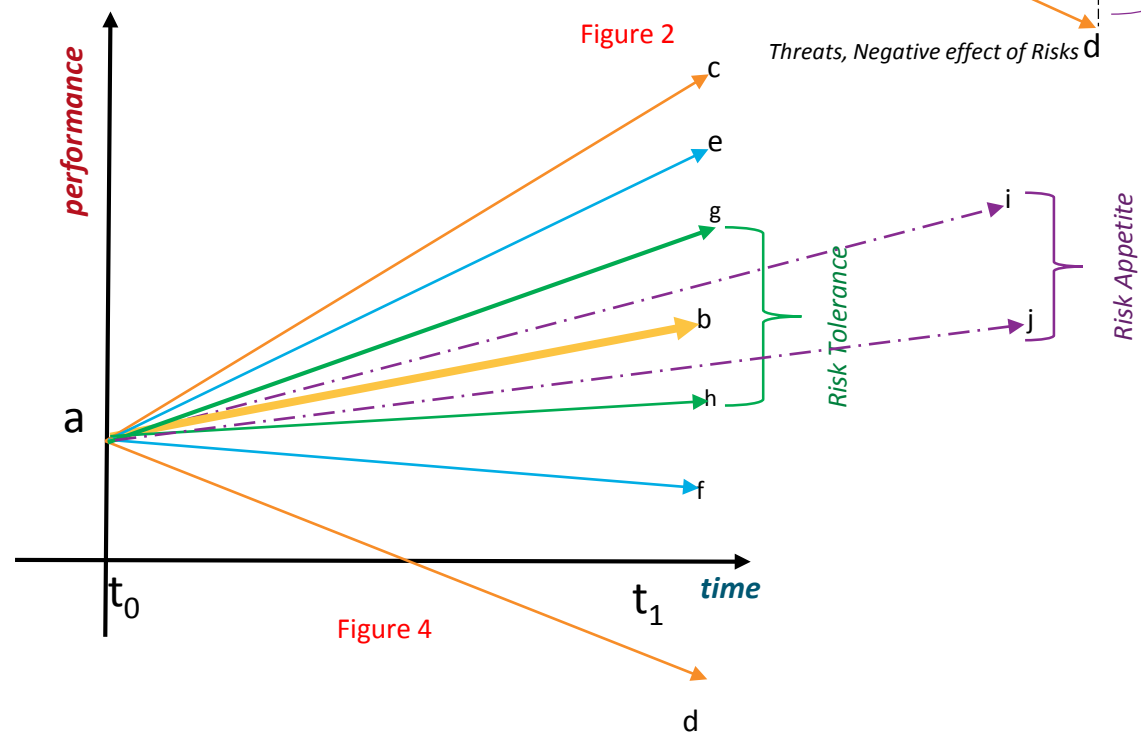
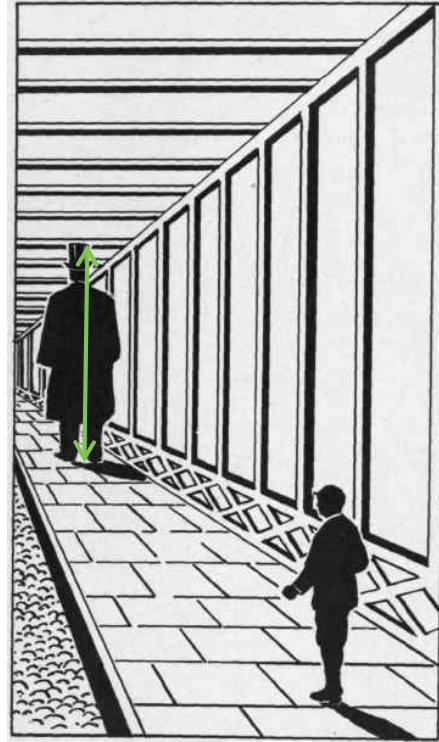
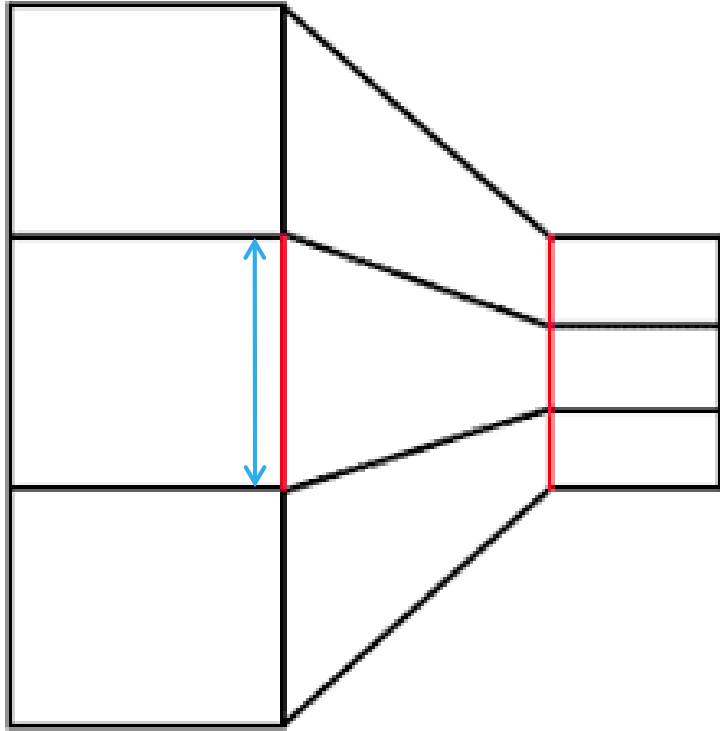
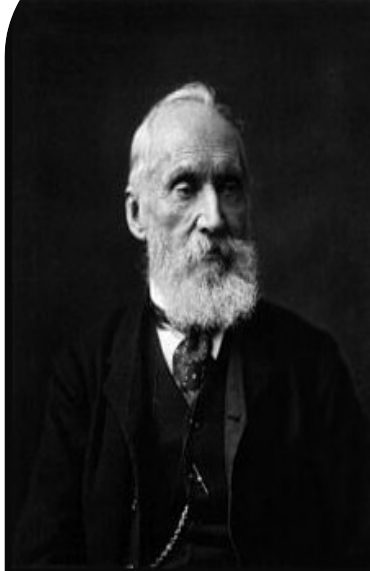


Figure 4





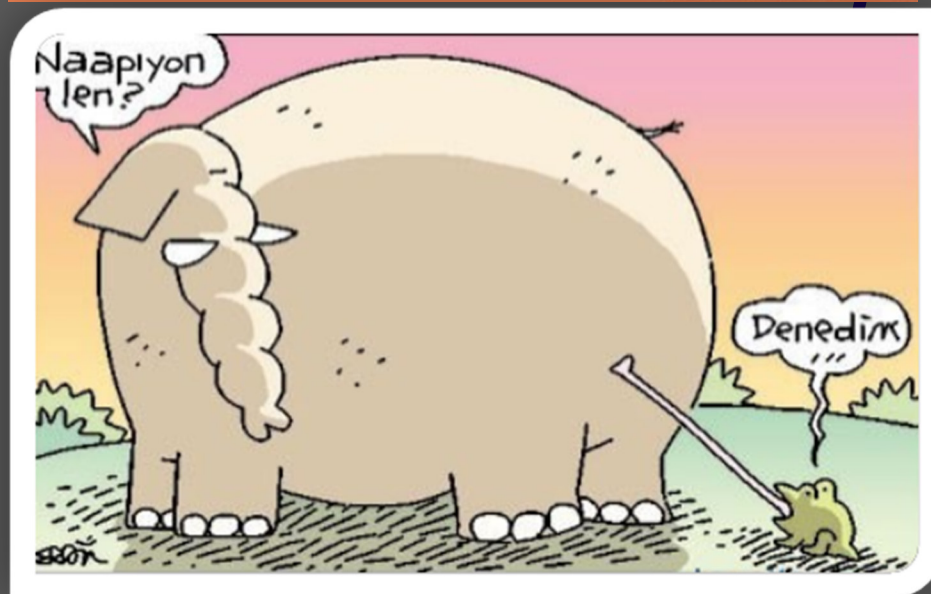


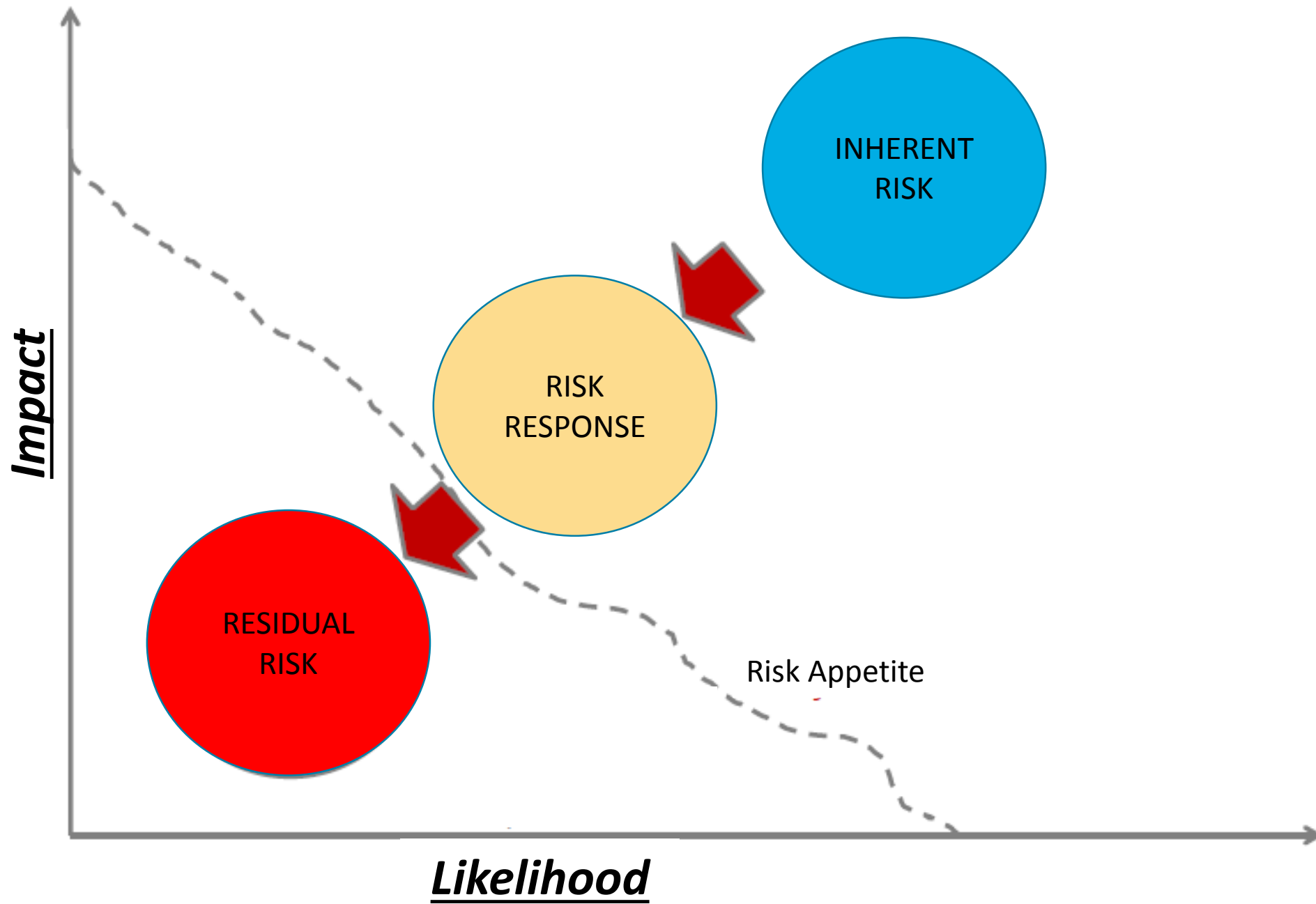
I often say that when you can measure what you are speaking about, and express it in numbers, you know something about it; but when you cannot measure it, when you cannot express it in numbers, your knowledge is of a meagre and unsatisfactory kind: it may be the beginning of knowledge, but you have scarcely, in your thoughts, advanced to the stage of science, whatever the matter may be.

(Lord Kelvin)



- How do we behave under certain risk circumstances?



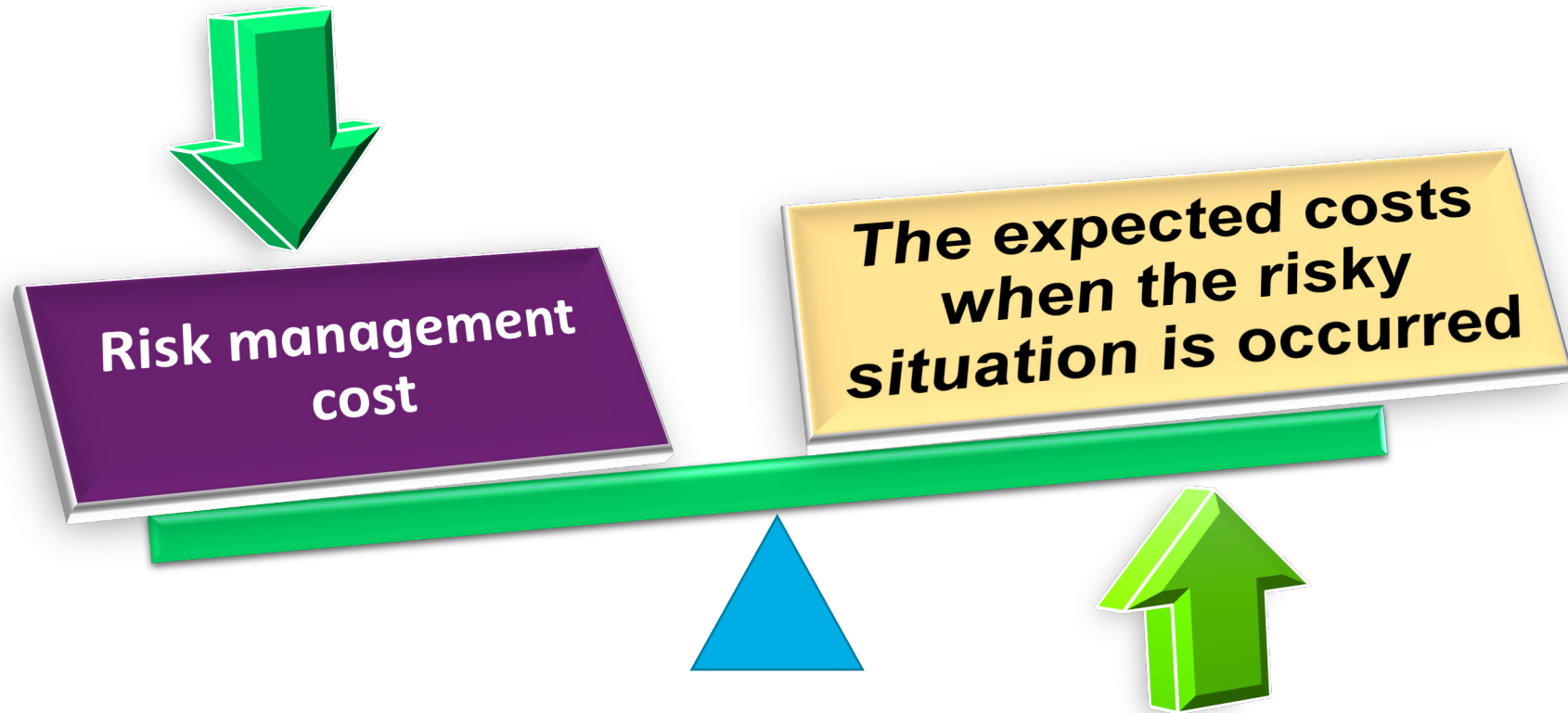


- Why do we need to manage risks?

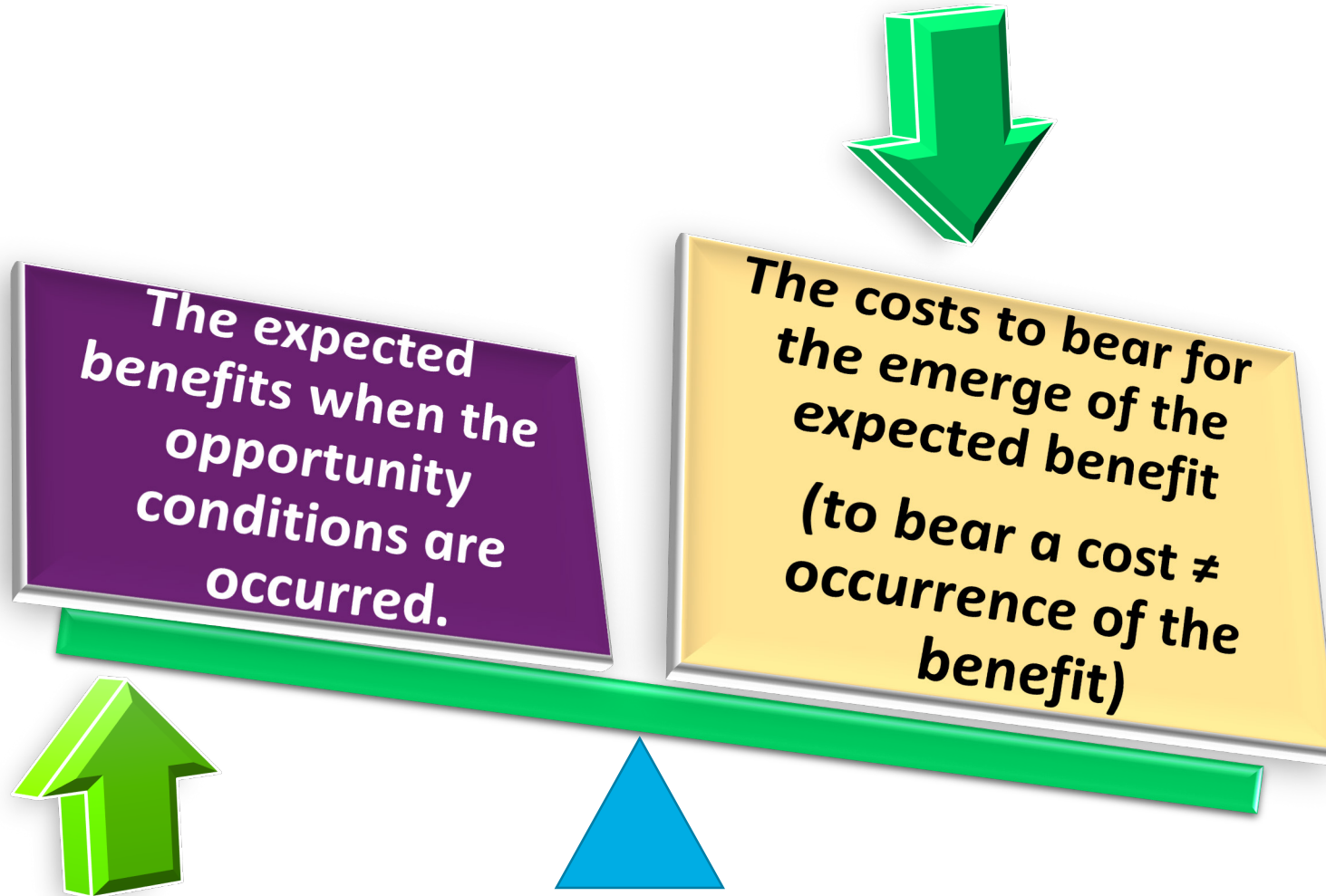
As that is so, the need for pre-designed risk management systems have been emerged.



- Why do we need to manage risks?

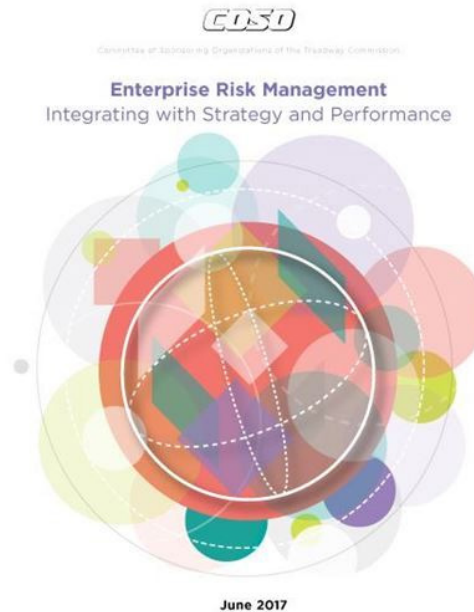


- Why do we need to manage risks?



- Common frameworks and standards?

Standards and frameworks give us predetermined paths, rules and principles for managing risks.



- Common frameworks and standards?

According to COSO (2004- 2013)

«ERM is defined as “a process, effected by the entity’s board of directors, management and other personnel, applied in a strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of objectives»

- » In September 2017, the Committee of Sponsoring Organizations of the Treadway Commission issued the much-awaited update to the 2004 ERM–Integrated Framework,
- » The newly released ERM Framework is authored named as “Enterprise Risk Management–Integrating with Strategy and Performance”.
- » The new framework reflects the evolution of ERM thinking and practices, and links the risk management approach with the fundamental business model and process.

The updated framework defines the ERM as:

Enterprise risk management is not a function or department. It is the culture, capabilities, and practices that organizations integrate with strategy-setting and apply when they carry out that strategy, with the purpose of managing risk in creating, preserving, and realizing value.

» The key highlights from the Framework

The Framework is focused on five easy-to-understand components of risk management:



It also introduced 20 key principles that support each component within each of the five components



The New Framework (2017) itself is a set of principles organized into five interrelated components:

1. Governance and Culture: Governance sets the organization's tone, reinforcing the importance of, and establishing oversight responsibilities for, enterprise risk management. Culture pertains to ethical values, desired behaviors, and understanding of risk in the entity.



2. Strategy and Objective-Setting: Enterprise risk management, strategy, and objective-setting work together in the strategic-planning process. A risk appetite is established and aligned with strategy; business objectives put strategy into practice while serving as a basis for identifying, assessing, and responding to risk.



3. Performance: Risks that may impact the achievement of strategy and business objectives need to be identified and assessed. Risks are prioritized by severity in the context of risk appetite. The organization then selects risk responses and takes a portfolio view of the amount of risk it has assumed. The results of this process are reported to key risk stakeholders.



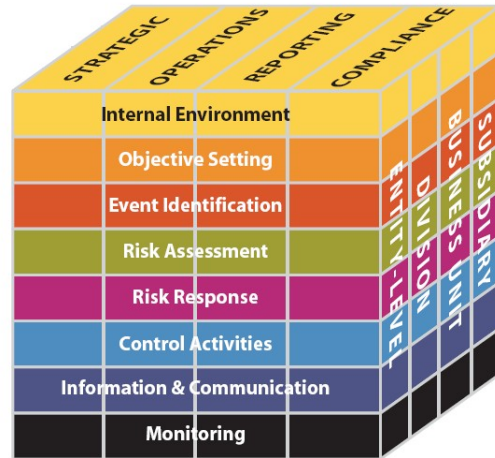
4. Review and Revision: By reviewing entity performance, an organization can consider how well the enterprise risk management components are functioning over time and in light of substantial changes, and what revisions are needed.



5. Information, Communication, and Reporting: Enterprise risk management requires a continual process of obtaining and sharing necessary information, from both internal and external sources, which flows up, down, and across the organization.

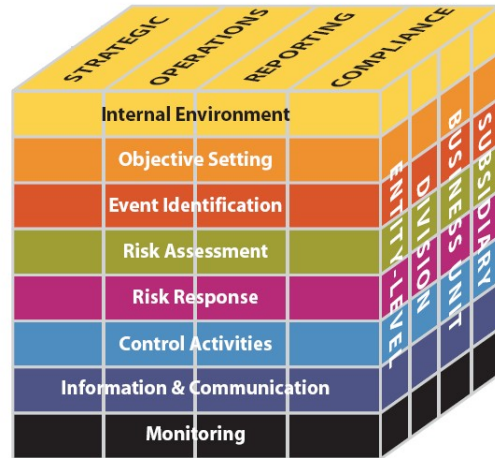


- COSO 2017 ERM Framework



- » Links between the ERM Framework update and COSO Internal Control – Integrated Framework
- » The document does not replace the Internal Control – Integrated Framework 2013
- » The two frameworks are distinct and complementary, with neither superseding the other
- » Both use a components and principles structure
- » Aspects of internal control common to enterprise risk management are not repeated

- COSO 2017 ERM Framework



- » Some aspects of internal control are developed further in this framework
- » Internal control is positioned within the Updated Document as a fundamental aspect of enterprise risk management.
- » The updated document will focus on requisite areas that go beyond internal control; however, the Internal Control–Integrated Framework remains a viable and suitable framework for designing, implementing, and conducting and assessing the effectiveness of internal control and for reporting, as required in some jurisdictions.



T.C.
MALİYE BAKANLIĞI
BÜTÇE VE MALİ KONTROL GENEL MÜDÜRLÜĞÜ



Kamu İç Kontrol Rehberi

Kontrol ortamı

Risk yönetimi

Kontrol faaliyetleri

Bilgi ve iletişim

İzleme

Bu rehber Avrupa Birliği tarafından finanse edilen TR07-IBFI-02 numaralı Eşleştirme Projesi kapsamında hazırlanmıştır.



VERSİYON 1.0



<http://www.idkk.gov.tr/Sayfalar/Mevzuat/Ucuncul%20Duzey%20Mevzuat/RiskDegerlendirmeRehberi.aspx>



References

- » *AKBAR, J., A new era in Risk Management: COSO ERM Framework 2017 Enterprise Risk Management–Integrating with Strategy and Performance*, https://www.linkedin.com/pulse/new-era-risk-management-coso-erm-framework-2017-javed?trk=portfolio_article-card_title
- » *COSO 2013*
- » *COSO Issues Important Update to ERM Framework First revision since 2004 addresses evolution of enterprise risk management*, <https://www.coso.org/Documents/COSO-Issues-Important-Update-to-ERM-Framework-September-2017.pdf>
- » *CHAMBERS, R., COSO ERM Update: A Vital Tool in 21st Century Risk Management*, <https://iaonline.theiia.org/blogs/chambers/2017/Pages/COSO-ERM-Update-A-Vital-Tool-in-21st-Century-Risk-Management.aspx>
- » *DIONNE, G., Risk Management; History, Definiton and Critique, CIRRELT, March, 2013*
- » *Enterprise Risk Management Integrating with Strategy and Performance Executive Summary*, <https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf>
- » *HILLSON, D., What is risk? Towards a common definition, InfoRM, Journal of the UK Institute of Risk Management, 2002*, www.theIRM.org
- » *HILLSON, D., Managing Risks in Projects, Gower Publishing, 2009*
- » *HOPKIN, P., Fundamentals of Risk Management; understanding, evaluating, and implementing effective risk management, 2010, Kogan Page Limited*
- » *Kamu İç Kontrol Rehberi*
- » *KARREN, H., Enterprise Risk Management, John Wiley and Sons, 2015*
- » *OBENG, S.G., (1997) Communication strategies: Persuasion and politeness in Akan judicial discourse. Text 17.1: 25-51*
- » *SCHNEIER, B., Information Security Magazine, October, 2008*
- » *All of the pictures and figures are obtained from various web sites, but the real sources could not be obtained for citation.*





Thank you for your kind attention....

