



مروری بر اصول و مبانی سیستم مدیریت ریسک سازمانی (ERM)

سخنران: محمود اسعد سامانی
PhD/ACII/AMII



بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ



پیشینه کارگاه

این دوره آموزشی، بخشی از یک دوره آموزشی جامع می‌باشد و هدف آن ارائه و ایجاد پایه‌ای محکم و مستدل برای درک و فهم اصول و مبانی و بهترین شیوه‌های مدیریت ریسک سازمانی (ERM) است. ظرف سال گذشته و سال جاری، این دوره آموزشی چندین بار در سازمان‌های مختلف برگزار گردیده و با استقبال و بازخورد خوبی مواجه شده است. در این دوره، از طریق طرح مباحث جدید، ارائه مطالعات موردی و مثال‌های کاربردی، شرکت‌کنندگان به درکی متفاوت و صحیح نسبت به برخی از موضوعات کلیدی مرتبط با سیستم مدیریت ریسک سازمانی دست می‌یابند. بنابراین، تجهیز شرکت‌کنندگان به دانش و ابزار لازم برای ارتقای قابلیت‌های مدیریت ریسک سازمانی و کمک به موفقیت کلی سازمان‌ها مد نظر است.



اطلاعات مدرس

الف) مشخصات فردی و مدارک تحصیلی

- محمود اسعد سامانی
- لیسانس مهندسی صنایع از دانشگاه صنعتی اصفهان
- فوق لیسانس مدیریت مهندسی از دانشگاه دولتی پوترای مالزی (UPM)
- دکترای تخصصی مهندسی صنایع از دانشگاه دولتی پوترای مالزی (UPM)
- مدرک عالی و حرفه‌ای بیمه موسوم به ACII از مؤسسه بیمه چارتر لندن (CII)
(مدرک حرفه‌ای ACII یکی از بالاترین مدارک بیمه‌ای دنیاست و در صنعت بیمه کشور معادل فوق لیسانس محسوب می‌شود)
- مدرک حرفه‌ای بیمه موسوم به Diploma in Insurance از مؤسسه بیمه چارتر لندن (CII)
- مدرک عالی و حرفه‌ای بیمه موسوم به AMII از مؤسسه بیمه مالزی (MII)



اطلاعات مدرس

(ب) اهم سوابق کاری

- ❑ بنیانگذاری، تأسیس و راهاندازی مرکز (ملی) توسعه مدیریت ریسک از طریق تهیه طرح توجیهی و تهیه و تدوین برنامه استراتژیک و پیاده‌سازی بخشی از اقدامات برنامه‌ریزی شده (زمستان ۱۳۹۹)
- ❑ تأسیس و راهاندازی اداره کل توسعه مدیریت ریسک بیمه مرکزی ج.ا.ایران (اردیبهشت ۱۳۹۶)
- ❑ همکاری با مؤسسه بیمه مالزی (MII) به عنوان مشاور مدیرعامل و برگزاری دوره‌های متعدد آموزش حرفه‌ای بیمه توسط اساتید این مؤسسه در دو کشور ایران و مالزی (برخی از این دوره‌ها مانند دوره آموزشی DMII پس از انقلاب اسلامی بی نظیر ارزیابی شده است)
- ❑ تدوین سیاستها، برنامه‌ریزی، برگزاری و ریاست اولین اجلاس سران بیمه‌ای کشورهای عضو اکو در حوزه بیمه ریسک بحران (آذر ۱۴۰۰)
- ❑ مدیرعامل و عضو هیأت مدیره شرکت گروه اقتصادی هورایزون در مالزی (۱۳۹۳ تا ۱۳۹۵)



بیان مسأله و ضرورت انجام کارگاه

لازمه **رهبری و هدایت** یک سازمان، ایجاد تفاوت و تمایز است. رهبران سازمان‌های قرن ۲۱ ام، چنانچه بخواهند تفاوتی به وجود آورند و سازمان خود را به سمت بزرگی هدایت کنند، باید قابلیت ناوبری سازمان خود در دنیایی که به شدت خطرناک و ریسکی است را داشته باشند. بنابراین، درک و فهم مدیریت ریسک برای رهبری و هدایت سازمان‌های امروزی بسیار حیاتی و ضروری است.



سوابق مطالعاتی و پژوهشی مربوطه

بنیان این دوره آموزشی بر پایه پژوهش‌ها و مطالعات قوی گذارده شده و کلیه مطالبی که ارائه می‌شود، از ادبیات شناخته شده موضوع و مراجع معتبر بین‌المللی تبعیت می‌کند. محتوای دوره با دقت و وسواس زیادی انتخاب و ساخته شده است.

توسعه این دوره آموزشی شامل بررسی چارچوب‌ها و استانداردهای مربوطه، مانند مستندات COSO ERM 2017 و ISO 31000:2018، همراه با بررسی مطالعات موردی صنایع مختلف بوده و گزارشات فنی و به روز رسانی‌های در حال ظهور در زمینه مدیریت ریسک سازمانی تا جایی که در دسترس بوده، به طور مداوم مورد پیگیری و بررسی قرار گرفته تا اطمینان حاصل شود که محتوای دوره مرتبط و همسو با نیازهای در حال تحول سازمان‌ها می‌باشد.



1. Nature and impact of risk (*strategic, tactical, operational*)
 - Definition of risk
 - Recording risk assessment
 - Risk classification systems
2. Principles of risk management
 - Context for risk management
 - Risk aware culture
 - **Risk management process**



فرآیند مدیریت ریسک

1. Recognition or identification of risk
2. Ranking or evaluation of risk
3. Responding (treatment) to significant risk
 - *Tolerate/accept*
 - *Treat/mitigation*
 - *Transfer*
 - *Terminate/avoid*
 - *Take the opportunity*
4. Resourcing controls
5. Reaction planning
6. Reporting and monitoring risk performance
7. Reviewing the risk management framework

Risk architecture

- Risk architecture specifies the roles, responsibilities, communication and risk reporting structure

Risk strategy

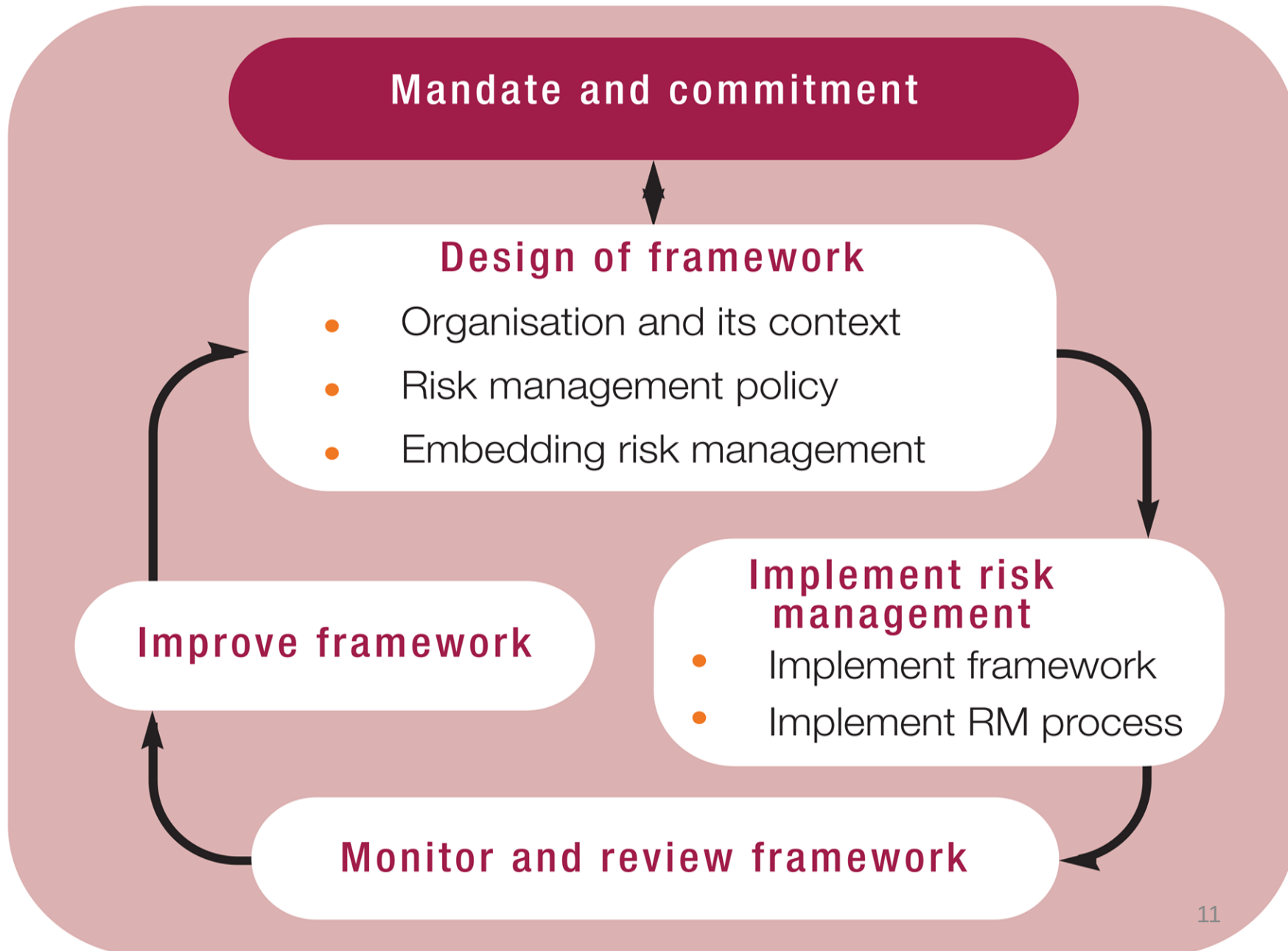
- Risk strategy, appetite, attitudes and philosophy are defined in the Risk Management Policy

Risk management process

Risk protocols

- Risk protocols are presented in the form of the risk guidelines for the organisation and include the rules and procedures, as well as specifying the risk management methodologies, tools and techniques that should be used

Framework for managing risk (based on ISO 31000)





بیشتر بدانیم ...

برای اطلاعات بیشتر در این خصوص، مستند زیر را مطالعه نمایید:

**A-Structured-Approach-to-ERM-
1683403478.pdf**





فهرست مطالب

۱. مقدمه ای بر اصطلاحات و مفاهیم مدیریت ریسک
۲. استانداردها و چارچوب های مدیریت ریسک (به عنوان مثال: ISO 31000، COSO ERM، ...)
۳. تکنیک ها و ابزارهای شناسایی ریسک
۴. روش های ارزیابی ریسک، از جمله رویکردهای کیفی و کمی
۵. اشتباهات ریسک و حد تحمل
۶. استراتژی ها و گزینه های مواجهه / رفتار با ریسک
۷. نظارت بر ریسک، گزارش دهی و ارتباطات
۸. یکپارچه سازی مدیریت ریسک در فرآیندهای تصمیم گیری
۹. مدیریت ریسک در برنامه ریزی، پیش بینی، بودجه بندی، ساخت و ساز، سرمایه گذاری و مدیریت عملکرد
۱۰. توسعه فرهنگ ریسک و مدیریت تغییر سازمانی
۱۱. نقش ها و مسئولیت های مدیریت ریسک در یک سازمان
۲۱. ابزارهای مدیریت ریسک و راه حل های نرم افزاری
۳۱. مطالعات موردی و نمونه هایی از اجرای موفق مدیریت ریسک
۴۱. خطرات و روندهای نوظهور در مدیریت ریسک
۵۱. جنبه های نظارتی و انطباقی مدیریت ریسک



مقدمه ای بر اصطلاحات و مفاهیم مدیریت ریسک

- مدیریت ریسک دارای **مفاهیم** اساسی و مهمی است؛
- واژگان خاصی دارد؛
- درک این مفاهیم، **پیشنیاز موفقیت** در پیاده سازی مدیریت ریسک است؛
- عدم درک صحیح این مفاهیم، باعث می شود که مدیریت ریسک به درستی درک نشود؛
- **مدیریت ریسک نیازمند یک سیستم مدیریت ریسک (RMS) یا (ERM) است؛**
- **مدیریت ریسک یک سیستم مدیریتی مستقل و جداگانه نیست؛**
- **مدیریت ریسک نیازمند "یکپارچه سازی یا نهادینه سازی (Integration/Embedment)" است؛ و**
- ...



مقدمه ای بر اصطلاحات و مفاهیم مدیریت ریسک

مرجع استاندارد اصطلاحات و مفاهیم مدیریت ریسک:

ISO 31073:2022(en) Risk management — Vocabulary

Table of contents:

- Foreword
- Introduction
- Scope
- Normative references
- Terms and definitions:
 - ☐ Terms related to risk
 - ☐ Terms related to risk management
 - ☐ Terms related to the risk management process
- Bibliography
- Index





واژگان مربوط به ریسک

3.1.1

risk

effect of [uncertainty \(3.1.3\)](#) on [objectives \(3.1.2\)](#)

Note 1 to entry: An effect is a deviation from the expected. It can be positive, negative or both, and can address, create or result in [opportunities \(3.3.23\)](#) and [threats \(3.3.13\)](#).

Note 2 to entry: Objectives can have different aspects and categories, and can be applied at different levels.

Note 3 to entry: Risk is usually expressed in terms of [risk sources \(3.3.10\)](#), potential [events \(3.3.11\)](#), their [consequences \(3.3.18\)](#) and their [likelihood \(3.3.16\)](#).





واژگان مربوط به ریسک

3.1.2

objective

result to be achieved

Note 1 to entry: An objective can be strategic, tactical or operational.

Note 2 to entry: Objectives can relate to different disciplines (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process).

Note 3 to entry: An objective can be expressed in other ways, e.g. as an intended outcome, a purpose, an operational criterion, as a management system objective, or by the use of other words with similar meaning (e.g. aim, goal, target).

3.1.3

uncertainty

state, even partial, of deficiency of information related to understanding or knowledge

Note 1 to entry: In some cases, uncertainty can be related to the [organization's \(3.3.7\)](#) context as well as to its [objectives \(3.1.2\)](#).

Note 2 to entry: Uncertainty is the root source of [risk \(3.1.1\)](#), namely any kind of “deficiency of information” that matters in relation to objectives (and objectives, in turn, relate to all relevant [interested parties' \(3.3.2\)](#) needs and expectations).





3.2.1

risk management

coordinated activities to **direct**
and control

an **organization (3.3.7)** with
regard to **risk (3.1.1)**





واژگان مربوط به مدیریت ریسک

3.2.2

risk management policy

3.2.3

risk management plan





واژگان مربوط به فرآیند مدیریت ریسک

3.3.1

risk management process

systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, [monitoring \(3.3.40\)](#) and reviewing [risk \(3.1.1\)](#)

3.3.2

interested party

stakeholder

person or [organization \(3.3.7\)](#) that can affect, be affected by, or perceives itself to be affected by a decision or activity





واژگان مربوط به فرآیند مدیریت ریسک

3.3.3

risk perception

3.3.4

external context

3.3.5

internal context

3.3.6

risk criteria

3.3.7

organization

3.3.8

risk assessment

3.3.9

risk identification

**33 more vocabulary and their definition from
3.3.10 up to 3.3.43**





بیشتر بدانیم ...

- ✓ تفاوت استاندارد ایزو ۳۷۰۷۳ با ایزو ۷۳ ([این فایل را ببینید](#))
- ✓ تعاریف مفاهیم و واژگانی مانند شرح ریسک، چارچوب مدیریت ریسک، ماتریس ریسک، پروفایل ریسک و فهرست عناوین ریسک در استاندارد نسخه ۲۰۲۲ حذف شده اند. چرا؟!
- ✓ تعاریف و واژگان مدیریت ریسک بر اساس مستند COSO ERM 2017





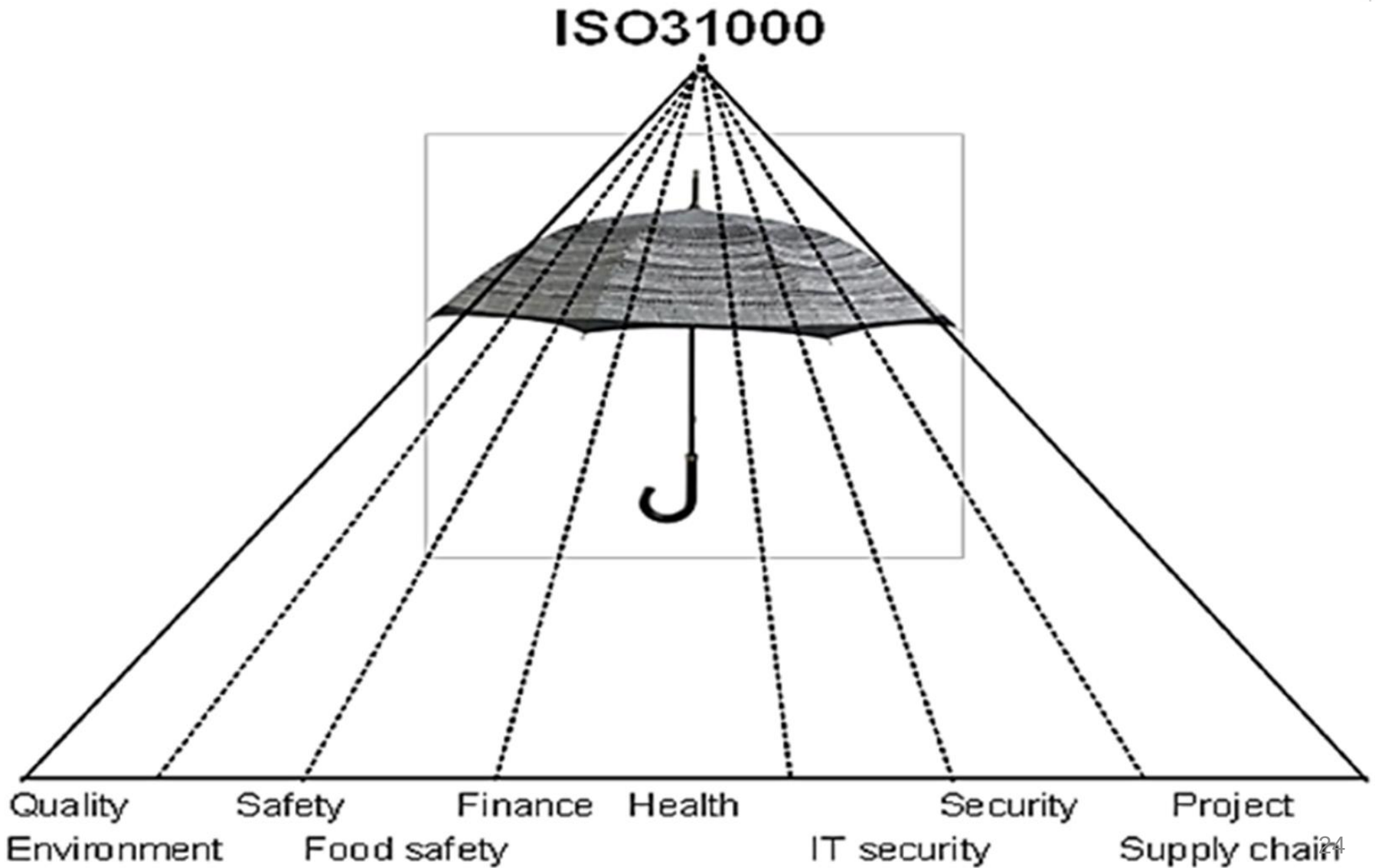
مدیریت ریسک و آینده‌نگری / آینده‌نگاری

- Dealing with the proliferation of data
- Leveraging artificial intelligence and automation
- Managing the cost of risk management
- Building stronger organizations





چتر گسترده سیستم مدیریت ریسک (ISO 31000)





ریسک، تغییر و عملکرد

We live in an **ever-changing** world where we are forced to deal with **uncertainty** every day.

But how an organization tackles that uncertainty can be a key predictor of its **success**.

در دنیایی زندگی می کنیم که هر لحظه در حال **تغییر** است و مجبوریم هر روز با **نااطمینانی و عدم قطعیت** مواجه شویم. اما، روش سازمان در رویارویی با عدم قطعیت، می تواند رمز **موفقیتش** باشد.





دلایل اهمیت و ضرورت مدیریت ریسک

- عدم اطمینان (Uncertainty) در تعریف و تحقق **اهداف** سازمان ها؛
- شدت **رقابت** ها؛
- تغییر **پارادایم** ها و **رویکردها**؛
- تغییر **بستر قوانین و مقررات** و الزامات محیط کسب و کار؛
- وجود **چالش های** اساسی و متعدد در اداره شرکت ها و سازمان ها.

برای اعمال مدیریت مؤثر بر این **چالشها**، رویکردهای نوین مدیریت مطرح شده است. **شناسایی، کنترل و مدیریت ریسک** ها یکی از این رویکردهای جدید است که برای تقویت و ارتقای **اثربخشی و کارایی** سازمانها مورد استفاده قرار می گیرد.





مشکلات و دغدغه هایی که سازمان های امروزی با آنها مواجهند

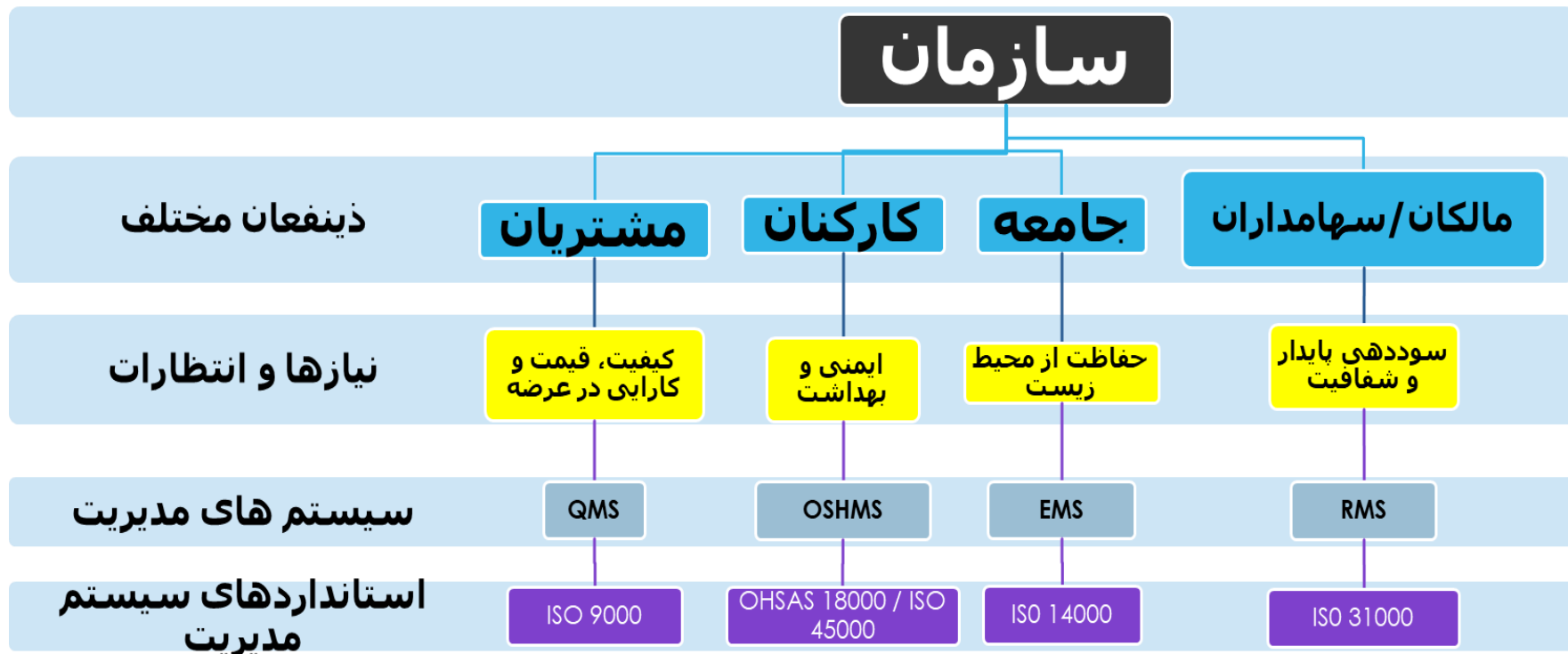


- Quality, S&H, Environment, Risk, Customer Relationship, etc.;
- These issues all require systematic approaches and procedures and must be managed; i.e.: they require **Management Systems (MSs)**.





دینفعان سازمان و نیازها و انتظارات آنها

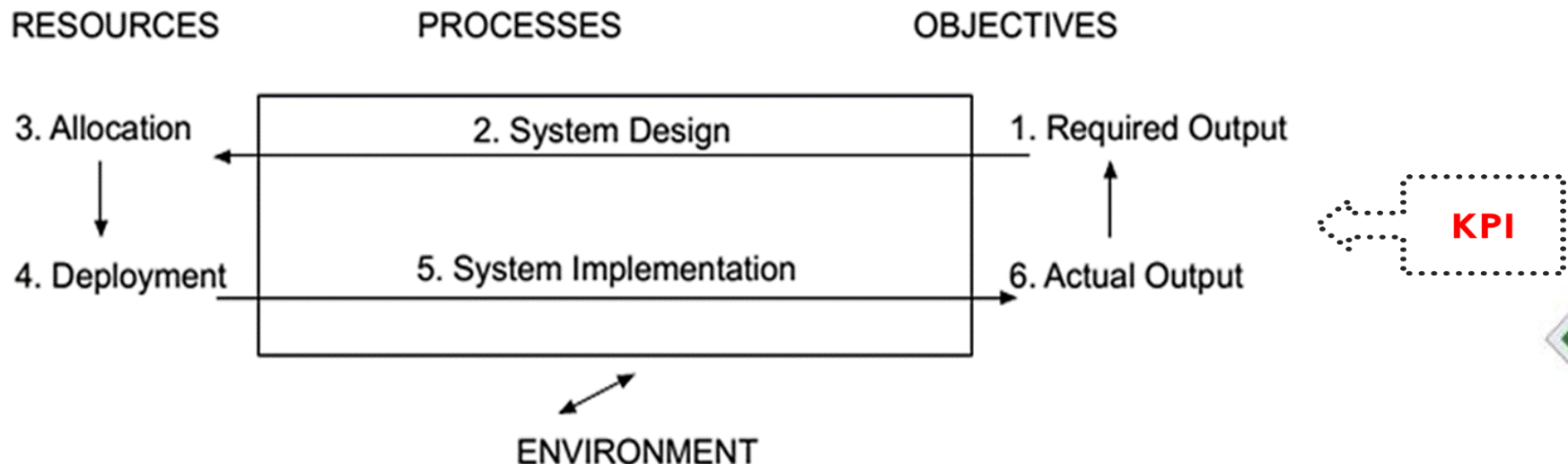


The main objective of each MSS is to systematically guide an organization **to satisfy each specific group of stakeholders and to supply their needs and expectations.**



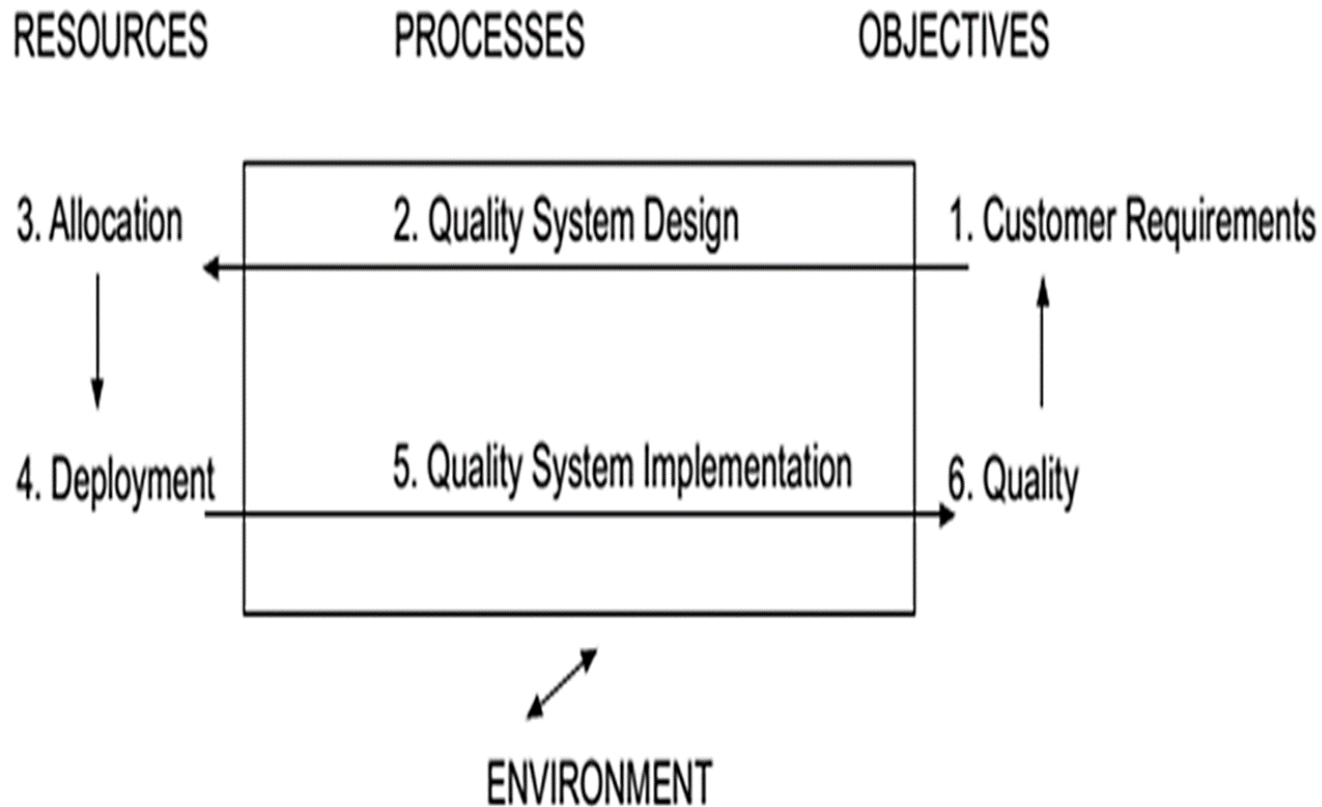
تعریف سیستم مدیریت

- As per ISO, **Management System** is defined as: *the set of procedures an organization needs to follow in order to meet its objectives*; سیستم مدیریت عبارتست از مجموعه روشهایی که سازمان باید دنبال کند تا به اهدافش برسد
- System design and process approach.*





شمای کلی سیستم مدیریت کیفیت





تعدادی از معروف ترین استانداردهای سیستم های مدیریتی سازمان ISO

- **ISO 9001:2015 – Quality Management Systems**
- ISO 14001:2014 – Environmental Management Systems
- ISO 45001:2018 – Occupational Health and Safety Management Systems

- **ISO 31000:2018 – Risk Management - Principles and Guidelines**

- ISO Guide 37073:2022 – Risk Management – Vocabulary

- ISO 27001:2005 – Information Security Management Systems
- ISO 22000:2005 – Food Safety Management Systems
- ISO 50001:2011 – Energy Management Systems
- ISO 26000:2010 – Guidance On Social Responsibility





استانداردها و چارچوب‌های مدیریت ریسک

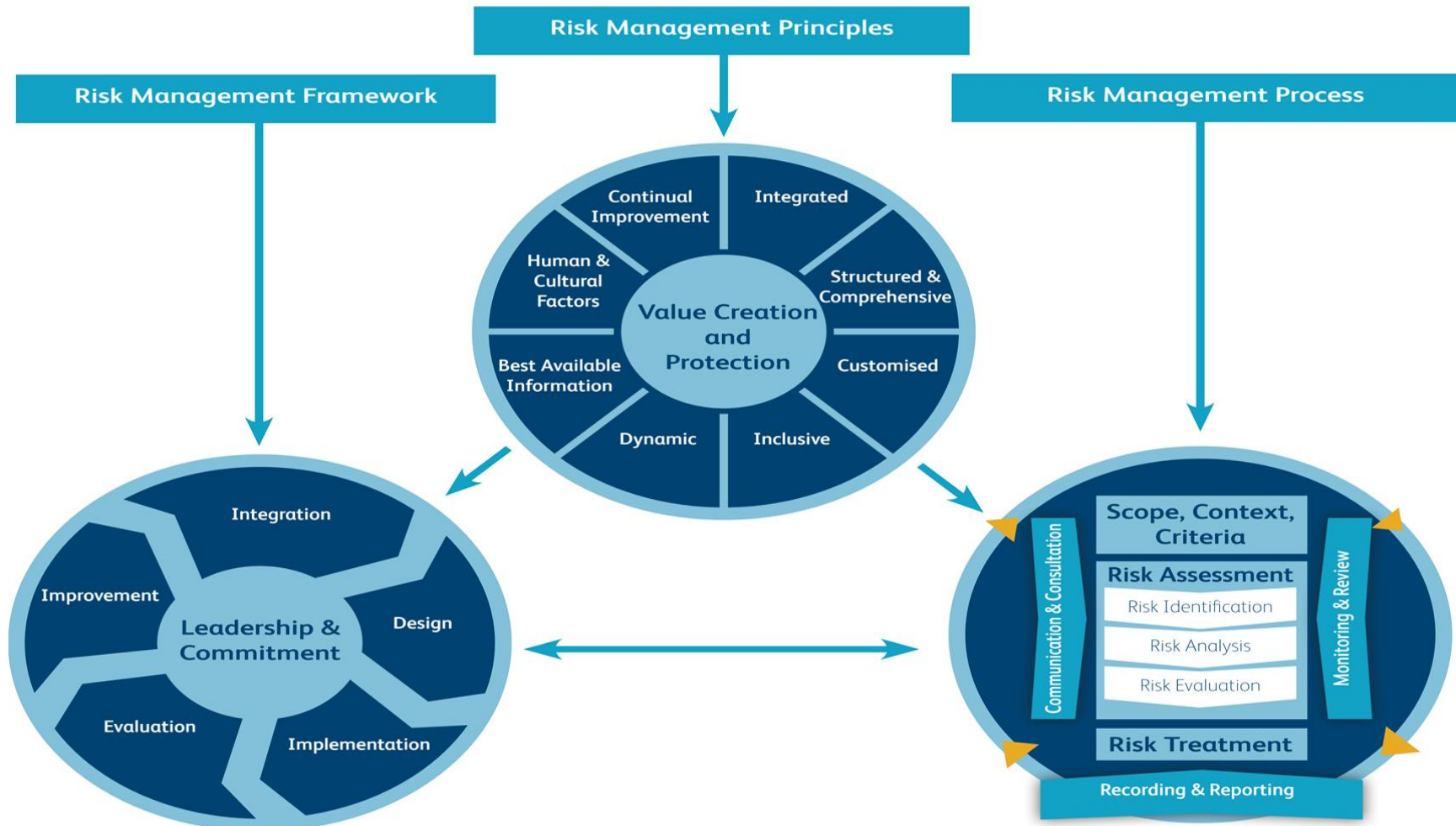
- There are many recommended approaches to risk management (RM) and several different guides and risk management frameworks and standards have been published:
 - [ISO 31000:2018 - Risk Management – Guidelines](#)
 - ISO 37073:2022 – Risk Management – Vocabularies
 - COSO ERM 2017 – Integrating with Strategy and Objectives





ISO 31000:2018 – Risk Management – Guidelines

Figure 3: Principles, framework and risk management process from ISO 31000





COSO ERM 2017 – Integrating Strategy with Performance

Our understanding of the nature of risk, the art and science of choice, lies at the core of our modern economy. Every choice we make in the pursuit of objectives has its risks. From day-to day operational decisions to the fundamental trade-offs in the boardroom, dealing with risk in these choices is a part of decision-making.

درک ما از ماهیت ریسک و هنر و علم انتخاب و تصمیم گیری، هسته اصلی اقتصاد مدرن را تشکیل می‌دهد. هر انتخابی که برای دستیابی به اهداف انجام می‌دهیم، ریسک‌های خود را دارد. از تصمیمات عملیاتی روزانه گرفته تا مبادلات اساسی در اتاق هیئت مدیره، مقابله با ریسک در این انتخاب‌ها بخشی از تصمیم گیری است.





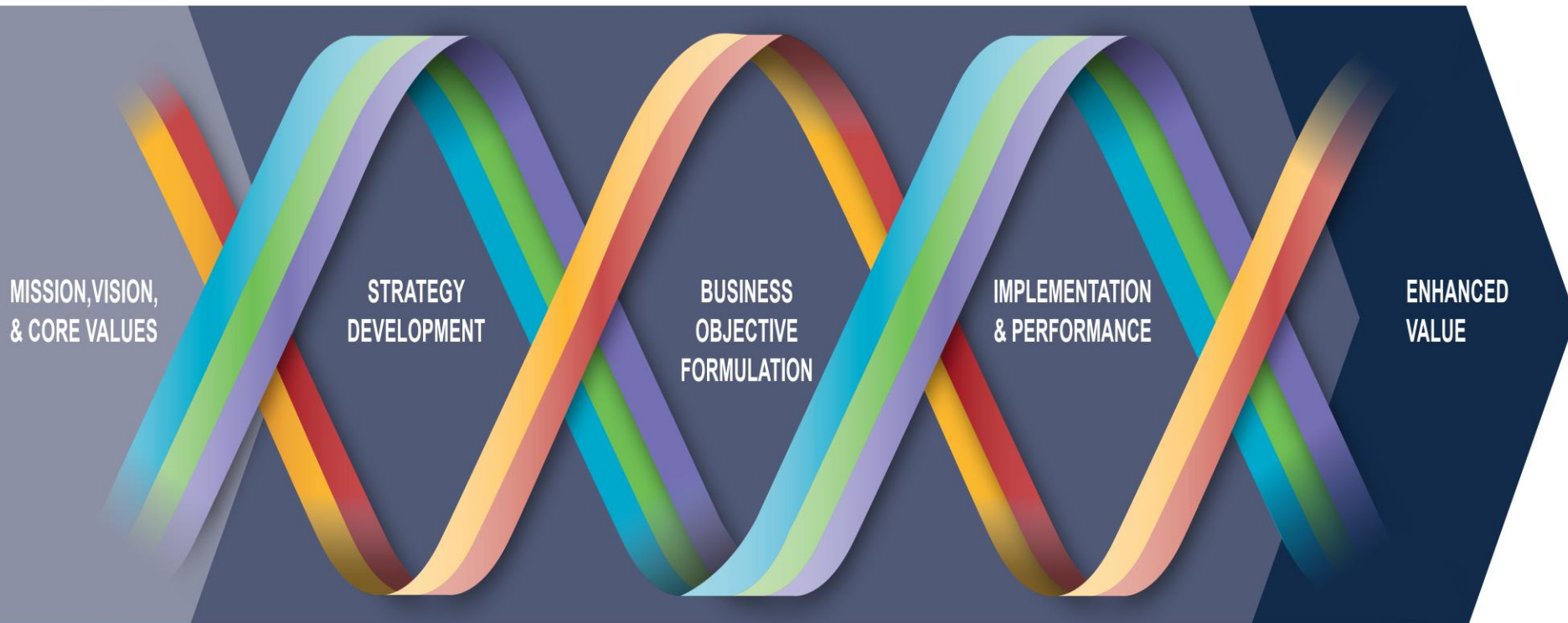
COSO ERM 2017 – Integrating Strategy with Performance





COSO ERM 2017 – Integrating Strategy with Performance

ENTERPRISE RISK MANAGEMENT



Governance
& Culture



Strategy &
Objective-Setting



Performance



Review
& Revision



Information,
Communication,
& Reporting



COSO ERM 2017 – Integrating Strategy with Performance



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



- استاندارد مرجع:

[IEC 31010:2019](#)

Risk Management – Risk Assessment Techniques

- ۱۰ دسته و مجموعاً ۴۲ تکنیک شناسایی و ارزیابی ریسک (کیفی و کمی)





- Brainstorming
- Delphi technique
- Nominal group technique
- Structured and semi-structured interviews
- Surveys





تکنیک‌هایی برای شناسایی ریسک

- Checklists, classifications and taxonomies
- Failure modes and effects analysis (FMEA) and failure modes, effects and criticality analysis (FMECA)
- Hazard and operability (HAZOP) studies
- Scenario analysis
- Structured what if technique (SWIFT)

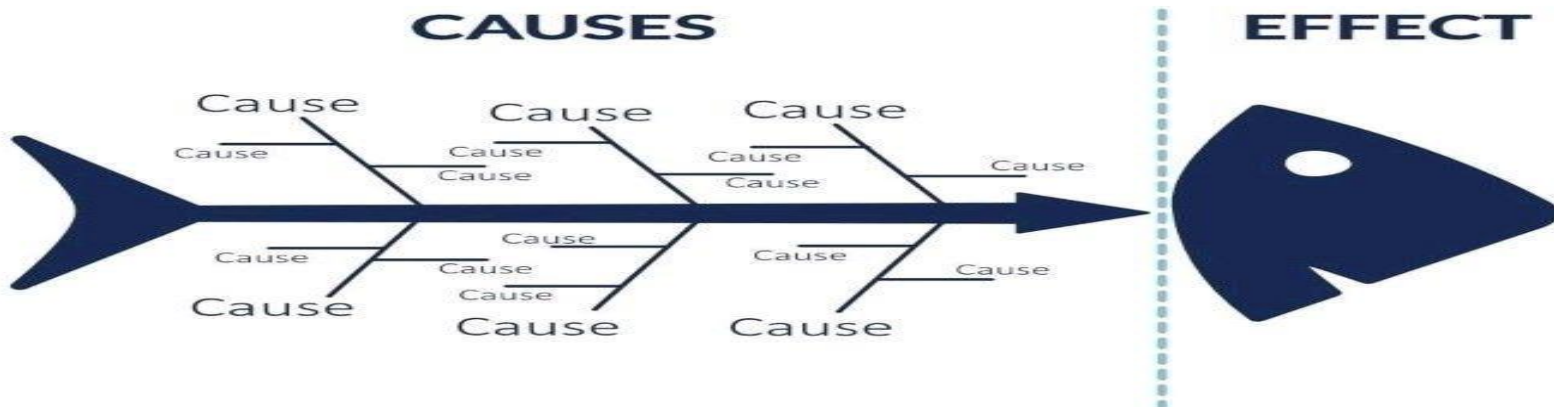




تکنیک هایی برای تعیین منابع، علل و عوامل ریسک

- Cindynic approach
- Ishikawa analysis (fishbone) method

ROOT CAUSE ANALYSIS FISHBONE METHOD



Use this method to visualize the brainstorming of potential root causes.





تکنیک‌هایی برای تجزیه و تحلیل کنترلرها

- Bow-tie analysis
- Hazard analysis and critical control points (HACCP)
- Layers of protection analysis (LOPA)





تکنیک‌هایی برای فهم پیامدها و احتمالات

- Bayesian analysis
- Bayesian networks and influence diagrams
- Business impact analysis (BIA)
- Cause-consequence analysis (CCA)
- Event tree analysis (ETA)
- Fault tree analysis (FTA)
- Human reliability analysis (HRA)
- Markov analysis
- **Monte Carlo simulation**
- Privacy impact analysis (PIA) / data protection impact analysis (DPIA)





تکنیک‌هایی برای تجزیه و تحلیل وابستگیها و تعاملات

- Causal mapping
- Cross impact analysis





تکنیک های اندازه گیری ریسک

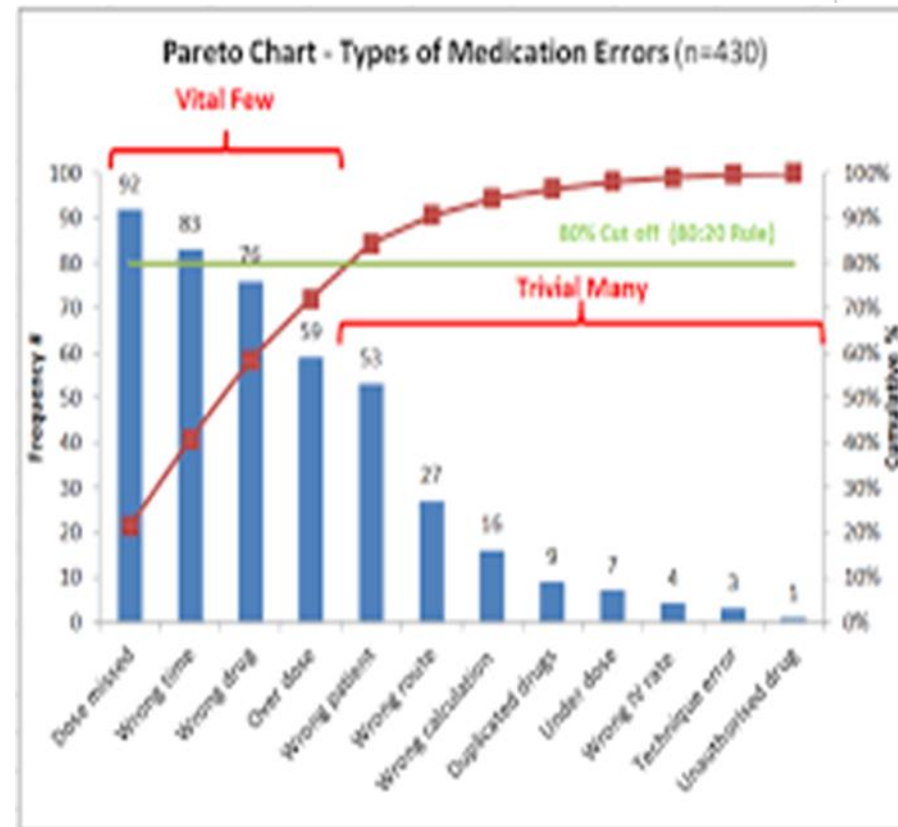
- Toxicological risk assessment
- Value at risk (VaR)
- Conditional value at risk (CVaR) or expected shortfall (ES)





تکنیک‌هایی برای ارزیابی اهمیت ریسک

- As low as reasonably practicable (ALARP) and so far as is reasonably practicable (SFAIRP)
- Frequency-number (F-N) diagrams
- Pareto charts
- Reliability centred maintenance (RCM)
- Risk indices





تکنیک‌هایی برای انتخاب بین گزینه‌ها

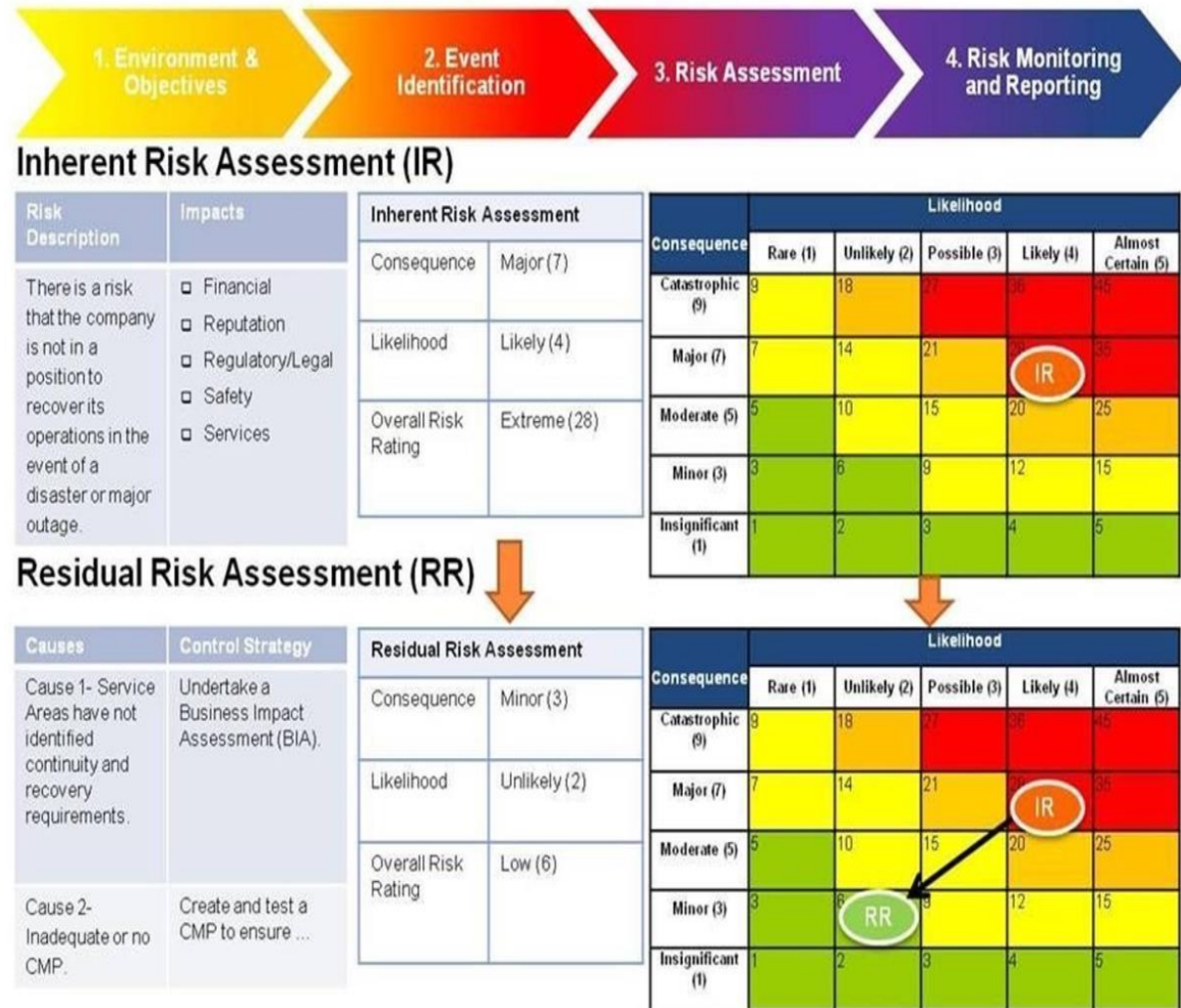
- Cost/benefit analysis (CBA)
- Decision tree analysis
- Game theory
- Multi-criteria analysis (MCA)





تکنیک های برای ثبت و گزارش دهی

- Risk registers
- **Consequence/likelihood matrix (risk matrix or heat map)**
- S-curves





روند تکنیک‌های شناسایی و ارزیابی ریسک

مشاوره و
ارتباطات

تجزیه و
تحلیل
وابستگیها و
تعاملات

اندازه‌گیری
ریسک



شناسایی
ریسک

فهم پیامدها و
احتمالات

ارزیابی
اهمیت
ریسک



تعیین منابع،
علل و عوامل
ریسک



تجزیه و
تحلیل کنترلرها

انتخاب بین
گزینه‌ها



ثبت و
گزارش
دهی



تکنیک های ضروری برای یادگیری و استفاده

- **Monte Carlo simulation**
- Decision tree
- Risk return spectrum
- Scenario analysis
- Business impact analysis
- PERT
- Sensitivity analysis
- Lessons learned
- Data analysis
- Horizon scanning
- ...





با سپاسی از شما

