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

سخنران: محمود اسعد سامانی
PhD/ACII/AMII

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 مثال های کاربردی، شرکت کنندگان به درکی متفاوت و صحیح نسبت به برخی از موضوعات کلیدی مرتبط با سیستم مدیریت ریسک سازمانی دست می‌یابند.

بنابراین، تجهیز شرکت کنندگان به دانش و ابزار لازم برای ارتقای قابلیت‌های مدیریت ریسک سازمانی و کمک به موفقیت کلی سازمان‌ها مد نظر است.

اطلاعات مدرس و همکاران

الف) مشخصات فردی و مدارک تحصیلی

- محمود اسعد سامانی
- لیسانس مهندسی صنایع از دانشگاه صنعتی اصفهان
- فوق لیسانس مدیریت مهندسي از دانشگاه دولتي پوترای مالزی (UPM)
- دکترای تخصصی مهندسی صنایع از دانشگاه دولتي 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 و همکاران

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، برگذاری و ریاست اوّلین 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

بنیاد 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 ساخته شده است.

توسعه این دوره آموزشی شامل بررسی کامل 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.

بسم الله الرحمن الرحیم

آشنایی با سیستم مدیریت ریسک سازمانی (ERM)

ارائه دهنده:
محمود اسعد سامانی *PhD/ACII/AMII*

حاکمیت/حکمرانی شرکتی

رویکرد نهادینه / یکپارچه به مدیریت ریسک هسته مرکزی حاکمیت شرکتی خوب (good governance) را تشکیل می دهد.

مقررات حاکمیت شرکتی و نهادهای ناظر مربوطه، مدیریت ریسک را در قلب و مرکز حاکمیت شرکتی قرار می‌دهند.

مدیریت ریسک باید با حاکمیت شرکتی در یک چارچوب واحد برای هر سازمانی که توسط هیئت مدیره یا سایر نهادهای حاکمیتی نظارت می شود، ادغام/یکپارچه‌سازی شود. هیئت مدیره باید یک فرآیند ساختارمند و مستمر برای شناسایی، مدیریت و پاسخگویی به ریسک ایجاد کند.

Governance Institute of Australia, 2022 *"Risk Management for Directors - A Guide."*

تفاوت حاکمیت با مدیریت

- **حاکمیت** مسیر حرکت سازمان را نشان داده، روابط بیرونی و درونی آن و وظایف، فرآیندها و روش‌های مورد نیاز برای رسیدن به اهداف را تعیین می‌کند.
- **ساختارهای مدیریتی** جهت‌گیری/سیاست‌گذاری تعیین شده توسط حاکمیت را به استراتژی و اهداف مربوطه تبدیل کرده، تا سطوح پایدار و مورد انتظار عملکردی و ماندگاری بلند مدت سازمان، حاصل شود.
- تعیین وظایف پاسخگویی و نظارت مربوط به مدیریت ریسک در یک سازمان، بخش جدایی ناپذیر حاکمیت سازمانی است.

- **Governance** guides the course of the organization, its external and internal relationships, and the rules, processes and practices needed to achieve its purpose.
- **Management structures** translate governance direction into the strategy and associated objectives required to achieve desired levels of sustainable performance and long-term viability.
- Determining risk management accountability and oversight roles within an organization are integral parts of the organization's governance.

Source: ISO 31000:2018; Clause 5.3 "Integration"

درباره حاکمیت شرکتی (با رویکرد شرکت‌های بیمه)

- آیین‌نامه ۹۳ شورایعالی بیمه (بدون تعریف حاکمیت شرکتی)
- دستورالعمل ماده ۱۱ آیین‌نامه ۹۳
- اصل بنیادین شماره ۷ انجمن بین‌المللی ناظران بیمه‌ای (IAIS - ICP7)

حاکمیت شرکتی (ICP 7):
ناظر از بیمه‌گران می‌خواهد که چارچوب حاکمیت شرکتی را ایجاد و اجراء کنند تا بتوانند [امکان] مدیریت و نظارت **دقیق و سنجیده** بر کسب و کار بیمه‌گری را فراهم کرده و به نحو مناسب منافع بیمه‌گذاران را شناسایی و از آن محافظت نمایند.

ICP 7 Corporate Governance
The supervisor requires insurers to establish and implement a corporate governance framework which provides for **sound and prudent** management and oversight of the insurer's business and adequately recognises and protects the interests of policyholders.

International Association of Insurance Supervisors 2019

ریسک و مدیریت ریسک چیست؟

- **ریسک‌پذیری کاری است که سازمان‌ها انجام می‌دهند – این بخشی از هر تصمیمی است که یک سازمان می‌گیرد.**
- **تعریف ریسک:** *"اثر عدم قطعیت بر اهداف"* (ISO Guide 31073:2022)
- **تعریف مدیریت ریسک:** *"فعالیت های هماهنگ شده برای* ***هدایت*** *و* ***کنترل*** *یک سازمان با توجه به ریسک"* (ISO Guide 31073:2022)

نقش کلیدی مدیریت ریسک در سازمان

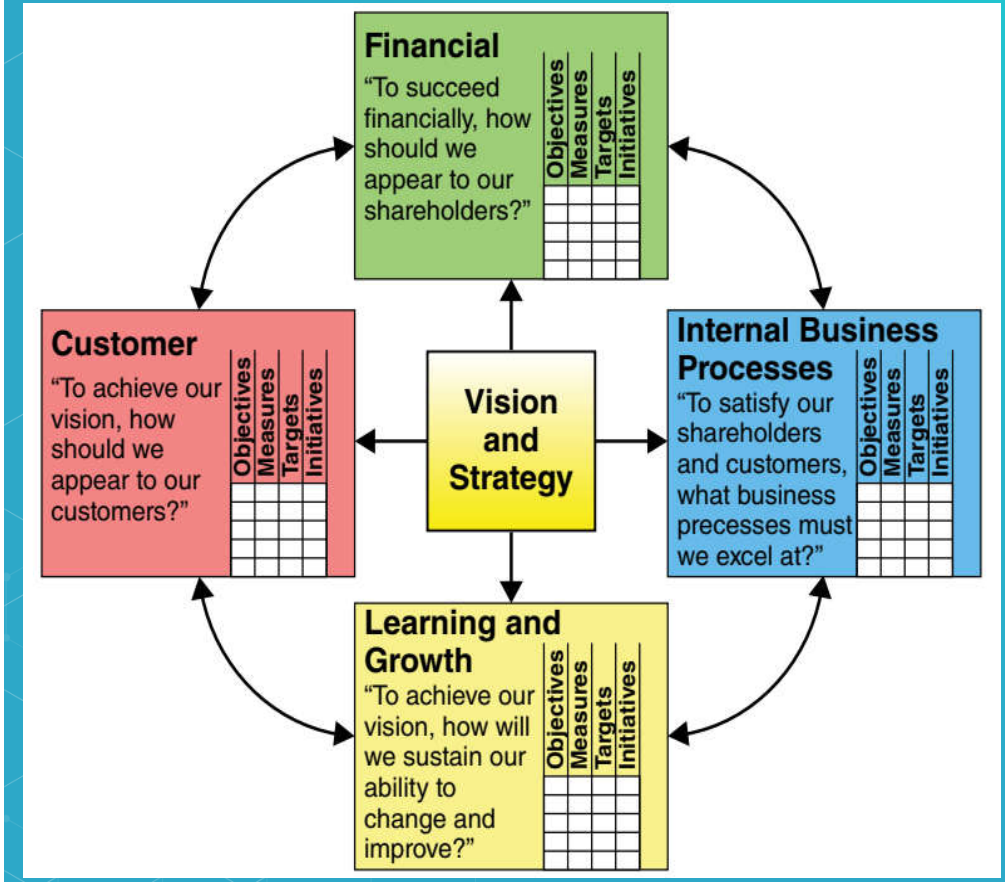
انواع ریسک (فهرست کامل نیست)

1. Financial Risk
2. Operational Risk
3. Cybersecurity Risk
4. Strategic Risk
5. Compliance Risk
6. Reputational Risk
7. Market Risk
8. Legal Risk
9. Human Resources Risk
10. Supply Chain Risk
11. Environmental Risk
12. Technology Risk
13. Political Risk
14. Economic Risk
15. Natural Disaster Risk

- طبقه بندی استانداری برای انواع ریسک وجود ندارد.

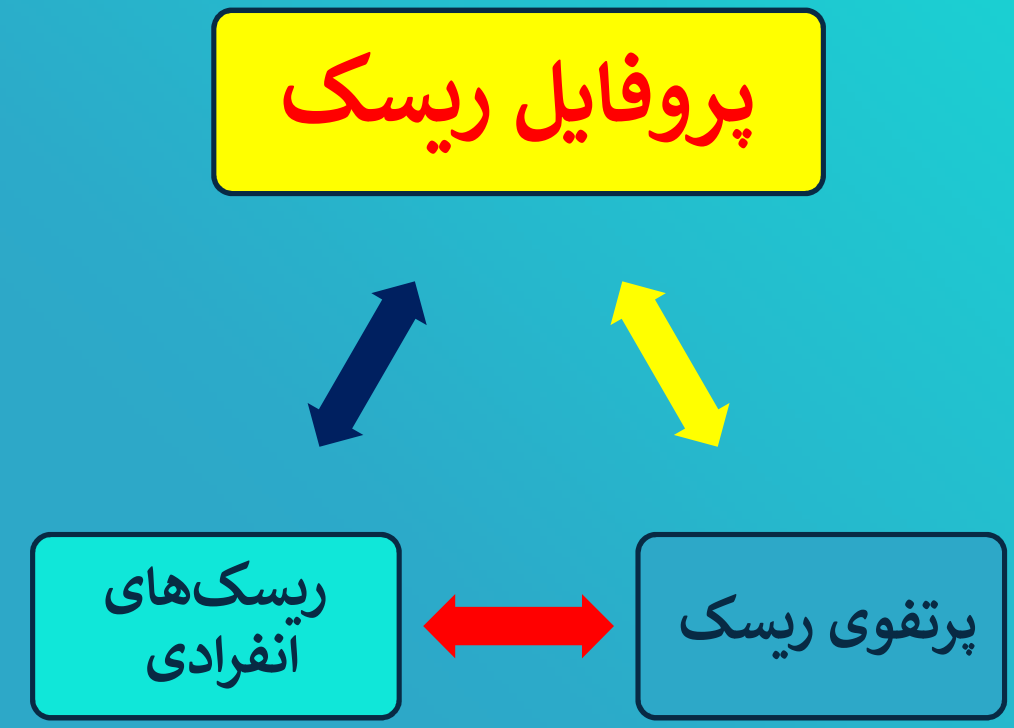
(این سایت را ملاحظه نمایید: **www.52risks.com**)

رویکرد به مدیریت ریسک: سیلویی یا کل نگر (ERM)

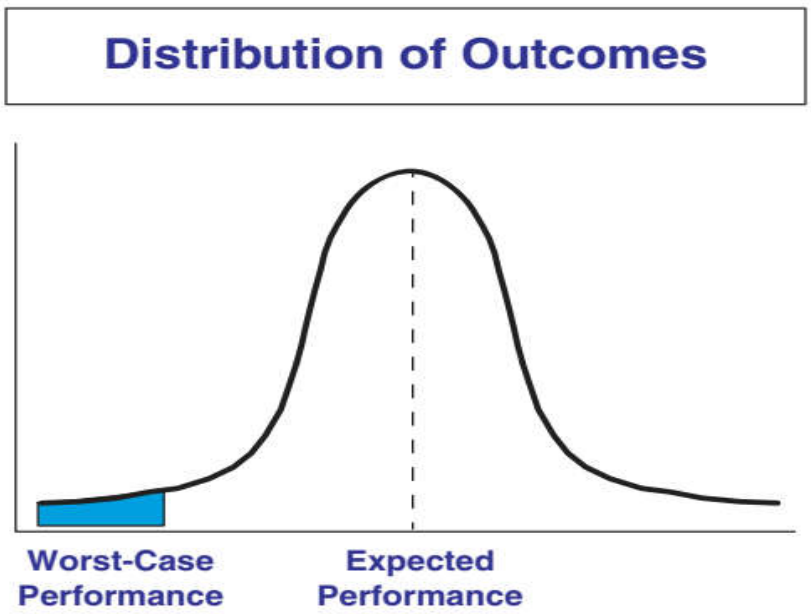


- اصول بنیادین بیمه ای ۸ و ۱۶ (ICPs 8 & 16) از مجموعه IAIS 2019
- تأکید بر نگاه کل نگر (Holistic) به مدیریت ریسک در قالب ERM به جای جزءنگری (رویکرد سیلویی)
- تمرکز بر استراتژی و پروفایل ریسک سازمان
- تعریف شاخص‌های کلیدی ریسک (KRI)
- تجزیه و تحلیل برنامه راهبردی سازمان با استفاده از تکنیک هایی نظیر BSC، PEST(LE)، SWOT، CSFs، ...

سطوح مدیریت ریسک سازمانی



عوامل مؤثر بر پروفایل ریسک سازمان



Risk is a variable that can cause deviation from an expected outcome, and as such may affect the achievement of business objectives and the performance of the overall organization.

- **درک کامل مفهوم پروفایل ریسک سازمان مستلزم درک موارد هفتگانه زیر است:**
  - میزان در معرض (مخاطره) بودن (Exposure)؛
  - میزان نوسان و ناپایداری (Volatility)؛
  - **احتمال (Probability)؛**
  - **شدت (Severity)؛**
  - افق زمانی (Time Horizon)؛
  - همبستگی (Correlation)؛
  - سرمایه (Capital).

ریسک متغیری است که می‌تواند باعث انحراف از آنچه که مورد انتظار است، شده و بدین ترتیب بر تحقق اهداف کسب و کار و عملکرد کلی سازمان تأثیر بگذارد.

در معرض (مخاطره) بودن (Exposure)

- **حداکثر خسارت اقتصادی ناشی از یک رویداد؛**
- **خسارت در شکل مالی یا آبرو و شهرت سازمان؛**
- **هرچه exposure بیشتر شود، ریسک نیز بیشتر می شود؛**
  - مثال (ریسک اعتباری): هر چقدر یک قرض دهنده وام بیشتری به قرض گیرنده بدهد، با exposure بیشتری از ناحیه وام‌گیرنده مواجه است؛
- **اندازه گیری exposure خصوصاً برای ریسک های بازار و اعتبار دشوار است؛**
- **برای ریسک‌های operational و compliance بیشتر کیفی اندازه گیری می‌شود؛**
- **اندازه گیری exposure منجر به سناریوی بدترین حالت ممکن می‌شود؛**
  - **MPL یا EML در بیمه برای عوامل خطر مهم (dominated perils)، معمولاً آتشسوزی، سیل، سرقت، ...**

نوسان و ناپایداری (Volatility)

- **معیاری است برای عدم قطعیت (Uncertainty)؛**
- **میزان تغییرپذیری و نوسان پیشامدهای بالقوه را نشان می دهد؛**
- **به طور مشخص، اندازه وجه مثبت و منفی ریسک پذیرفته شده را نشان می‌دهد؛**
- **هر چه Volatility بیشتر باشد، ریسک بزرگتر است؛**
  - **مثال (ریسک اعتباری):** تعداد موارد نکول (عدم بازپرداخت) در کارت‌های اعتباری به مراتب بیشتر از همین موارد در اعتبار (وام) خرید املاک است؛
  - میزان Volatility نکول اعتبار (وام) املاک از کارت های اعتباری بیشتر است؛

احتمال

- **هر چه وقوع رویدادی محتمل تر باشد (احتمالش بزرگتر باشد)، ریسک آن رویداد بزرگ تر است؛**
- **نوسانات نرخ بهره و تورم و نکول کارت‌های اعتباری، رویدادهای محتمل بوده و نیاز به آمادگی دارند؛**
- **ریسک حمله سایبری به یک مرکز داده (data center) مدرن به نسبت ریسک آتش‌سوزی آن مرکز محتمل‌تر است؛**
  - در صورت آتش سوزی مرکز داده، خسارت وارده سنگین‌تر خواهد بود؛
  - اگر back up داده ها در جای امنی موجود و در دسترس باشد، کافی است که سازمان فقط به فکر مدیریت ریسک آتش سوزی باشد.

شدت

- میزان خسارتی که احتمالاً اتفاق می‌افتد؛
- شدت با exposure فرق دارد؛
- هر چه شدت بیشتر باشد، ریسک بیشتر است؛
- اگر بدانیم که رویدادی چقدر محتمل است و پیامد آن نیز چقدر است، احساس نسبتاً (و نه لزوماً کاملاً) درستی از ریسک آن واقعه داریم؛
- شدت اغلب تابعی از عوامل دیگر است. مانند: volatility در ریسک بازار؛
- در مورد ریسک اعتبار، احتمال تابعی است از اعتبارسنجی اعتبار گیرنده ولی شدت به میزان وثایق اخذ شده مربوط است.

افق زمانی

- طول مدت در معرض ریسک بودن؛
- هر چه این مدت بیشتر باشد، ریسک بزرگتر است؛
- مثال: دادن وام یک ساله یا ده ساله به یک قرض گیرنده؛
- اوراق قرضه دارای پشتیبانی دولتی نسبت به سهام فهرست نشده و مشتقات از ریسک کمتری برخوردارند چراکه افق زمانی نقدشوندگی آنها کوتاه‌تر است؛
- در مورد ریسک عملیاتی چطور؟ (میزان آمادگی سازمان)؛

همبستگی

- **چگونگی ارتباط ریسک های یک کسب و کار با هم؛**
- **دو ریسک از همبستگی بالایی برخوردارند اگر رفتاری مشابه داشته و به دلایل مشابه یا مقدار مشابه افزایش یابند؛**
- **همبستگی مفهومی کلیدی در تنوع بخشی به ریسک (risk diversification) محسوب می‌شود؛**
- **ریسک های دارای همبستگی بالا، باعث افزایش تمرکز ریسک می‌شوند؛**
  - پرداخت وام به یک صنعت واحد یا سرمایه گزاری در یک دارایی واحد یا انجام عملیات مختلف در یک ساختمان؛
- **برای تنوع بخشی به ریسک های بازار و اعتبار می توان برای آنها سقف تعیین کرد؛**
- **برای ریسک عملیاتی می‌توان از روش تفکیک ریسک استفاده کرد؛**

سرمایه

- **دلایل اصلی نگهداری سرمایه (کاری) در سازمانها:**
  - انجام سرمایه گزاری و پرداخت هزینه ها؛
  - جبران خسارات ریسک های محقق شده؛
- **میزان سرمایه‌ای که برای دو منظور فوق لحاظ می‌شود را سرمایه اقتصادی می‌نامند؛**
- **میزان سرمایه اقتصادی بستگی به سطح رتبه اعتباری مورد انتظار دارد؛**
- **رتبه اعتباری برآوردی است از میزان محتمل بودن شکست یک سازمان؛**
- **هر چه رتبه اعتباری بالاتر باشد، سرمایه اقتصادی هم بایستی بیشتر باشد؛**
- **مدیران ریسک باید سرمایه انسانی (استعداد و ظرفیت مدیریتی، تجربه و سوابق) و ذخایر نقدی سازمان را نیز در نظر بگیرند؛**
- **مجموع سرمایه اقتصادی، سرمایه انسانی و ذخایر نقدی یک سازمان را ظرفیت ریسک آن می‌نامند.**

تعریف مدیریت ریسک سازمانی (ERM)

ERM is an integrated and continuous process for managing enterprise-wide risks—including strategic, financial, operational, compliance, and reputational risks—in order to minimize unexpected performance variance and maximize intrinsic firm value.
This process empowers the board and management to make more informed risk/return decisions by addressing fundamental requirements with respect to governance and policy (including risk appetite), risk analytics, risk management, and monitoring and reporting.

LAM, JAMES; 2017 *"Implementing Enterprise Risk Management – From Methods to Applications"*

مدیریت ریسک سازمانی (ERM) فرآیندی یکپارچه و مستمر برای مدیریت ریسک‌های کل شرکت - از جمله ریسک‌های استراتژیک، مالی، عملیاتی، انطباق و اعتباری - به منظور به حداقل رساندن واریانس عملکرد غیرمنتظره و به حداکثر رساندن ارزش ذاتی شرکت است. این فرآیند هیئت مدیره و مدیریت را قادر می سازد تا با پرداختن به الزامات اساسی با توجه به حاکمیت و خط مشی (از جمله اشتهای ریسک)، تجزیه و تحلیل ریسک، مدیریت ریسک، و نظارت و گزارش، تصمیمات آگاهانه تری درباره ریسک/بازده اتخاذ کنند.

COSO ERM 2017 vs. ISO 31000:2018

Enterprise risk management (ERM):

The culture, capabilities and practices, integrated with strategy-setting and its performance, that organizations rely on to manage risk in creating, preserving and realizing value.

COSO ERM 2017-Integrating with Strategy and Performance

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

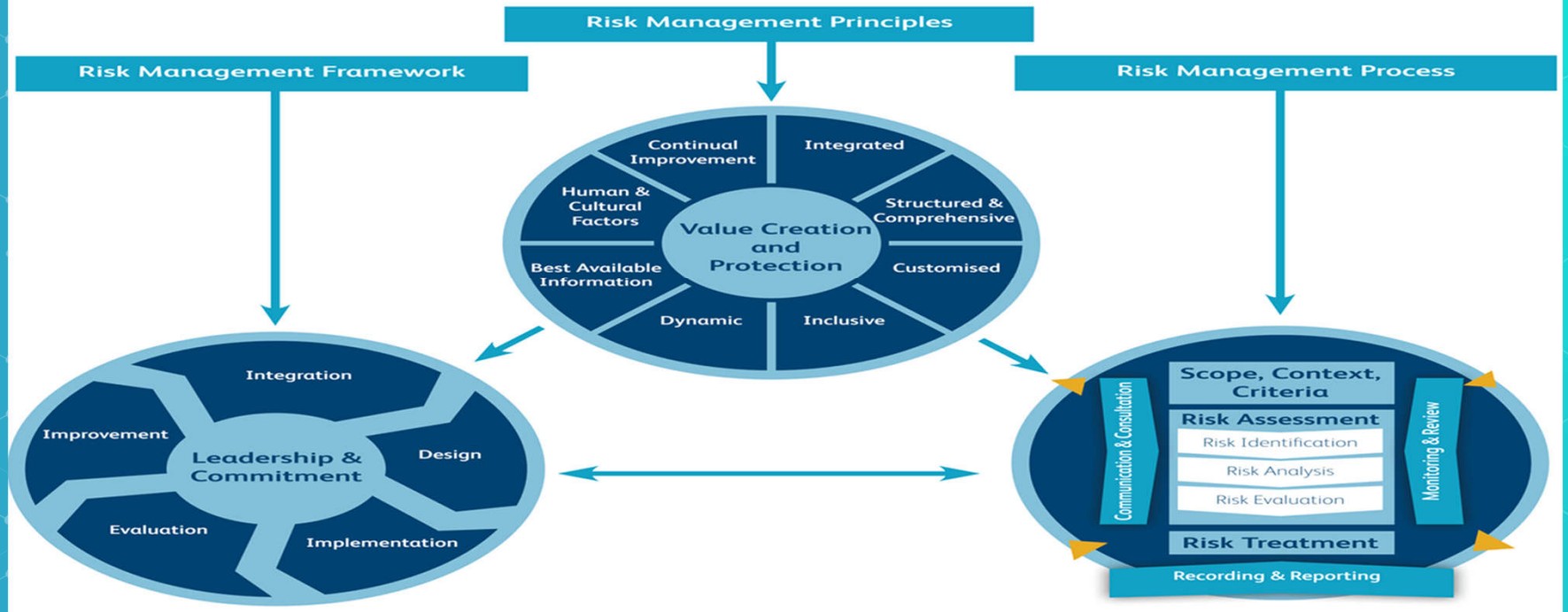
15. Assesses Substantial Change
16. Reviews Risk and Performance
17. Pursues Improvement in Enterprise Risk Management

Information, Communication, & Reporting

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

COSO ERM 2017 vs. ISO 31000:2018

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

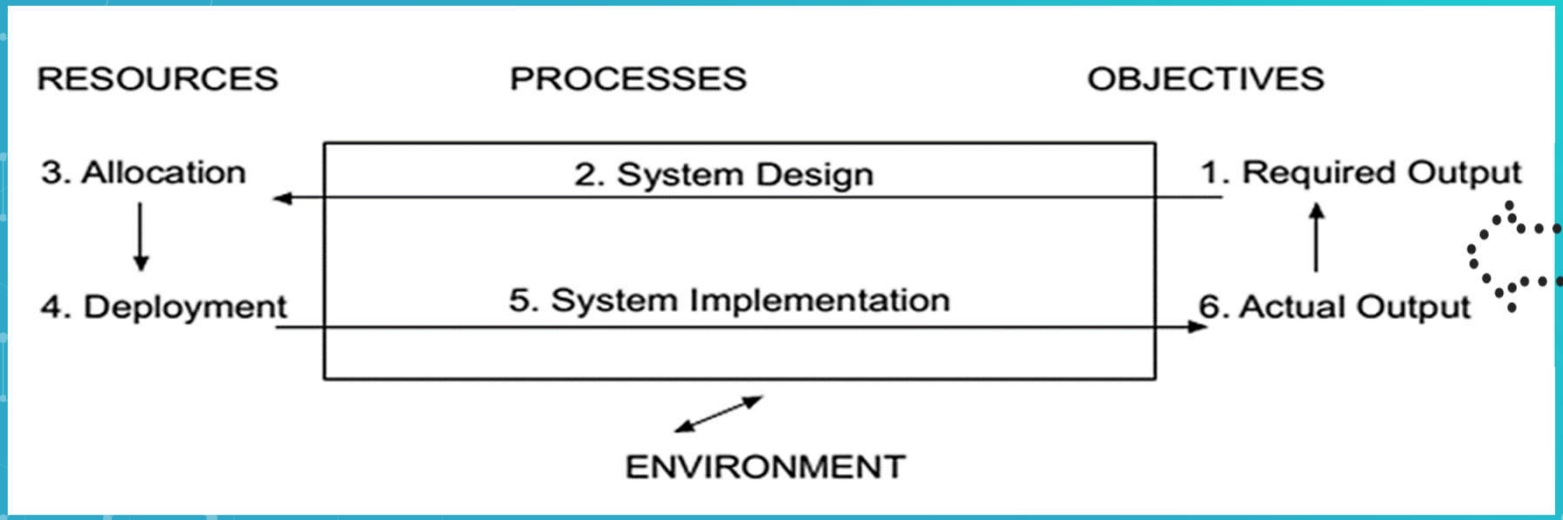


risk management

coordinated activities to direct and control an organization (3.3.7) with regard to risk (3.1.1)

مدل مفهومی سیستم مدیریتی (Management System)

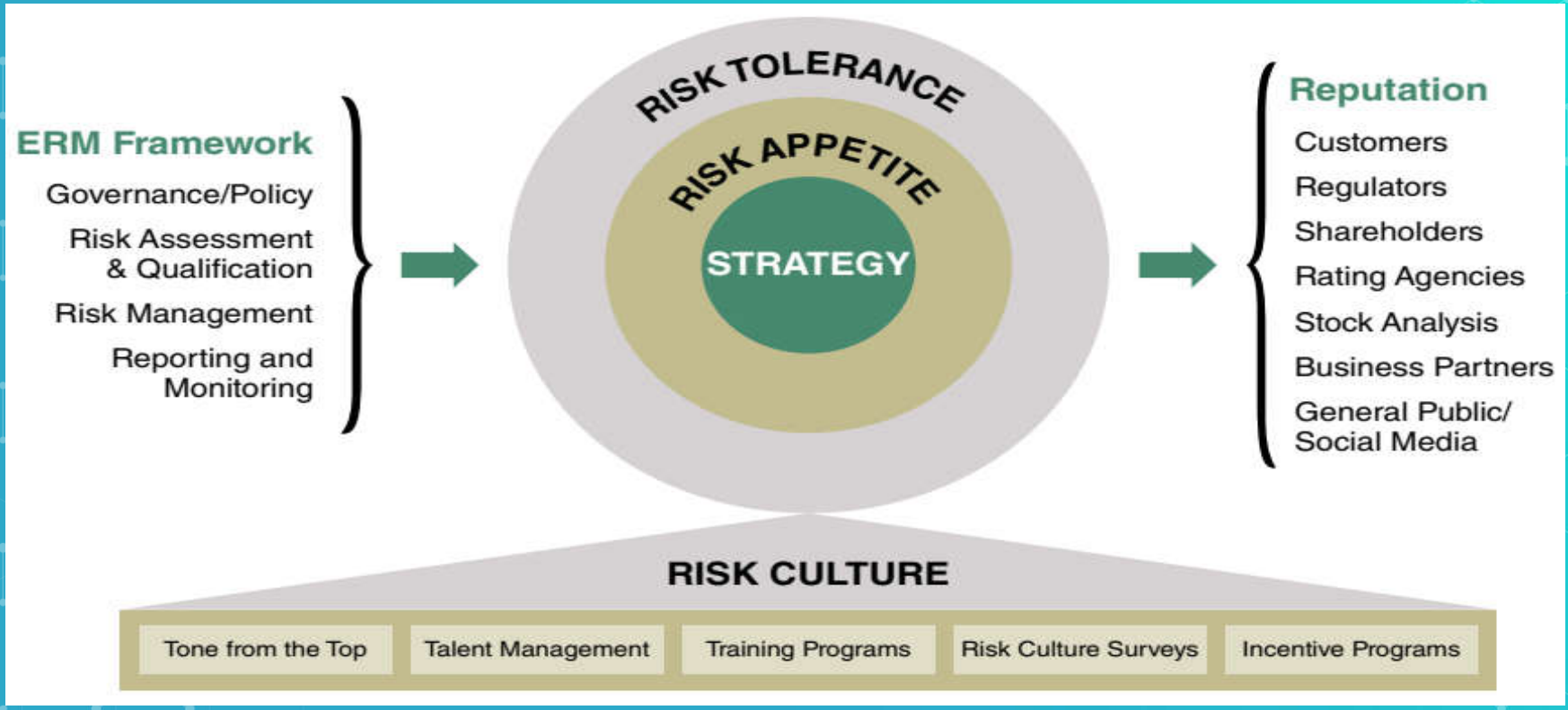
- As per ISO, Management System is defined as: *"the set of procedures an organization needs to follow in order to meet its objectives"*; سیستم مدیریت عبارتست از مجموعه روشهایی که سازمان باید دنبال کند تا به اهدافش برسد
- System design and process approach.



عناصر کلیدی چارچوب مدیریت ریسک سازمانی

- ارزیابی **اشتها و تحمل ریسک** سازمان
- راهنمای شفاف و مستند مسئولیت و پاسخگویی مدیریت ریسک و تصمیمات مربوطه (حاکمیت ریسک)
- فرآیندی مستند برای **شناسایی** انواع رویدادهایی که می تواند دستیابی به اهداف سازمان و همچنین فرصت‌هایی برای ایجاد ارزش را به خطر بیندازد.
- ایجاد سیاست‌ها و فرآیندهایی برای **مواجهه** با ریسک‌های شناسایی شده (treatment)
- **نظارت و مدیریت** ریسک‌ها در طول زمان در سطح عملیاتی
- ایجاد برنامه‌های اضطراری برای خسارات سنگین و شرایط اضطراری که ممکن است رخ دهد (BCM)
- ارزیابی منظم **کفایت** چارچوب مدیریت ریسک.

ارتباط عناصر کلیدی چارچوب ERM



LAM, JAMES; 2017 *"Implementing Enterprise Risk Management – From Methods to Applications"*

نقش مقررات و نظارت در توسعه مدیریت ریسک سازمانی

مدیریت ریسک به هیچ وجه مفهوم جدیدی نیست، با اینحال:

- به شدت مورد توجه نهادهای نظارتی در بسیاری از حوزه‌های اقتصادی است
- هیچ بخشی از اقتصاد از این قاعده کلی مستثنی نیست
- هیئت مدیره سازمان (Full Board) به عنوان مسؤل غایی و نهایی مدیریت ریسک شناخته می‌شود
- سازمان‌ها با مجموعه‌ای فزاینده و پیچیده از مقررات حاکمیتی و مدیریت ریسک در سطوح ملی، منطقه‌ای و بین المللی مواجهند
- ترکیبی از رژیم های نظارتی اجباری، داوطلبانه، مبتنی بر اصول (Principle-based) و مبتنی بر قواعد و مقررات (Rule-based) ایجاد شده است
- برخی از بخش‌های اقتصادی نسبت به سایرین به شدت تحت نظارتند، مانند خدمات مالی
- همه کدها و مقررات وضع شده همسو نیستند و بسیاری از آنها در سطح جزئیات در مورد مدیریت ریسک تفاوت‌هایی با یکدیگر دارند.

پویایی و سرعت تحولات قوانین و مقررات ناظر بر مدیریت ریسک سازمانی

- تغییرات جوی (Climate Change)
- فنآوری‌های نوآورانه و تحول آفرین (Disruptive Innovative Technologies):
  - هوش مصنوعی
  - یادگیری ماشینی
  - اینترنت اشیاء
  - بلاک‌چین
  - ...

گزیده‌ای از قوانین و مقررات نوظهور

- مقررات مربوط به امنیت سایبری و حفاظت از زیرساخت‌های حیاتی مرتبط با اموال و دارایی‌ها
- حفاظت از محیط زیست
- قوانین ضد تبعیض و نژادپرستی
- قوانین مبارزه با پولشویی و تأمین مالی تروریسم
- مقررات سوت‌زنی (Whistleblowing)
- ...

برخی قوانین و مقررات قدیمی‌تر:

- قانون تجارت و ثبت شرکتها
- قانون مالیات
- قانون تأمین اجتماعی
- قانون کار
- قانون ایمنی و بهداشت محیط کار
- ...

What this rapidly evolving regulatory environment underscores is the board's ultimate accountability for risk management and the importance of directors taking an integrated, organization-wide [ERM] perspective to the oversight of the risk.

آنچه که این محیط نظارتی به سرعت در حال تحول بر آن تأکید می‌کند، مسئولیت‌پذیری نهایی هیئت مدیره در قبال مدیریت ریسک و اهمیت اتخاذ دیدگاهی یکپارچه و فراگیر در سطح سازمانی (ERM) برای نظارت بر ریسک است .

سؤالات کلیدی از هیأت مدیره شرکت‌های (بیمه)

- اگر سازمان شما توسط حسابرسان/ممیزان رسمی خارجی مورد حسابرسی قرار گیرد، به نظر شما چه ضعف‌هایی را در چارچوب حاکمیتی و مدیریت ریسک‌تان ممکن است شناسایی کنند؟
- فکر می‌کنید که تیم مدیریت ارشد شما چگونه به سؤالات حسابرسی پاسخ خواهند داد؟

پنج وظیفه اصلی هیأت مدیره شرکت (بیمه)

- **تعیین استراتژی صحیح و حصول اطمینان از پیاده سازی مناسب آن توسط تیم مدیریت اجرایی**
- **مدیریت** (تعیین مدیرعامل و تیم اجرایی و جبران خدمات آنها به نحو مناسب، تعیین ساختار پاداش، جانشین پروری، ...)
- **حصول اطمینان از اثربخش بودن هیأت مدیره**
- **حسابرسی / ممیزی** (صحیح بودن حسابها و صورتهای مالی، وجود کنترل‌های داخلی مناسب، برآورده شدن الزامات بازار سرمایه و افشای عمومی اطلاعات، ...)

حوزه تمرکز کمیته حسابرسی داخلی

- **ریسک و تطبیق** (مدیریت مناسب ریسک و تطبیق با الزامات قوانین و مقررات حاکم بر فعالیت سازمان، ...)

حوزه تمرکز کمیته مدیریت ریسک

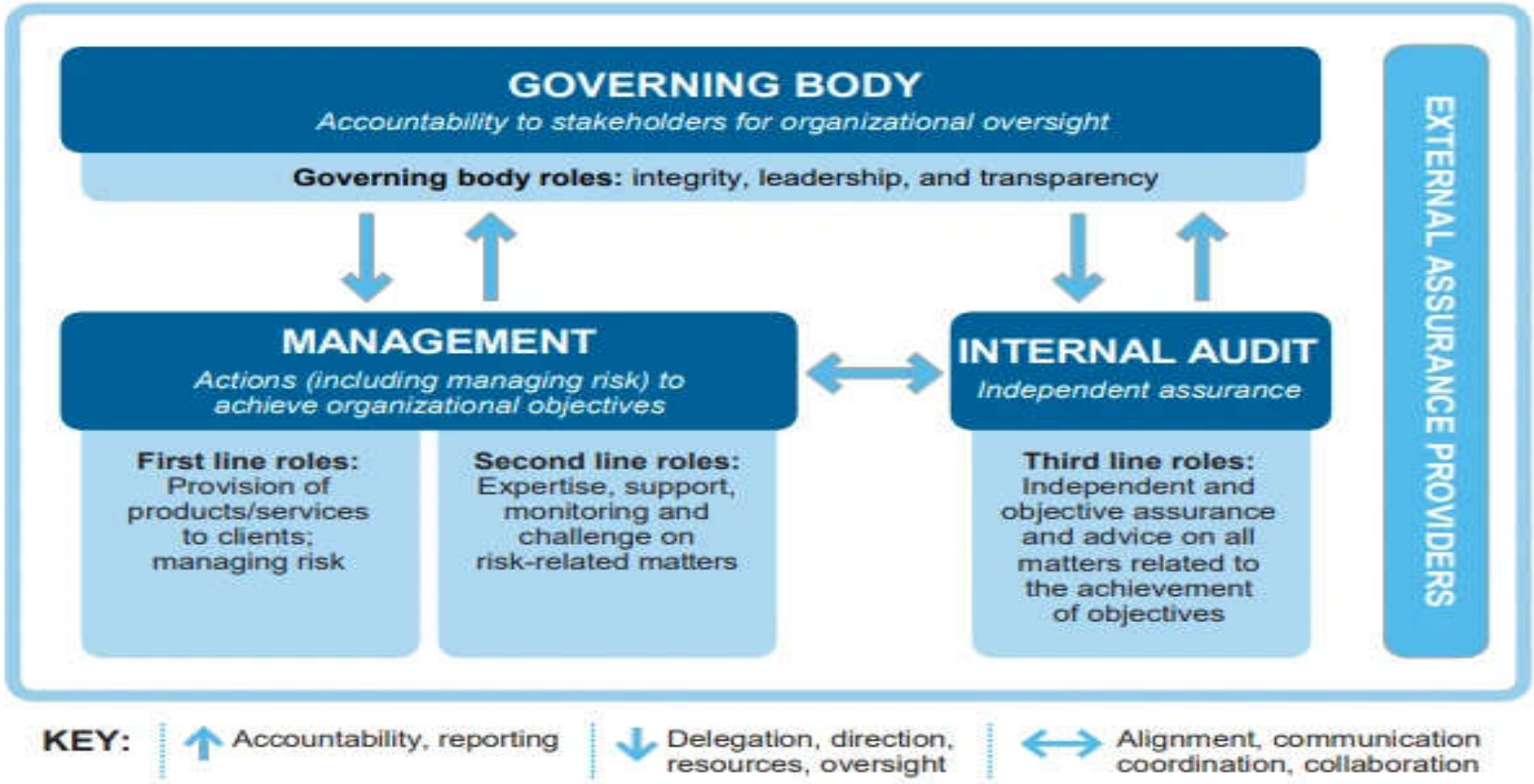
LAM, JAMES; 2017 *"Implementing Enterprise Risk Management – From Methods to Applications"*

موضوعات مهم مرتبط با سیستم مؤثر مدیریت ریسک سازمانی

- **توزیع مسؤلیت‌ها** (وظایف اعضای هیئت مدیره، تفویض اختیارات، شفافیت، پاسخگویی، ...)
- **کمیته های هیئت مدیره** (حسابرسی، ریسک، ...)
- **وظایف تیم مدیریت اجرایی**
- **وظایف و ارتباطات مدیر ارشد ریسک (CRO)**
- **حسابرسی داخلی و خارجی**
- **وظایف مدیران و کارکنان عملیاتی**
- **ESG**
- **فرهنگ سازمانی (Risk aware culture)**
- **مشوق‌ها/جبران خدمات**

- **ابزارها، تکنیک‌ها، فرآیندها**
- **طبقه بندی انواع ریسک و فهم مشترک آن**
- **اشتهاء و تلرانس (حد تحمل) ریسک**
- **فرم ثبت ریسک و ماتریس ریسک**
- **دیتا آنالیتیک، رویکردهای کمی و داشبورد**
- **ماتریس مهارت‌های اعضای هیئت مدیره (Qualified Risk Directors)**
- **صلاحیت اعضای هیئت مدیره در زمینه ریسک**
- **فرهنگ حاکم بر جلسات هیئت مدیره**
- **BCM**
- **صورتجلسات و گزارشات هیئت مدیره**

مدل ۳ لایه دفاعی



اشتهاء و تحمل (تلرانس) ریسک

اشتهاء و حد تحمل ریسک

- تعیین اشتهای ریسک و تلرانس به وضوح پایه و اساس مناسبی برای مدیریت ریسک فراهم می کند
- اغلب این دو عبارت به جای هم استفاده می‌شوند
- در یک نگاه کلی، برنامه استراتژیک/کسب و کار (BP) عبارت است از بیان هیئت مدیره از ریسک پذیری یک سازمان
- مرسوم است که هیئت مدیره یک بیانیه رسمی ریسک پذیری جدا از استراتژی خود صادر کنند
- نهادهای تحت نظارت APRA ملزم به داشتن بیانیه‌های ریسک پذیری مورد تأیید هیئت مدیره اند
- هیئت مدیره از مدیریت ارشد انتظار دارند که در تعقیب اهداف استراتژیک سازمان عمل کنند

... اشتهای ریسک و حد تحمل

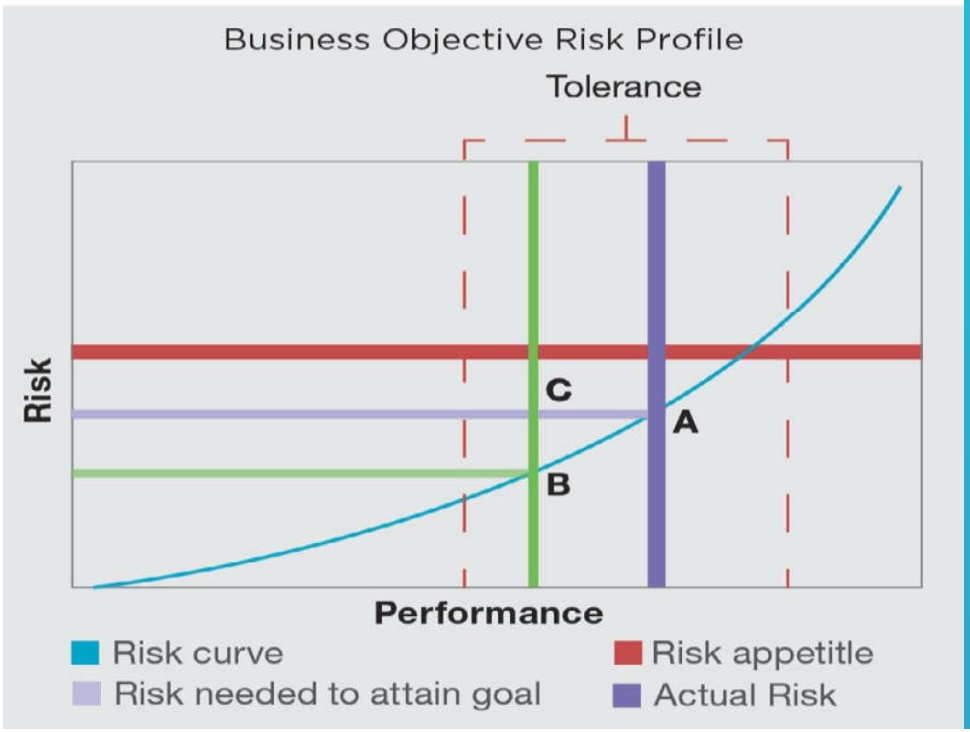
- **بسیاری از سازمان‌ها برای انواع تصمیم گیری‌ها و فعالیت‌های کاری سطوح اشتهای ریسک را مستندسازی کرده‌اند. مانند:**
  - تفکیک وظایف
  - حدود تأمین مالی و معاملات
  - معیارهای انتخاب پیمانکار
  - حدود و سقف سپرده گذاری در بانک
  - تلرانس صفر برای ایمنی و کلاهبرداری
  - وقتی برای کارایی مورد انتظار (مثلاً مدت زمان رسیدگی و تعیین تکلیف پرونده خسارت بیمه) رنج زمانی مشخصی تعیین شده است
  - شاخص‌های NPV و IRR در پروژه های سرمایه گذاری؛ و
  - ....

تعریف ایزو ۳۱۰۷۳ ویرایش ۲۰۲۲ درباره اشتهای ریسک

3.3.27
risk appetite
amount and type of risk (3.1.1) that an organization (3.3.7) is willing to pursue or retain
[SOURCE:ISO Guide 73:2009, 3.7.1.2]
3.3.28
risk tolerance
organization's (3.3.7) or interested party's (3.3.2) readiness to bear the residual risk (3.3.38) in order to achieve its objectives (3.1.2)
Note 1 to entry: Risk tolerance can be influenced by legal or regulatory requirements.

تفاوت اشتهاء و تلرانس ریسک طبق راهنمای COSO ERM 2017

Figure D.11:
Using Risk Profiles to Monitor Performance



- اشتهای ریسک: انواع و میزان ریسکی که به طور کلی یک سازمان در راستای دستیابی به اهداف خود می‌پذیرد
- اشتهای ریسک موضوعی راهبردیست و به رویکرد کلی سازمان نسبت به ریسک مربوط است
- تلرانس ریسک عبارتست از کاربرد عملیاتی اشتهای ریسک در تبادلات یا فعالیت‌های معین
- برای نمونه، برنامه راهبردی در حکم اشتهای ریسک و برنامه BP مربوط به واحدهای کسب و کار (BU) در حکم تلرانس ریسک است

اشتهای ریسک چیست؟

- **در ۱۰ درصد مواقع اشتهای ریسک توسط قانون و مقررات تعیین می‌شود. مانند:**
  - تلرانس صفر برای ایمنی، رشوه، فساد، پولشویی، آلودگی زیست محیطی، ...
- **در ۱۰ درصد مواقع نوعی توافق و هماهنگی بین هیأت مدیره و هیأت عامل/اجرایی است. مانند:**
  - تمامی حدود و صغوری که هیأت مدیره برای تصمیمات هیأت عامل تعیین می کند. مثل سقف پرداخت خسارت، تخفیفات حق بیمه، ...
- **در ۸۰ درصد مواقع بستگی به رویکرد تصمیم گیری مبتنی بر ریسک و پاداش (Risk and Reward/Return) در هر مورد خاص دارد. مانند:**
  - تصمیماتی که مشابه آن قبلاً گرفته نشده و متناسب با مورد در خصوص اشتهای ریسک تصمیم‌گیری می‌شود.

مستند سازی اشتهای ریسک

- **معمولاً مستند سازی الزامی نیست، مگر در مقررات تأکید شده باشد. ولی اگر انجام شود، خوب است.**
- **هیئت مدیره به عنوان متولی و مسؤل اصلی سیستم مدیریت ریسک سازمانی باید از هیأت عامل و واحد مدیریت ریسک بخواهد که خط مشی‌ها/سیاست‌ها و رویه‌های تعیین شده توسط هیأت مدیره را بررسی و رعایت کنند. مانند:**
  - ممنوعیت همکاری با سازمانهایی که حقوق کودکان یا حیوانات را رعایت نمی‌کنند
  - سیاست عدم سرمایه گذاری در پروژه هایی که ریسکشان از حد مشخص شده بالاتر است
  - بسیاری از موارد دیگر
- **برای ریسک‌هایی که از قبل رویه و اشتهایی ندارند، واحد مدیریت ریسک بایستی با واحدهای اجرایی برای تعیین و پیشنهاد سطوح اشتهاء همکاری کند.**
- **...**

بازنگری سند اشتهای ریسک

- همکاری واحد مدیریت ریسک با تیم حسابرسی داخلی انجام شود
- در ۸۰ درصد مواقع برای بسیاری از تصمیمات بیزنسی شناخته شده و معمول سطوح اشتهای ریسک مشخص است و کاری که مدیر ریسک باید انجام دهد، تأیید و تصدیق و پایش و بازنگری انجام آنهاست

درباره اشتهاء و تلرانس ریسک بیشتر بدانیم ...

- برای اطلاعات بیشتر در خصوص اشتها و تلرانس ریسک، دو مستند زیر را مطالعه نمایید:
- RIMS, 2012 “Exploring Risk Appetite and Risk Tolerance
- Risk- Academy’s Guide on RISK APPETITE

مواجهه/رفتار با ریسک

تعریف ایزو ۳۱۰۷۳ درباره مواجهه/رفتار با ریسک

risk treatment

*process to modify **risk** (3.1.1)*

***Note 1** to entry: Risk treatment can involve:*

- *— **avoiding** the risk by deciding not to start or continue with the activity that gives rise to the risk;*
- *— **taking or increasing** risk in order to pursue an **opportunity** (3.3.23);*
- *— **removing** the **risk source** (3.3.10);*
- *— **changing** the **likelihood** (3.3.16);*
- *— **changing** the **consequences** (3.3.18);*
- *— **sharing** the risk with another party or parties [including contracts and **risk financing** (3.3.36)]; and*
- *— **retaining** the risk by informed decision.*

***Note 2** to entry: Risk treatments that deal with negative consequences are sometimes referred to as "risk mitigation", "risk elimination", "risk prevention" and "risk reduction".*

***Note 3** to entry: Risk treatment can create new risks or modify existing risks.*

تعاریف ایزو ۳۱۰۷۳ درباره راهبردهای مواجهه با ریسک

risk control

measure that maintains and/or modifies **risk** (3.1.1)
Note 1 to entry: Risk controls include, but are not limited to, any process, policy, device, practice, or other conditions and/or actions which maintain and/or modify risk.
Note 2 to entry: Risk controls do not always exert the intended or assumed modifying effect.

risk avoidance

informed decision not to be involved in, or to withdraw from, an activity in order not to be exposed to a particular **risk** (3.1.1)
Note 1 to entry: Risk avoidance can be based on the result of **risk evaluation** (3.3.25) and/or legal and regulatory obligations.

risk sharing

form of **risk treatment** (3.3.32) involving the agreed distribution of **risk** (3.1.1) with other parties
Note 1 to entry: Legal or regulatory requirements can limit, prohibit or mandate risk sharing.
Note 2 to entry: Risk sharing can be carried out through insurance or other forms of contract.
Note 3 to entry: The extent to which risk is distributed can depend on the reliability and clarity of the sharing arrangements.

تعاریف ایزو ۳۱۰۷۳ درباره راهبردهای مواجهه با ریسک

risk financing

form of **risk treatment** (3.3.32) involving contingent arrangements for the provision of funds to meet or modify the financial **consequences** (3.3.18) should they occur

risk retention

acceptance of the potential benefit of gain, or burden of loss, from a particular **risk** (3.1.1)
Note 1 to entry: Risk retention includes the acceptance of **residual risks** (3.3.38).
Note 2 to entry: The **level of risk** (3.3.22) retained can depend on **risk criteria** (3.3.6).

residual risk

risk (3.1.1) remaining after **risk treatment** (3.3.32)
Note 1 to entry: Residual risk can contain unidentified risk.
Note 2 to entry: Residual risk can also be known as “retained risk”.

برنامه عملیاتی رفتار/مواجهه با ریسک

- **مسئولیت‌ها، برنامه‌ها، نتایج مورد انتظار از مواجهه، بودجه، اقدامات عملکردی و فرآیند بازنگری را مشخص می کند.**
- **معمولاً جزئیاتی را در مورد موارد زیر ارائه می دهد:**
  - اقداماتی که باید انجام شود و ریسک‌هایی که به آنها رسیدگی می شود
  - چه کسی مسئولیت اجرای طرح مواجهه با ریسک را دارد
  - چه منابعی باید استفاده شود
  - تخصیص بودجه
  - جدول زمانی اجرا
  - جزئیات مکانیسم و دفعات بررسی وضعیت برنامه مواجهه با ریسک

درباره رفتار/مواجهه با ریسک بیشتر بدانیم ...

- برای اطلاعات بیشتر در خصوص اشتها و تلرانس ریسک، مستند زیر را مطالعه نمایید:

IIRM, 2015; *"A Practical Gide to Enterprise Risk Management"*

پایش و بازنگری، مستندسازی و گزارشات

تعاریف ایزو ۳۱۰۷۳ درباره پایش، بازنگری، گزارش دهی و ارتباطات

monitoring

continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected

Note 1 to entry: Monitoring can be applied to a risk management framework, **risk management process** (3.3.1), **risk** (3.1.1) or **risk control** (3.3.33).

review

activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established **objectives** (3.1.2)

Note 1 to entry: Review can be applied to a risk management framework, **risk management process** (3.3.1), **risk** (3.1.1) or **risk control** (3.3.33).

risk reporting

form of **communication** intended to inform particular internal or external **interested party** (3.3.2) by providing information regarding the current state of **risk** (3.1.1) and its management

پایش و بازنگری

- **هدف:** تضمین و بهبود کیفیت و اثربخشی طراحی فرآیند، اجراء و نتایج
- پایش مستمر و بازنگری دوره‌ای فرآیند مدیریت ریسک و نتایج آن
- بخشی برنامه‌ریزی‌شده از فرآیند مدیریت ریسک
- تعریف روشن مسئولیت‌ها و وظایف
- انجام در تمام مراحل فرآیند
- بررسی روند برنامه ریزی، جمع آوری و تجزیه و تحلیل اطلاعات، ثبت نتایج و ارائه بازخورد
- به کارگیری نتایج پایش و بازنگری در سراسر فعالیت‌های مدیریت عملکرد، اندازه گیری و گزارش دهی سازمان.

ایزو ۳۱۰۰۰ ویرایش ۲۰۱۸

مستندسازی و گزارش‌دهی

- **هدف مستندسازی عبارتست از:**
  - ارتباط فعالیت‌ها و نتایج مدیریت ریسک در سرتاسر سازمان
  - ارائه اطلاعات برای تصمیم گیری
  - بهبود فعالیت‌های مدیریت ریسک
  - کمک به تعامل با ذینفعان، از جمله کسانی که مسئولیت و پاسخگویی برای فعالیت های مدیریت ریسک دارند.
- **گزارش‌دهی بخشی جدایی ناپذیر از حاکمیت سازمان است و باید کیفیت گفت‌وگو با ذینفعان را افزایش دهد و از مدیریت عالی و نهادهای نظارتی در انجام مسئولیت‌های خود حمایت کند.**
- **عواملی که برای گزارش باید در نظر گرفته شوند عبارتند از:**
  - ذینفعان مختلف و نیازها و الزامات اطلاعاتی خاص آنها
  - هزینه، فراوانی و به موقع بودن گزارش
  - روش گزارش دهی
  - ارتباط اطلاعات با اهداف سازمانی و تصمیم گیری.

نکات مهم در خصوص ارتباطات/مشاوره

- **توجه به تعریف و چرایی اهمیت ارتباطات**
- **مراحل کلیدی ارتباطات عبارتست از:**
  - ایجاد اهداف ارتباطی و مشاوره ای
  - تجزیه و تحلیل ذینفعان یا گیرندگان پیام
  - توسعه پیام های کلیدی و هدف
  - شناسایی صاحبان و فرستندگان ارتباطات
  - شناسایی کانال های مناسب
  - تعیین زمان ارتباط
  - تحویل پیام های کلیدی

اهداف فرآیند ارتباطات/مشاوره

- ایجاد آگاهی و درک در مورد یک موضوع خاص
- یادگیری از ذینفعان
- تأثیرگذاری بر مخاطبان هدف
- به دست آوردن درک بهتری از زمینه، معیارهای ریسک، ریسک، یا اثر برنامه مواجهه با ریسک
- دستیابی به تغییر نگرشی یا رفتاری در رابطه با موضوعی خاص
- هر ترکیبی از موارد فوق.

گزارش دهی ریسک و مدیریت ریسک

- یک برنامه مدیریت ریسک موفق مستلزم ارتباط مکرر و باز با گروه وسیعی از ذینفعان داخلی و خارجی است.
- تعریف یک برنامه ارتباطی و گزارش دهی منسجم ریسک جزء کلیدی یک برنامه مدیریت ریسک سازمانی (ERM) موفق ارزیابی می شود.
- گزارش‌دهی موثر ریسک به استحکام حاکمیت شرکتی کمک می‌کند.
- ارائه اطلاعات به هیئت مدیره، مدیران ارشد و سایر ذینفعان در مورد ریسکهای پیش روی سازمان را تسهیل می کند.
- گزارش برنامه های مواجهه/رفتاری موجود برای مدیریت ریسکها را ارائه می نماید.

مخاطبان گزارشات ریسک و مدیریت ریسک

- گزارش های ریسک باید به طیف وسیعی از ذینفعان سازمانی ارائه شود:
- مدیرعامل و هیئت مدیره
- مدیران واحدها و وظایف اصلی کسب و کار
- کمیته های حاکمیت شرکتی(به ویژه حسابرسی داخلی و مدیریت ریسک)
- کارکنان مسئول مستقیم طراحی و اجرای برنامه های رفتاری مدیریت ریسک
- کارکنانی که نیاز به کمک در شناسایی ریسک و اجرای برنامه های ریسک دارند
- وزارتخانه ها و سازمان های دولتی
- عموم مردم (از طریق دسترسی به گزارش های سالانه و بیانیه های مطبوعاتی)

بیشتر بدانیم ...

برای اطلاعات بیشتر در خصوص اشتها و تلرانس ریسک، مستند زیر را مطالعه نمایید:

A-Practical-Guide-to-Enterprise-Risk-Management-pdf-1678481615.pdf

یکپارچه سازی مدیریت ریسک در فرآیندهای تصمیم گیری

مفهوم یکپارچگی بر اساس استاندارد ایزو ۳۱۰۰۰ ویرایش ۲۰۱۸

- مدیریت ریسک بخشی جدایی ناپذیر از تمام فعالیت های سازمانی است (کلوز 4-a)
- یکپارچه سازی مدیریت ریسک در یک سازمان یک فرآیند پویا و تکراری است و باید متناسب با نیازها و فرهنگ سازمان تنظیم شود.
- مدیریت ریسک باید بخشی جدایی ناپذیر از هدف سازمانی، حکمرانی، رهبری و تعهد، استراتژی اهداف و عملیات باشد. (کلوز 3-5)

Clause 4-a):
"Risk management is an integral part of all organizational activities."
Clause 5.3) Integration:
"Integrating risk management into an organization is a dynamic and iterative process, and should be customized to the organization's needs and culture. Risk management should be a part of, and not separate from, the organizational purpose, governance, leadership and commitment, strategy, objectives and operations."
Clause 6.1):
"…The risk management process should be an integral part of management and decision-making and integrated into the structure, operations and processes of the organization. It can be applied at strategic, operational, program or project levels."

مفهوم یکپارچه سازی

- **سیستم مدیریت ریسک سازمانی (ERM) ابزاری (Tool) است برای کمک به مدیریت و تصمیم گیری مبتنی بر ریسک. بنابراین بایستی در تمامی هدف گذاری ها، استراتژیها، رویه ها و دستورالعملها، فرآیندها، پروژه ها، ... از جمله موارد زیر یکپارچه سازی شود:**
  - برنامه ریزی
  - پیش بینی
  - بودجه بندی
  - ساخت و ساز
  - سرمایه گذاری
  - مدیریت عملکرد
  - ...

بیشتر بدانیم ...

برای اطلاعات بیشتر در خصوص اشتها و تلرانس ریسک، مستند زیر را مطالعه نمایید:

BS ISO 31000-2018.pdf