



کارگاه آموزشی

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

ارائه دهنده: 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 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 مدنظر 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 كاري

- 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 اگو 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.



آشنایی با سیستم مدیریت ریسک سازمانی (ERM)

ارائه دهنده:

محمود اسعد سامانی PhD/ACII/AMII

فهرست مطالب

۱. مقدمه‌ای بر تاریخچه، اصطلاحات و مفاهیم مدیریت ریسک
۲. استانداردها و چارچوب‌های مدیریت ریسک (به عنوان مثال: ISO 31000، COSO ERM، ...)
۳. تکنیک‌ها و ابزارهای شناسایی ریسک
۴. روش‌های ارزیابی ریسک، از جمله رویکردهای کیفی و کمی
۵. اشتهای ریسک و حد تحمل
۶. استراتژی‌ها و گزینه‌های مواجهه/ رفتار با ریسک
۷. نظارت بر ریسک، گزارش دهی و ارتباطات
۸. یکپارچه‌سازی مدیریت ریسک در فرآیندهای تصمیم‌گیری
۹. مدیریت ریسک در برنامه‌ریزی، پیش‌بینی، بودجه‌بندی، ساخت و ساز، سرمایه‌گذاری و مدیریت عملکرد
۱۰. توسعه فرهنگ ریسک و مدیریت تغییر سازمانی
۱۱. نقش‌ها و مسئولیت‌های مدیریت ریسک در یک سازمان
۲۱. ابزارهای مدیریت ریسک و راه‌حل‌های نرم‌افزاری
۳۱. مطالعات موردی و نمونه‌هایی از اجرای موفق مدیریت ریسک
۴۱. خطرات و روندهای نوظهور در مدیریت ریسک
۵۱. جنبه‌های نظارتی و انطباقی مدیریت ریسک

مروری بر تاریخچه مدیریت ریسک

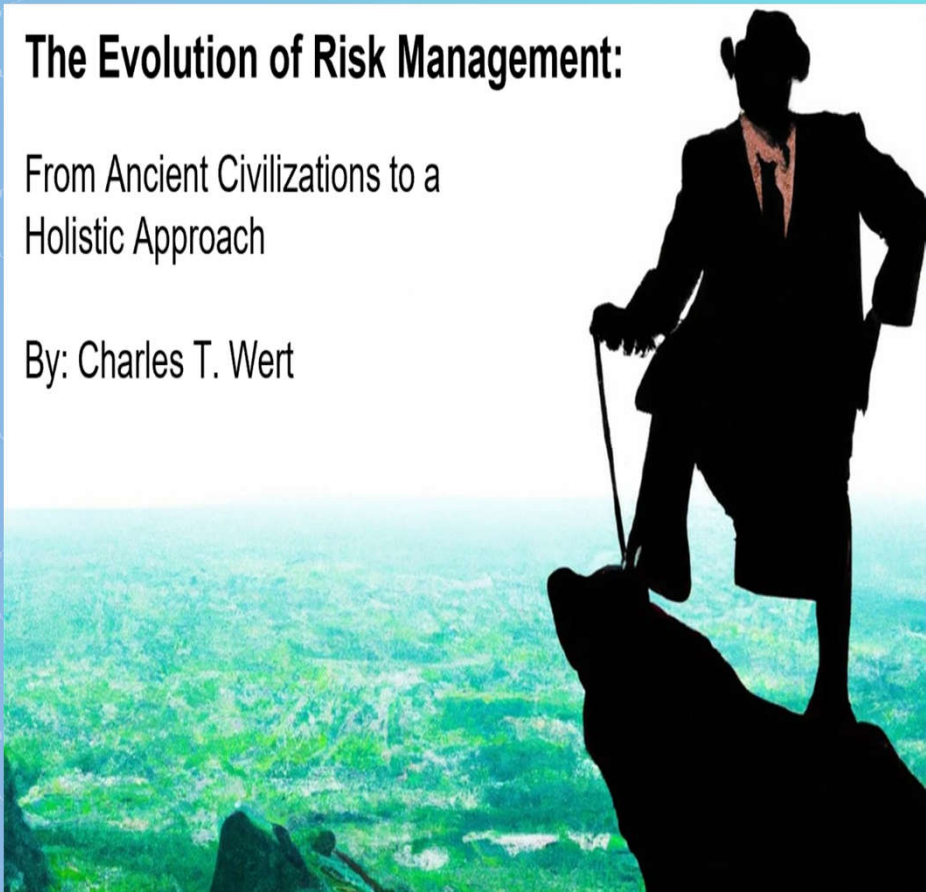


تاریخچه مختصر مدیریت ریسک

The Evolution of Risk Management:

From Ancient Civilizations to a
Holistic Approach

By: Charles T. Wert



◆ مدیریت ریسک ایده‌ای قدیمی است.

◆ به طرز عجیبی طی چند دهه اخیر
متحول شده است

◆ از زمان تمدن بابل:

❖ تجار و بازرگان‌ها ریسک عملیات بازرگانی
خود را مدیریت می‌کرده‌اند

❖ پرداخت وام توسط خریداران به فروشندگان
و بازپرداخت اصل و بهره وام در صورت
وصول سلامت کالاها در مقصد

عصر روشنگری/رنسانس و فراتر از آن

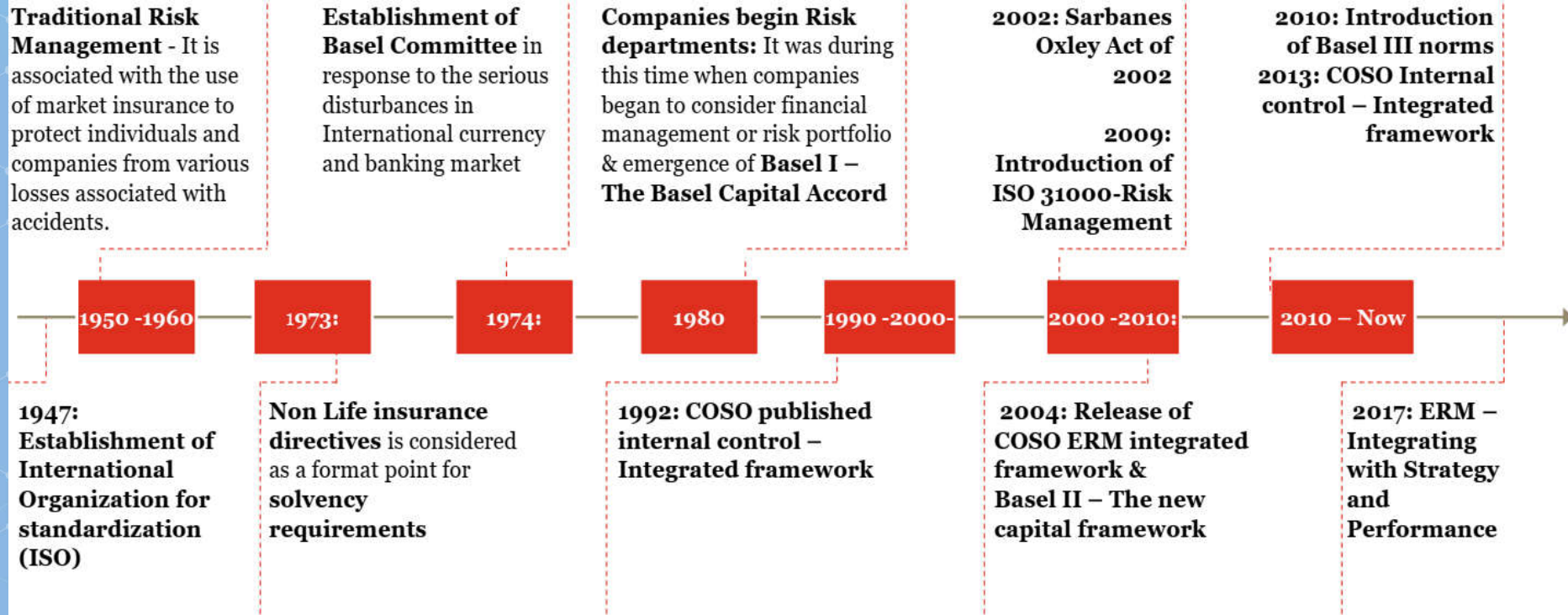


- ◆ رویکرد **سیستمی** به ارزیابی ریسک
- ◆ توسعه **تئوری احتمالات و آمار** در قرن ۱۷ میلادی و کمی سازی ریسک‌ها به طرق معقول
- ◆ توسعه **روش‌های سنجش و ارزیابی کمی ریسک** عمدتاً توسط شرکت‌های بیمه و بانک‌ها از قرن ۱۸ تا اوایل قرن ۲۰ میلادی

سیر تحولات مدیریت ریسک

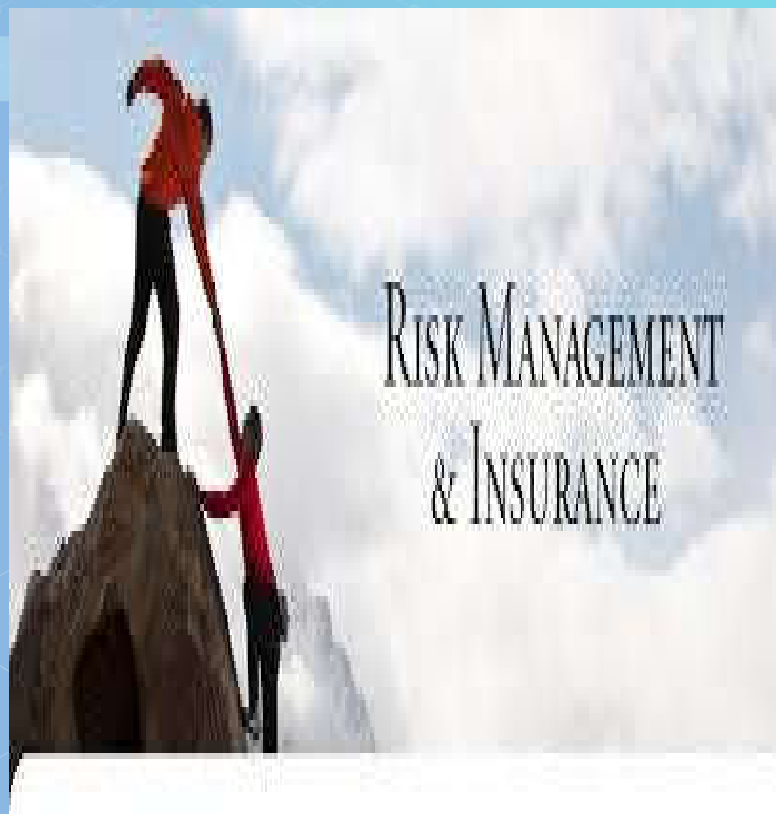
- ❖ فقدان تاریخچه مشخص برای بررسی سیر تحولات مدیریت ریسک
- ❖ عجین بودن با بیمه از قدیم
- ❖ شروع مطالعات مدیریت ریسک در شکل مدرن پس از جنگ جهانی دوم (۱۹۴۴-۱۹۵۵)
- ❖ انتشار اولین کتب مربوط به مدیریت ریسک در سال های ۱۹۶۳ و ۱۹۶۴
- ❖ تمرکز اولیه بر مدیریت ریسک های خالص (Pure) و بی توجهی به ریسک های سوداگرانه (اعتبار، بازار، نقدینگی و ...)
- ❖ **تفاوت ریسک خالص و سوداگرانه؟**
- ❖ هم زمان با این پیشرفت ها، مهندسان نیز مدل های مدیریت ریسک تکنولوژی را توسعه می دهند (LOPA، HAZOP، FMEA، ...)
- ❖ ورود ریسک های عملیاتی، سیاسی، استراتژی، ...

...سیر تحولات مدیریت ریسک سازمانی (ادامه)



PwC has been the knowledge partner with Committee of Sponsored Organizations ("COSO") in all its initiatives, including the latest ERM 2017 framework.

ارتباط بیمه و مدیریت ریسک



- ❖ بیمه همان مدیریت ریسک است ولی عکس آن صادق نیست
- ❖ بیمه زیرمجموعه‌ی مدیریت ریسک و نوعی از انواع آنست
- ❖ مدیریت ریسک برابر با بیمه نیست بلکه بسیار فراتر و گسترده‌تر از بیمه است
- ❖ انجام مدیریت ریسک در شکل جامع و فراگیر، متضمن بیمه نامه‌ها و پوشش‌های بیمه‌ای خوب و صحیح و ایمنی و پیشگیری از خسارت مطلوب هم می‌شود
- ❖ دیسپلین مدیریت ریسک برابر تعاریف و چارچوب‌های بین‌المللی، بسیار گسترده است و تمامی ارکان سازمان از صدر تا ذیل را شامل می‌شود

... ارتباط بیمه و مدیریت ریسک (ادامه)

- ❖ بیمه با ریسک های خالص (Pure) سر و کار دارد
- ❖ بعضی از انواع ریسک مانند ریسک مالی، سوداگرانه اند (Speculative)
- ❖ اعتقاد به گران و ناقص بودن بسته های بیمه ای در دهه ۱۹۵۰
- ❖ خلق مفاهیم خودبیمه گری، حفاظت فردی، ایمنی و بهداشت شغلی، ...
- ❖ شتاب فعالیت های مربوط به توسعه و برنامه ریزی برای مواقع اضطراری در دهه ۱۹۶۰
- ❖ استفاده از مشتقات (Derivatives) به عنوان جایگزین پوشش بیمه ای از اواسط ۱۹۷۰ و سرعت رشد آن در دهه ۱۹۸۰
- ❖ ایجاد مدیریت ریسک به عنوان یک وظیفه سازمانی جدید
- ❖ معرفی مدیریت ریسک مالی به عنوان مکمل مدیریت ریسک های خالص طی دهه های ۷۰ و ۸۰ میلادی
- ❖ شدت بخشیدن مؤسسات مالی، شامل بانک ها و بیمه ها به مدیریت ریسک های بازار و اعتبار
- ❖ اضافه شدن مدیریت ریسک عملیاتی و نقدینگی در دهه ۱۹۹۰
- ❖ ایجاد واحد/دپارتمان و پست سازمانی مدیر ارشد ریسک (CRO) در دهه ۹۰ میلادی.

چهار اسب ارابه مدیریت ریسک (همچنان در حال تحول)



❖ آکچوئرها (Actuaries)

- ✓ استفاده از روش‌های علمی، ریاضیات، آمار و احتمالات
- ✓ اختصاصاً کار در زمینه ارزیابی ریسک‌های بیمه‌ای و صندوق‌های بازنشستگی
- ✓ ورود به سایر حوزه‌های ریسک

❖ مهندسان دوران جنگ (War quants)

- ✓ مهندسان و دانشمندان دوران WWII
- ✓ ابداع روش‌های جدید ریاضی مانند شبیه‌سازی مونت کارلو، PRA، DA و OR

❖ اقتصاددانانها (Economists)

- ✓ توسعه روش‌های ارزیابی و مدیریت ریسک انواع ابزارها و پرتفویهای مالی
- ✓ این روش‌ها امروزه توسط تحلیل‌گران مالی مورد استفاده قرار می‌گیرد
- ✓ همپوشانی این روش‌ها با روش‌های مهندسی

❖ مشاوران مدیریت (Management Consultants)

- ✓ ابداع و معرفی روش‌های کیفی (Soft)
- ✓ انواع ممیزان/حسابرسان (ایمنی، حسابداری، ...)
- ✓ اتکاء بر تجربه شخصی مشاور

مدیریت ریسک به عنوان مترادف بیمه

عدم استفاده از RM در عملیات،
محصولات جدید، بازاریابی، ... تا
اواسط قرن بیستم

RM مترادف با بیمه بوده
است

حصول اطمینان از اعمال کلیه
احتیاطات لازم

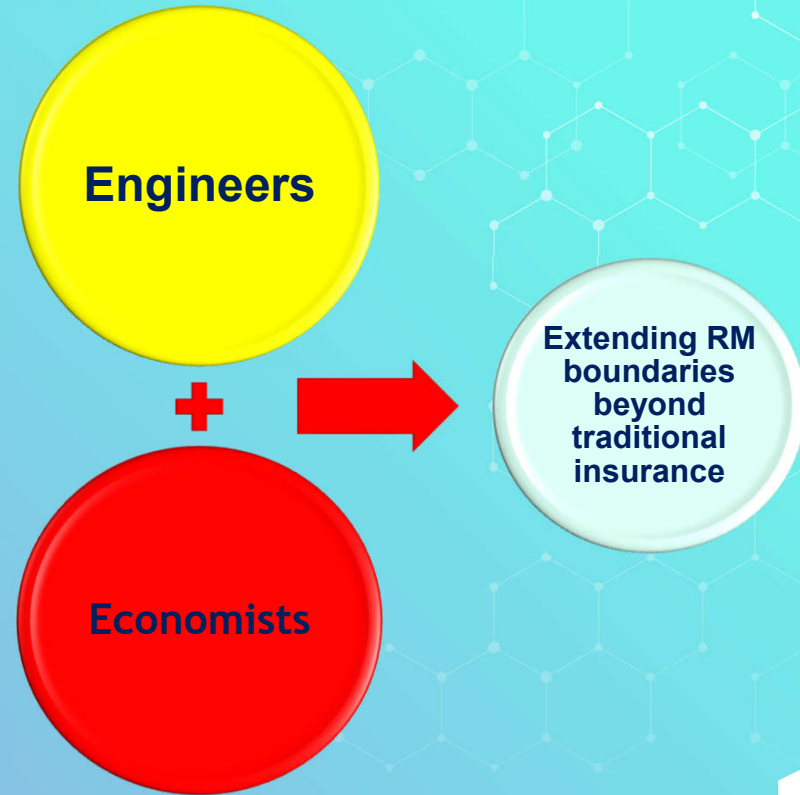
New
products

Insurance

Major
acquisitions

Operations

درنوردیدن مرزهای بیمه سنتی



خود بیمه گری

◆ **گران و ناقص** بودن پوشش‌های متداول بیمه‌ای؛

◆ **عدم پوشش خسارت‌های کوچک توسط بیمه گران** (در قالب فرانشیز، اکسس، ...)

◆ **تعریف خود بیمه گری (Erllich and Becker 1972):**

◆ **خود بیمه گری** عواقب مالی ناگوار ناشی از وقوع حادثه و خسارت‌های مربوط به آن

را پوشش می‌دهد. خود بیمه گری در ساده‌ترین شکل می‌تواند شامل ایجاد یک

ذخیره مالی نسبتاً نقد شونده به منظور پوشش خسارت‌های ناشی از وقوع حادثه و یا

نوسانات منفی بازار باشد

◆ **روش تقلیل ریسک (Risk Mitigation)** که به شکلی فراگیر و گسترده برای کاهش

عواقب مالی بلایای طبیعی مورد استفاده قرار می‌گیرد، نوعی خود بیمه‌گری است.

فعالیت‌های حفاظت از خود (Self-protection)



- ❖ این روش‌ها در سنوات اخیر اهمیت یافته
- ❖ تأثیر بر احتمال یا شدت خسارت قبل از وقوع آن
- ❖ پیشگیری از حادثه یکی از اشکال طبیعی self-protection
- ❖ احتیاط و مراقبت (Precaution)
- ❖ کلیه فعالیت‌های حفاظت و پیشگیری از خسارت بخشی از مدیریت ریسک محسوب می‌شود

رهبری و مدیریت ریسک در قرن ۲۱ ام

Leadership is about making a difference. If leaders of organizations in the 21st Century are to make a difference and grow their organizations to greatness, they must have the capability to navigate in a very risky and dangerous world. Thus, understanding and managing risk has become imperative for successful leadership of organizations in today's world.

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.

برگرفته از مستند *ERM, Frameworks, Elements and Integration* از سری انتشارات مؤسسه IMA.

عوامل تأثیرگذار بر چشم انداز ریسک و مدیریت آن



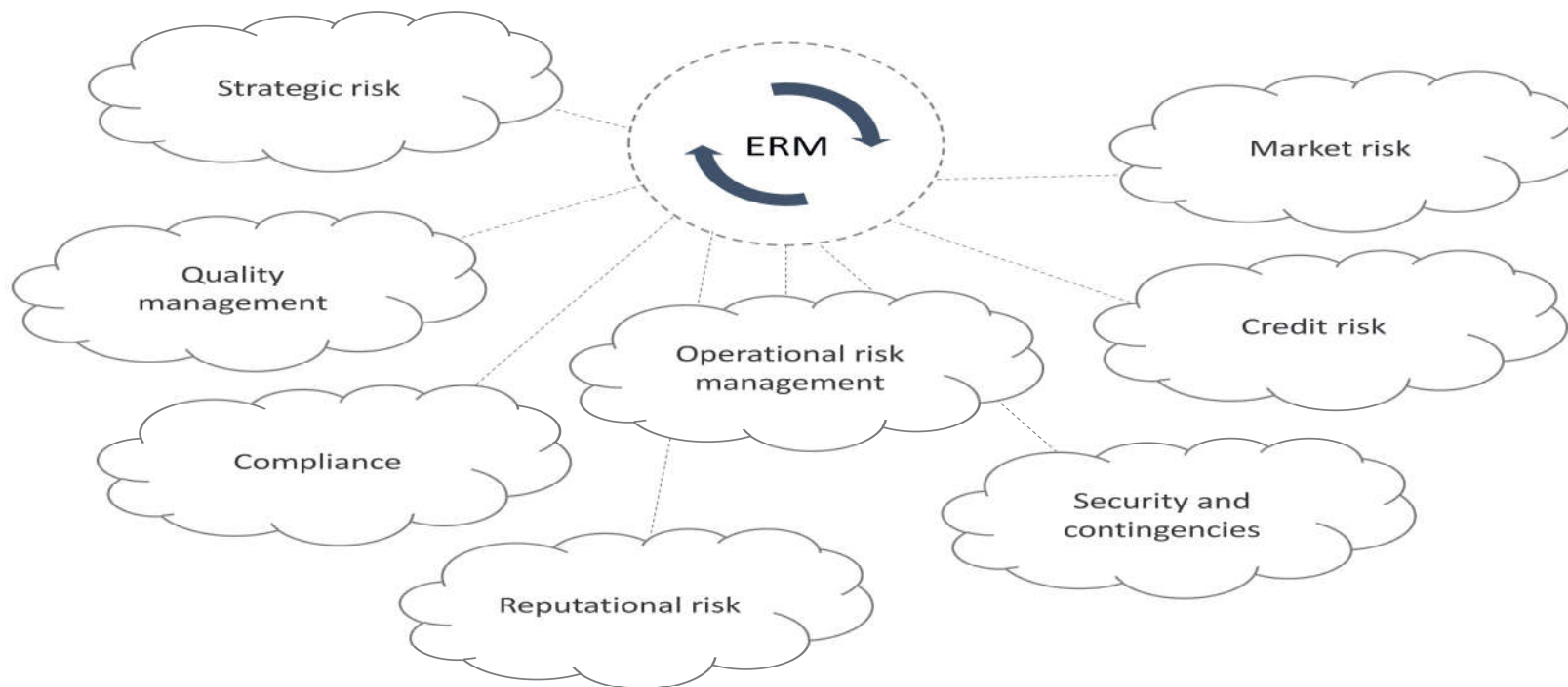
نقش ها و مسئولیت های مدیریت ریسک در یک سازمان

گستره موضوعی سیستم مدیریت ریسک سازمانی (ERM)

- ◆ Financial RM (Market, Credit, Liquidity, ...)
- ◆ DRM/DRR
- ◆ Insurance RM
- ◆ ESG
- ◆ Operational RM
- ◆ Strategic RM
- ◆ Safety/Security RM
- ◆ Fraud RM
- ◆ Compliance RM
- ◆ Cybersecurity RM
- ◆ BCM
- ◆ ...



برخی موضوعات متنوع و مختلف برای هماهنگی و مدیریت توسط CRO



تنوع مزایای سیستم مدیریت ریسک سازمانی (ERM)

❖ افزایش دامنه فرصت‌هایی که در صورت مدیریت مؤثر، نتایج مثبت را تضمین می‌کند

❖ بهبود مدیریت و افزایش نتایج پروژه‌ها

❖ مدیریت بهتر قراردادها

❖ کاهش تغییرپذیری (واریانس) عملکرد

❖ استفاده متمرکز و مؤثر از منابع

❖ اطمینان بیشتر در ارائه ابتکارات موفق

❖ رویکرد پیشگیرانه به مدیریت ریسک و نحوه پشتیبانی آن از اهداف استراتژیک

❖ پایداری کسب و کار

❖ حمایت از رویکرد رشد پایدار برای کسب و کار؛ و

❖ شناسایی و مدیریت ریسک‌های سازمانی

RMS functions as per ICP 8:

- ◆ Risk Management
- ◆ Actuarial Matters
- ◆ Compliance
- ◆ Internal Audit

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

- ◆ ابزارها، تکنیک‌ها، فرآیندها
- ◆ طبقه بندی انواع ریسک و فهم مشترک آن
- ◆ **اشتهاء و تolerانس (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
- ◆ 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

مدل ۳ لایه دفاعی

OWNERS			
Board/ Audit Committee			
Executive Management			
1 st Line of defence	2 nd Line of defence	3 rd Line of defence	
Operational management, Internal controls	Control activities and functions in staff organisation - Controller - Quality and security - Risk Management - Compliance - HSE etc.	Internal Audit	External audit
Operational controls performed by line management.	Various forms of ongoing risk management monitoring and control activities which are performed by administrative and control functions	The internal audit function will provide objective assurance on the effectiveness of the processes for governance, risk management and control, including the manner in which the first and second lines of defence operate.	External accounting control providing an independent opinion of financial reporting

مدل سه لایه دفاعی راه ساده و موثری برای ارتقای ارتباطات به منظور مدیریت و کنترل ریسک از طریق تبیین نقش‌ها و وظایف ضروری، ارائه می‌کند

در این مدل، مدیریت عملیاتی و کنترل‌های داخلی اولین خط دفاعی مدیریت ریسک است وظایف مختلف نظارت بر ریسک داخلی و انطباق ایجاد شده توسط مدیریت دومین خط دفاعی؛ و

تضمین مستقل، سومین خط دفاعی است

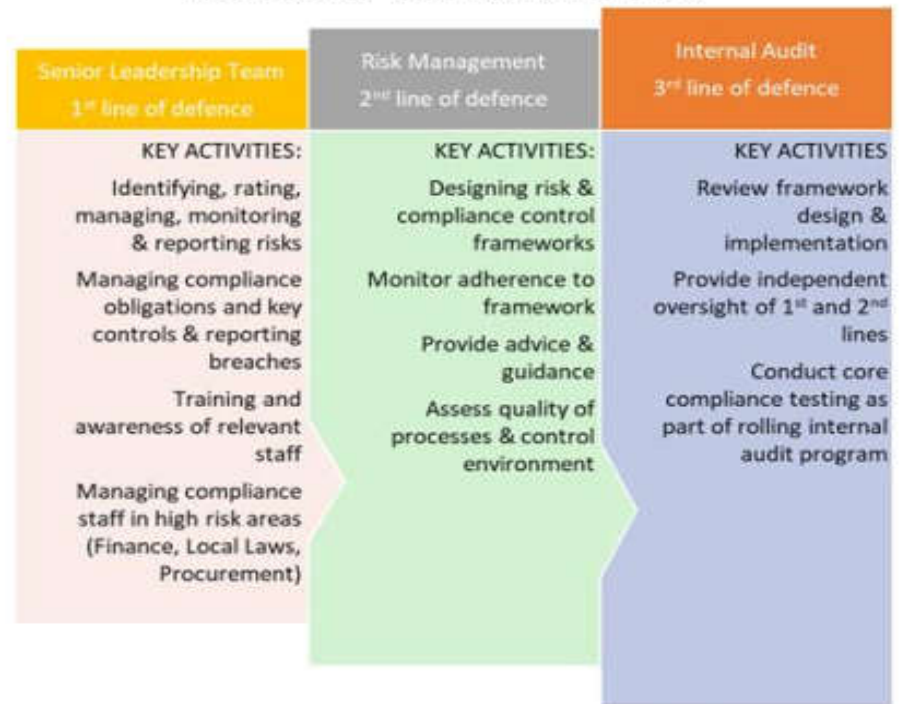
برای اطلاعات بیشتر: "IIA POSITION PAPER 2013: THE THREE LINES OF DEFENSE IN EFFECTIVE RISK MANAGEMENT AND CONTROL"

... مدل ۳ لایه دفاعی (ادامه)

LINES OF ACCOUNTABILITY & REPORTING



3 LINES OF DEFENCE MODEL



مرور برخی اصطلاحات و مفاهیم مهم مدیریت ریسک



کلیات

- ❖ 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).

واژگان مربوط به مدیریت ریسک

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**



حاکمیت شرکتی و مدیریت ریسک

حاکمیت/حکمرانی شرکتی

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

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

مدیریت ریسک باید با حاکمیت شرکتی در یک چارچوب واحد برای هر سازمانی که توسط هیئت مدیره
یا سایر نهادهای حاکمیتی نظارت می‌شود، 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

- ◆ **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 37001:2018; Clause 5.3 "Integration"

◆ **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.

درباره حاکمیت شرکتی (با رویکرد شرکت‌های بیمه)

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.

◆ آیین‌نامه ۹۳ شورای عالی بیمه (بدون
تعریف حاکمیت شرکتی)

◆ دستورالعمل ماده ۱۱ آیین‌نامه ۹۳

◆ اصل بنیادین شماره ۷ انجمن

بین‌المللی ناظران بیمه‌ای (IAIS -)
(ICP7)

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 (effects
of uncertainty on objectives) (ISO Guide
31073:2022

◆ تعریف مدیریت ریسک: "فعالیت‌های هماهنگ شده
برای **هدایت** و **کنترل** یک سازمان با توجه به ریسک"
(ISO Guide 31073:2022)

سایر تعاریف ریسک

◆ **COSO ERM 2017-** *“possibility that events will occur and affect the achievement of strategy and business objectives.”*

◆ **James Lam, 2017 –** *“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.”*

◆ امکان رویداد وقایع و اثر آنها بر دستیابی به استراتژی و اهداف کسب و کار
(COSO ERM 2017)

◆ ریسک متغیری است که می‌تواند موجب انحراف از رویداد مورد انتظار شده و از اینرو بر تحقق اهداف کسب و کار و عملکرد کلی سازمان اثر بگذارد
(James Lam, 2017)

با این تعریف، ریسک یک متغیر تصادفی دارای تابع توزیع احتمال است.

نقش کلیدی مدیریت ریسک در سازمان

تعیین
استراتژی

COSO ERM 2017 – *Integrating
Strategy with Performance*

پیشگیری
از
خسارت

مدیریت
ریسک

تحقق
اهداف

VUCA
(WEF,
2018)

تصمیمات
آگاهانه

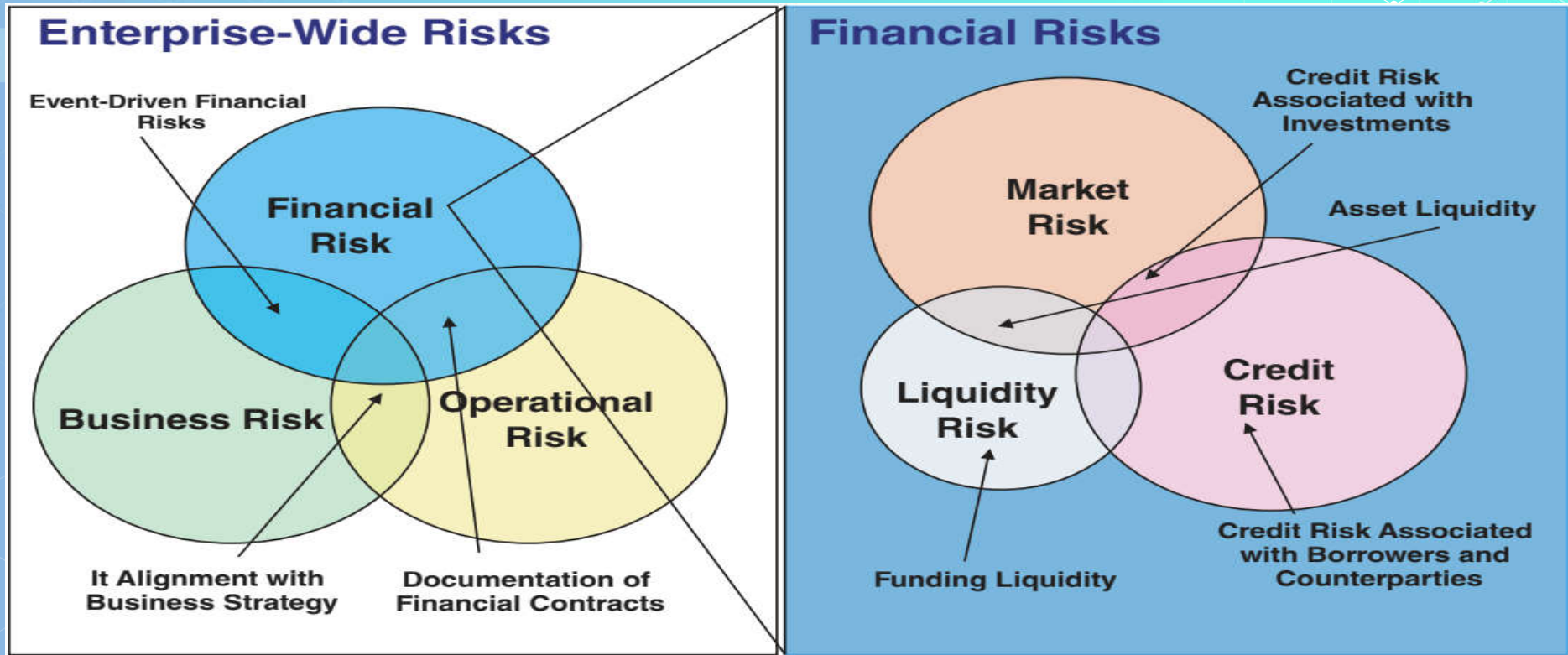
انواع ریسک (فهرست کامل نیست)

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

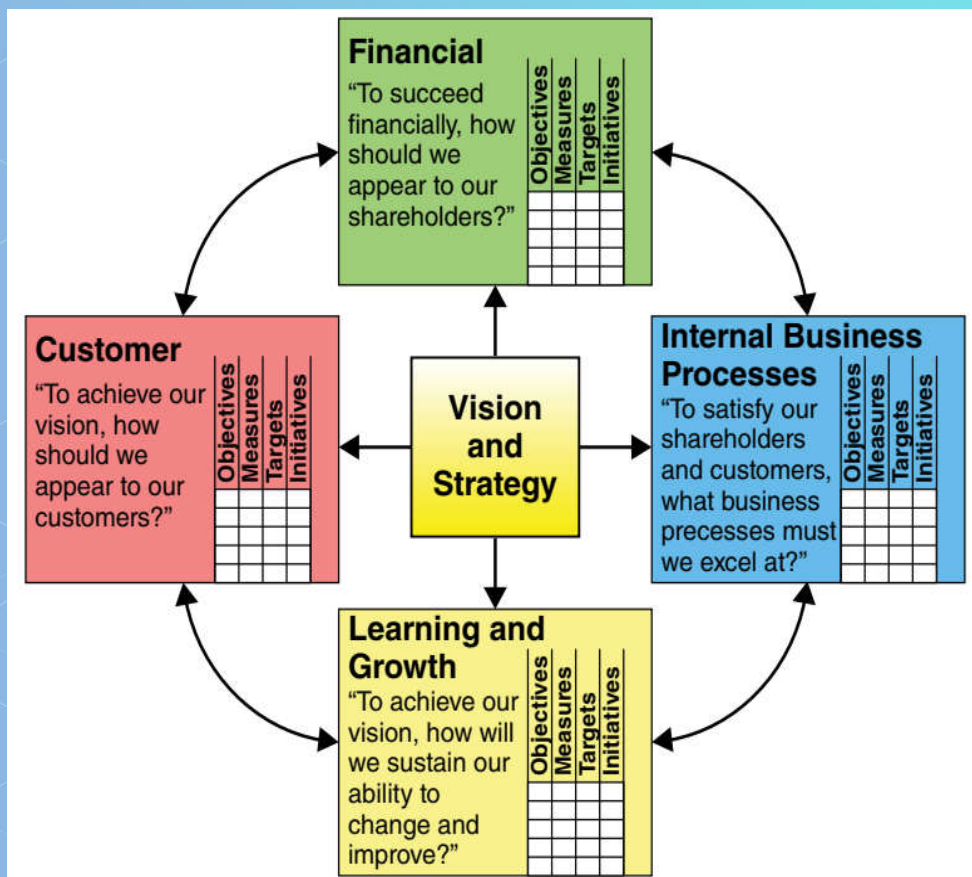
◆ طبقه بندی استاندارد برای انواع ریسک وجود ندارد.
(این سایت را ملاحظه نمایید: www.52risks.com)

Enterprise-Wide Risks



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

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



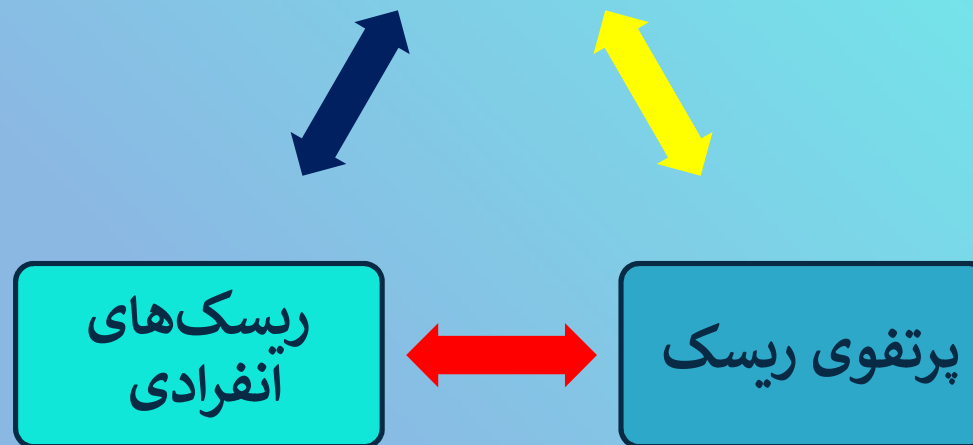
- ◆ اصول بنیادین بیمه ای ۸ و ۱۶ (ICPs 8 & 16) از مجموعه IAIS 2019
- ◆ تأکید بر نگاه کل نگر (Holistic) به مدیریت ریسک در قالب ERM به جای جزءنگری (رویکرد سیلویی)
- ◆ تمرکز بر استراتژی و پروفایل ریسک سازمان
- ◆ تعریف شاخص‌های کلیدی ریسک (KRI)
- ◆ تجزیه و تحلیل برنامه راهبردی سازمان با استفاده از تکنیک‌های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

پروفایل ریسک



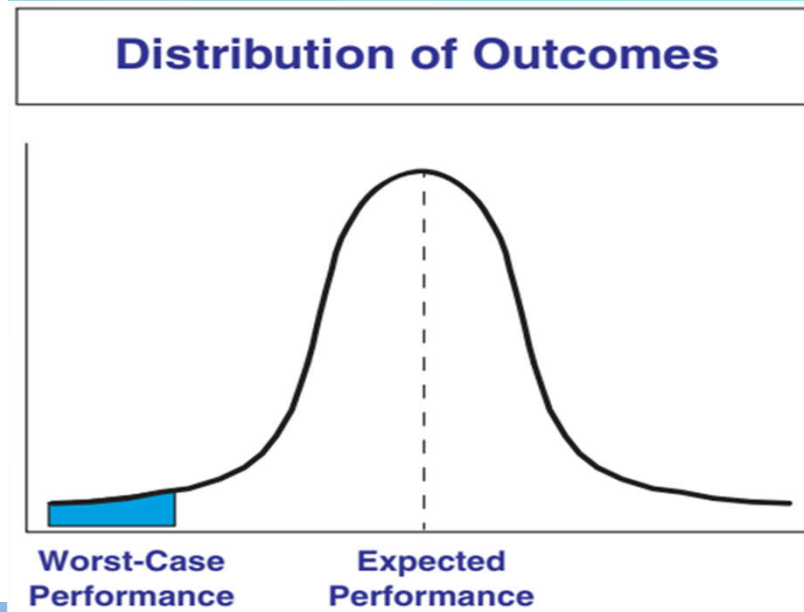
سطوح مدیریت ریسک سازمانی

پروفایل ریسک



متغیر تصادفی ریسک و تابع توزیع احتمال آن

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.



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.

تحليل داده ريسک

- ◆ موقعيت داده (ميانه/ميانگين/مد)
- ◆ پراکندگي داده (واريانس و انحراف معيار)
- ◆ ارتباط و همبستگي داده (رگرسيون و ضريب همبستگي)



تابع توزیع پروفایل ریسک

Credit Risk

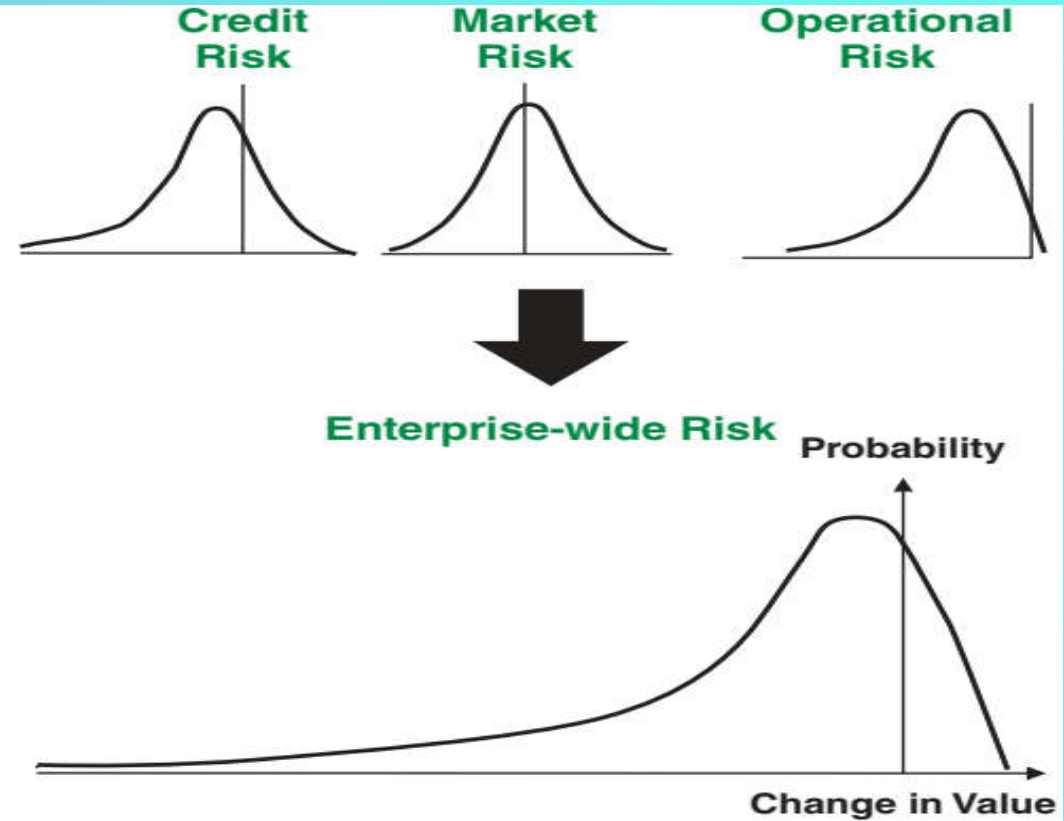
Earnings volatility due to variation in credit losses

Market Risk

Earnings volatility due to market price movements

Operational Risk

Earnings volatility due to people, process, technology, or one-off events



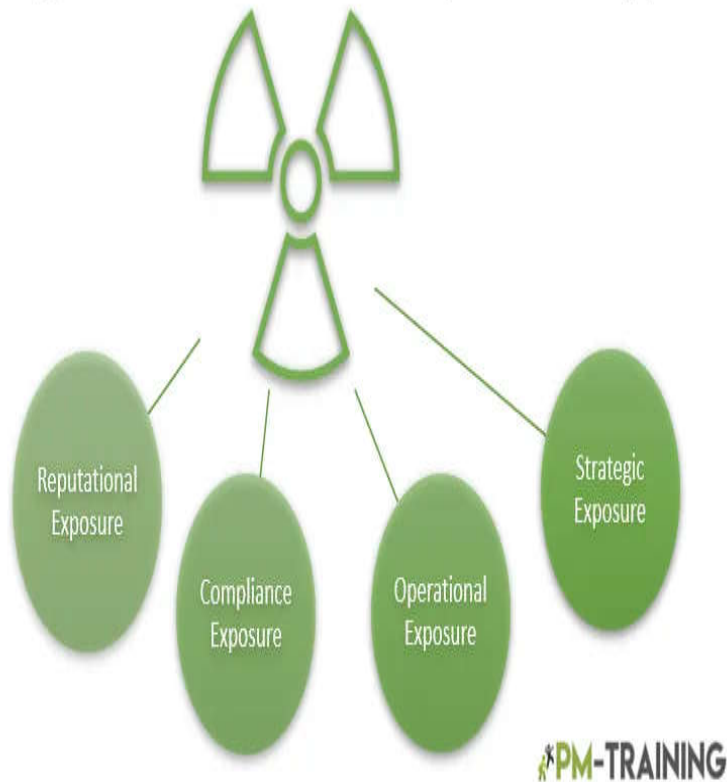
عوامل مؤثر بر پروفایل ریسک سازمان

◆ 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).

در معرض (مخاطره) بودن (Exposure)

Organizational Risk Exposure Types



◆ 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 وام گیرنده مواجه است؛

◆ اندازه گیری exposure خصوصاً برای ریسک های بازار و

اعتبار دشوار است؛

◆ برای ریسک های operational و compliance بیشتر کیفی

اندازه گیری می شود؛

◆ اندازه گیری exposure منجر به سناریوی بدترین حالت

ممکن می شود؛

● 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 می دهد؛

◆ هر چه Volatility بیشتر باشد، ریسک بزرگتر است؛

● **مثال (ریسک اعتباری):** تعداد موارد نکول (عدم بازپرداخت) در کارت های 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 آتش سوزی آن مرکز محتمل تر است؛

در صورت آتش سوزی مرکز داده، خسارت وارده سنگین تر 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.

	Probability of Occurrence Definitions				
	Extremely improbable	Extremely remote	Remote	Reasonably probable	Frequent
Qualitative definition	Should virtually never occur in the whole fleet life.	Unlikely to occur when considering several systems of the same type, but nevertheless has to be considered as being possible.	Unlikely to occur during the total operational life of each system but may occur several times when considering several systems of the same type.	May occur once during total operational life of one system.	May occur once or several times during operational life.
Quantitative definition	< 10 ⁻⁹ per flight hour	10 ⁻⁷ to 10 ⁻⁹ per flight hour	10 ⁻⁵ to 10 ⁻⁷ per flight hour	10 ⁻³ to 10 ⁻⁵ per flight hour	1 to 10 ⁻³ per flight hour

شدت

- ◆ میزان خسارتی که احتمالاً اتفاق می افتد؛
- ◆ 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.

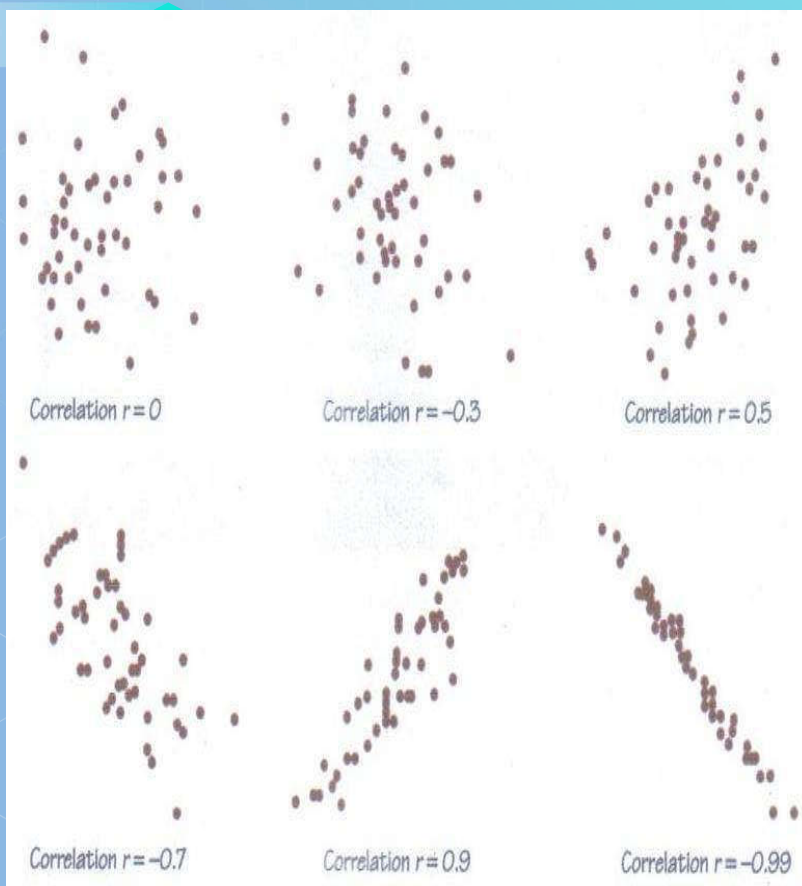
SEVERITY		
Verbal	Numeric	Description
Catastrophic	5	Likely to result in death
Critical	4	Potential for severe injury
Moderate	3	Potential for moderate injury
Minor	2	Potential for minor injury
Negligible	1	No significant risk of injury

افق زمانی



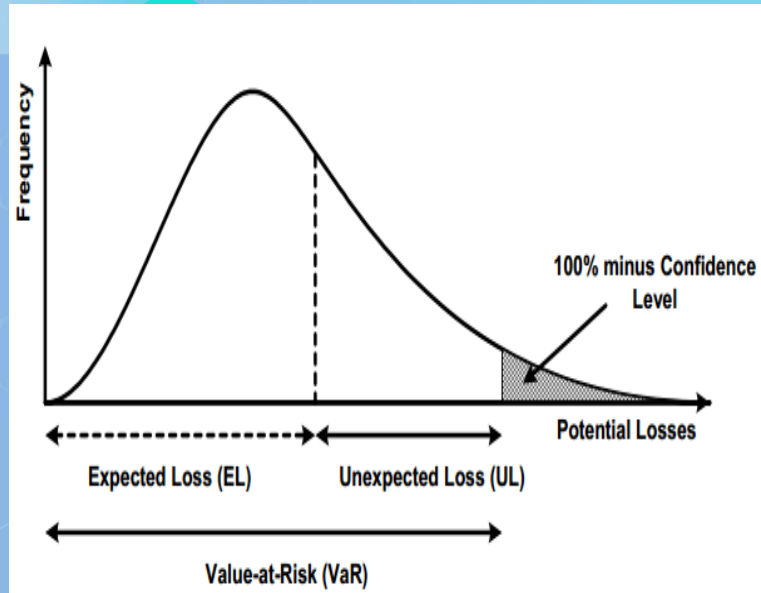
- ◆ طول مدت در معرض ریسک بودن؛
- ◆ هر چه این مدت بیشتر باشد، ریسک بزرگتر است؛
- ◆ مثال: دادن وام یک ساله یا ده ساله به یک قرض گیرنده؛
- ◆ اوراق قرضه دارای پشتیبانی دولتی نسبت به سهام فهرست نشده و مشتقات از ریسک کمتری برخوردارند چراکه افق زمانی نقدشوندگی آنها کوتاهتر است؛
- ◆ در مورد ریسک عملیاتی چطور؟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

همبستگی



- ◆ چگونه 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 می شود؛
- ◆ ریسک های دارای همبستگی بالا، باعث افزایش تمرکز ریسک می شوند؛
- پرداخت وام به یک صنعت واحد یا سرمایه گذاری 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 می توان از روش تفکیک ریسک استفاده کرد؛

سرمایه



دلایل اصلی نگهداری سرمایه (کاری) در سازمانها:

- انجام سرمایه‌گذاری و پرداخت هزینه‌ها؛
- جبران خسارات ریسک‌های 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.



**استانداردها و چارچوب‌های مدیریت ریسک
(به عنوان مثال: ISO 31000، COSO، ERM، ...)**

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 می‌سازد تا با پرداختن به الزامات اساسی با توجه به حاکمیت و خط مشی (از جمله اشتباهات ریسک)، تجزیه و تحلیل ریسک، مدیریت ریسک، و نظارت و گزارش، تصمیمات آگاهانه تری درباره **ریسک/بازده** اتخاذ کنند.

COSO ERM 2017 – Integrating Strategy with Performance



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

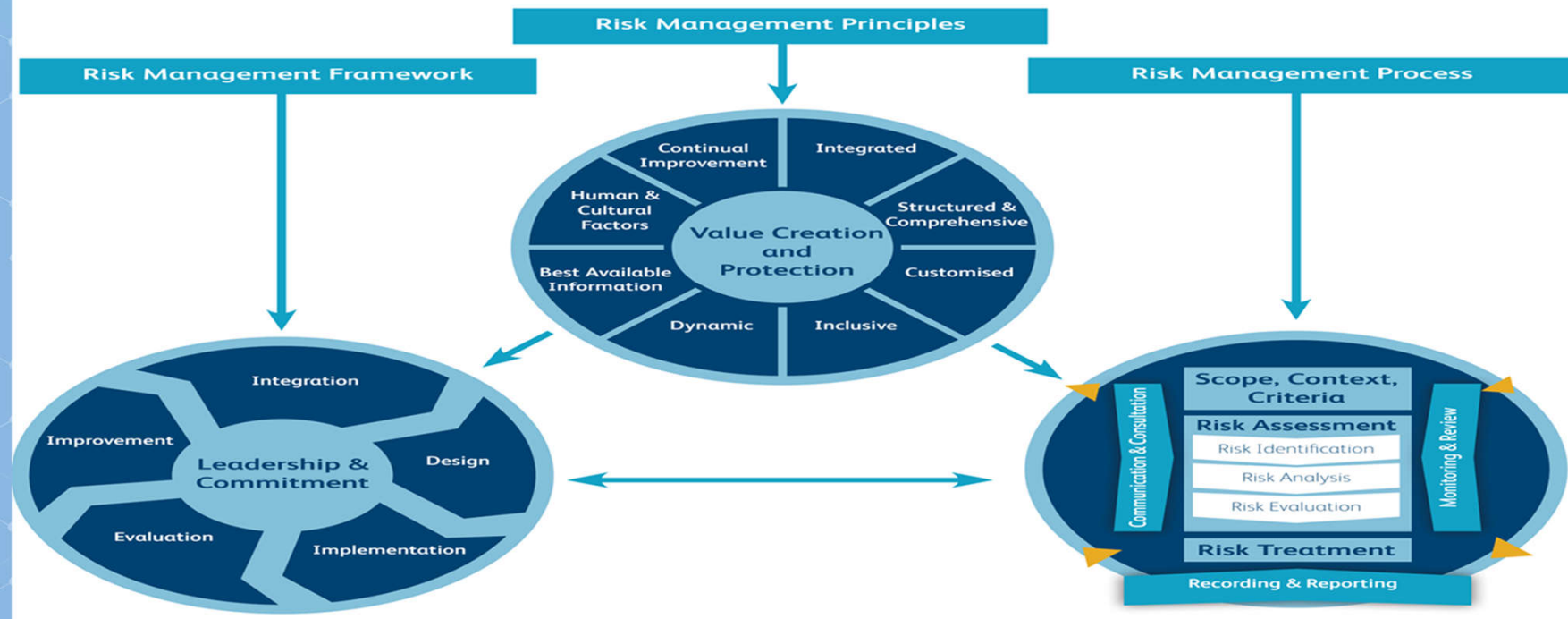


Information, Communication, & Reporting

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

ISO 31000:2018 –Risk Management Guidelines

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



risk management

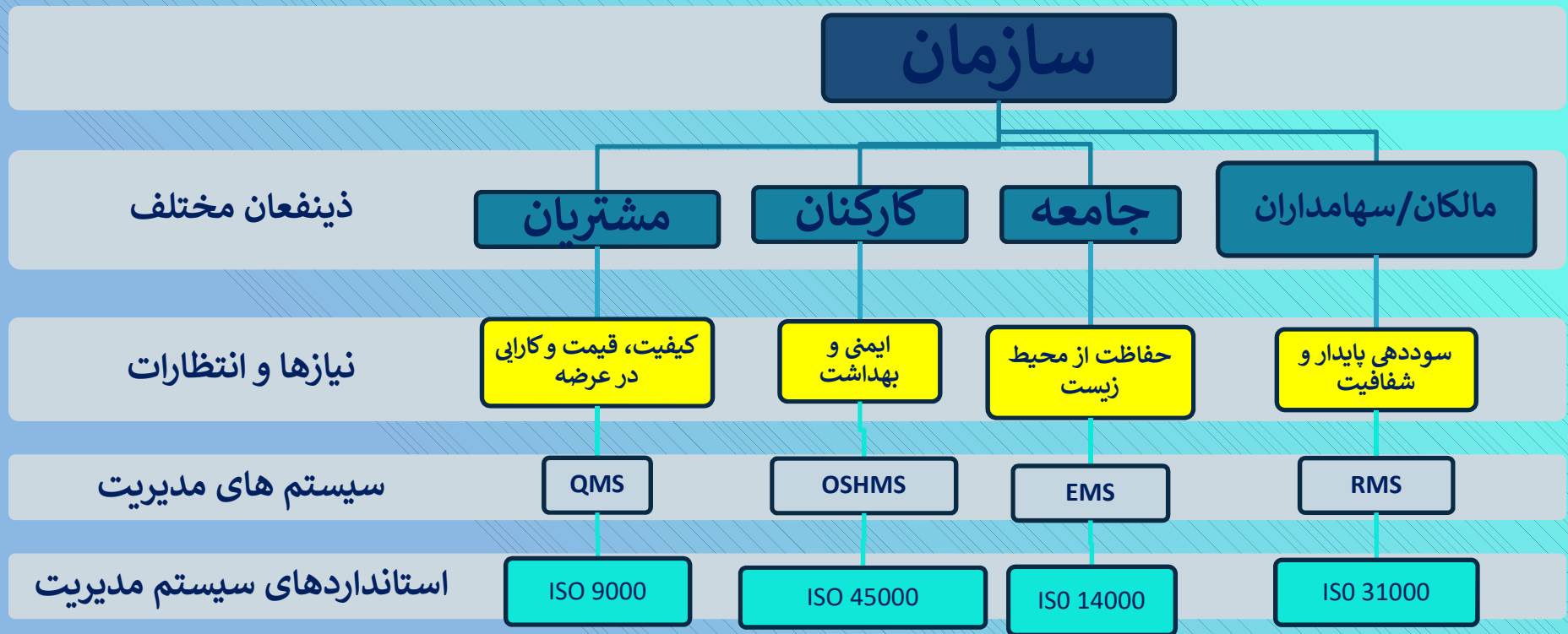
coordinated activities to direct and control an organization (3.3.7) with regard to risk (3.1.1)

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)**.

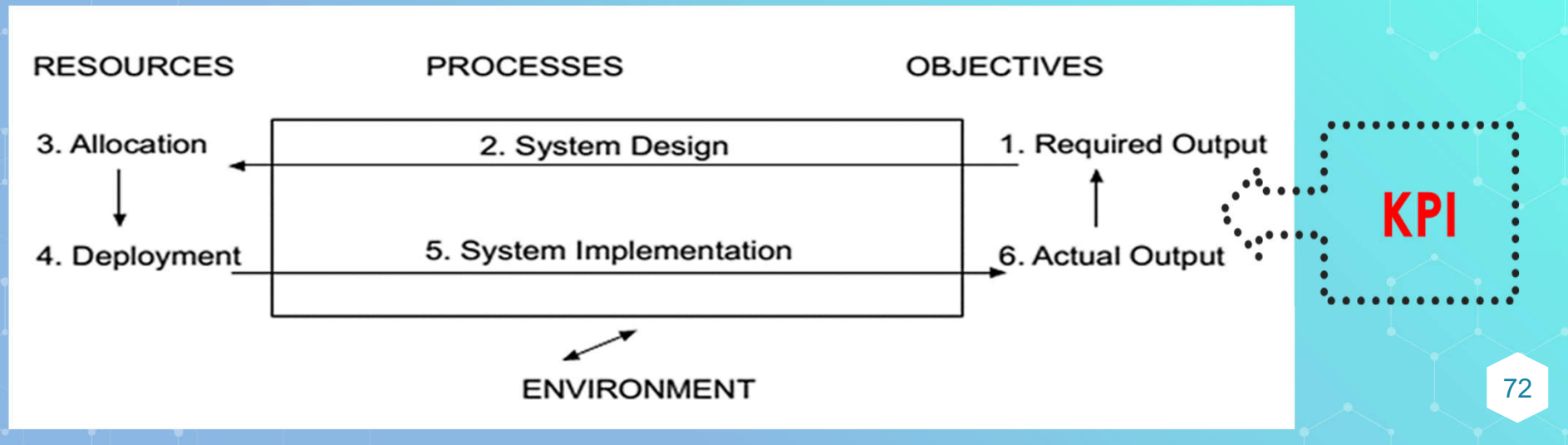
ذینفعان سازمان و نیازها و انتظارات آنها



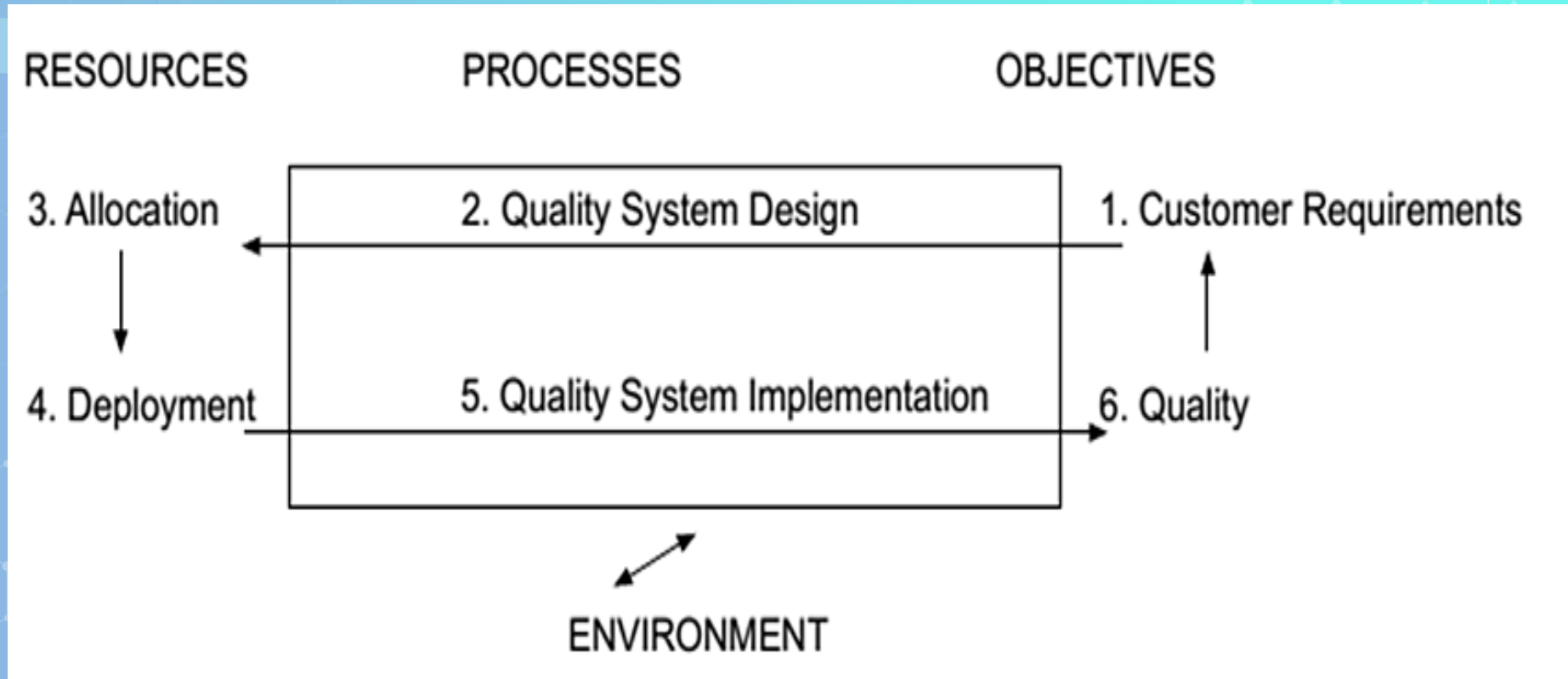
The main objective of each MSS is to systematically guide an organization **to satisfy each specific group of stakeholders and to supply their needs and expectations.**

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.



شمای کلی سیستم مدیریت کیفیت



تعدادی از معروف ترین استانداردهای سیستم های مدیریتی سازمان ISO

- **ISO 9001:2008 – Quality Management Systems**
 - ISO/TS 16949:2009 – Quality Management System requirements for the automotive sector
 - ISO 13485:2003 – Quality Management System requirements for medical devices
- ISO 14001:2004 – Environmental Management Systems
- ISO 45001 – Occupational Health and Safety Management Systems
- **ISO 31000:2018 – Risk Management - Principles and Guidelines**
 - ISO Guide 31073:2022 – 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

عناصر تشکیل دهنده سیستم مدیریتی (IAIS 2019)

As per ICP 8, the systems typically include:

- ❖ **Strategies** setting out the approach of the insurer for dealing with specific areas of risk and legal and regulatory obligation
- ❖ **Policies** defining the procedures and other requirements that members of the Board and employees need to follow
- ❖ **Processes** for the implementation of the insurer's strategies and policies; and
- ❖ **Controls** to ensure that such strategies, policies and processes are in fact in place, are being observed and are attaining their intended objectives.

طبق ICP 8 عناصر تشکیل دهنده

سیستمها عبارتند از:

- ❖ استراتژیها
- ❖ خط مشیها
- ❖ فرآیندها
- ❖ کنترلها

عناصر کلیدی چارچوب مدیریت ریسک سازمانی

“

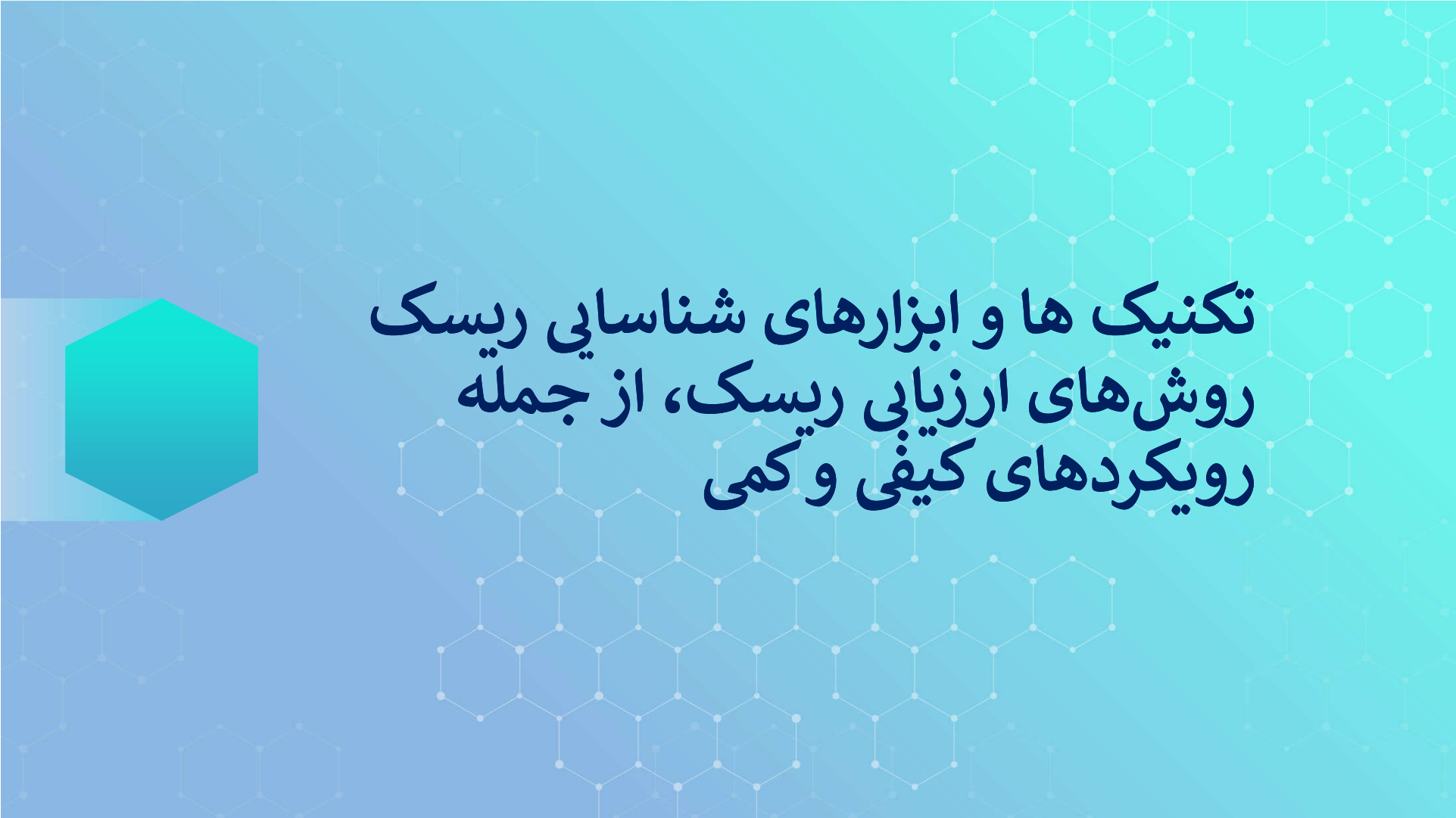
- ◆ ایجاد سیاست‌ها و فرآیندهایی برای **مواجهه** با ریسک‌های شناسایی شده (treatment)
- ◆ **نظارت و مدیریت** ریسک‌ها در طول زمان در سطح عملیاتی
- ◆ ایجاد برنامه‌های اضطراری برای خسارات سنگین و شرایط اضطراری که ممکن است رخ دهد (BCM)
- ◆ ارزیابی منظم **کفایت** چارچوب مدیریت ریسک.

- ◆ 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 می‌تواند دستیابی به اهداف سازمان و همچنین فرصت‌هایی برای ایجاد ارزش را به خطر بیندازد.

ارتباط عناصر کلیدی چارچوب ERM



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



**تکنیک ها و ابزارهای شناسایی ریسک
روش های ارزیابی ریسک، از جمله
رویکردهای کیفی و کمی**

تکنیک ها و ابزارهای شناسایی و روشهای کیفی و کمی ارزیابی ریسک



IEC 31010

Edition 2.0 2019-08

INTERNATIONAL
STANDARD

NORME
INTERNATIONALE



Risk management – Risk assessment techniques

Management du risque – Techniques d'appréciation du risque

for more information please follow

@jefrimron
@jeapconsultant

Jeap Consultant Library

◆ استاندارد مرجع:

IEC 31010:2019

Risk Management – Risk
Assessment Techniques

◆ ۱۰ دسته و مجموعاً ۴۲ تکنیک

شناسایی و ارزیابی ریسک
(کیفی و کمی)

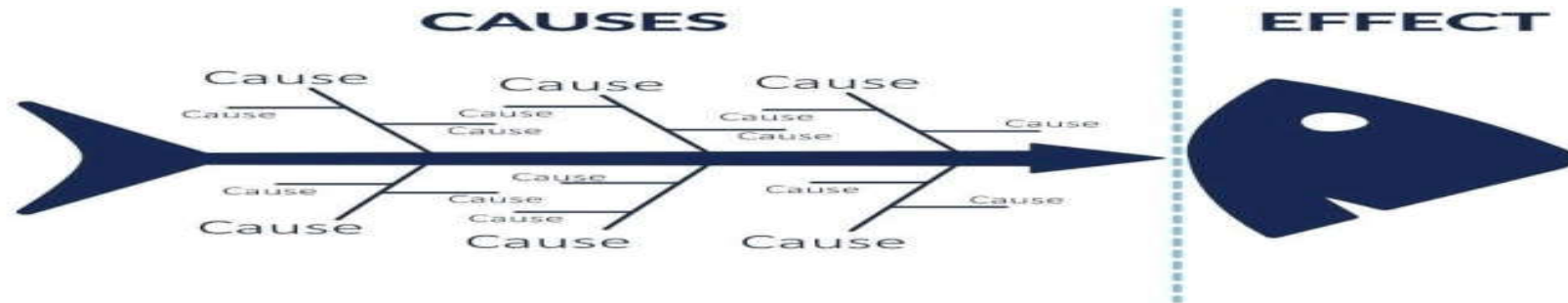
تکنیک‌هایی برای شناسایی ریسک

- ◆ **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

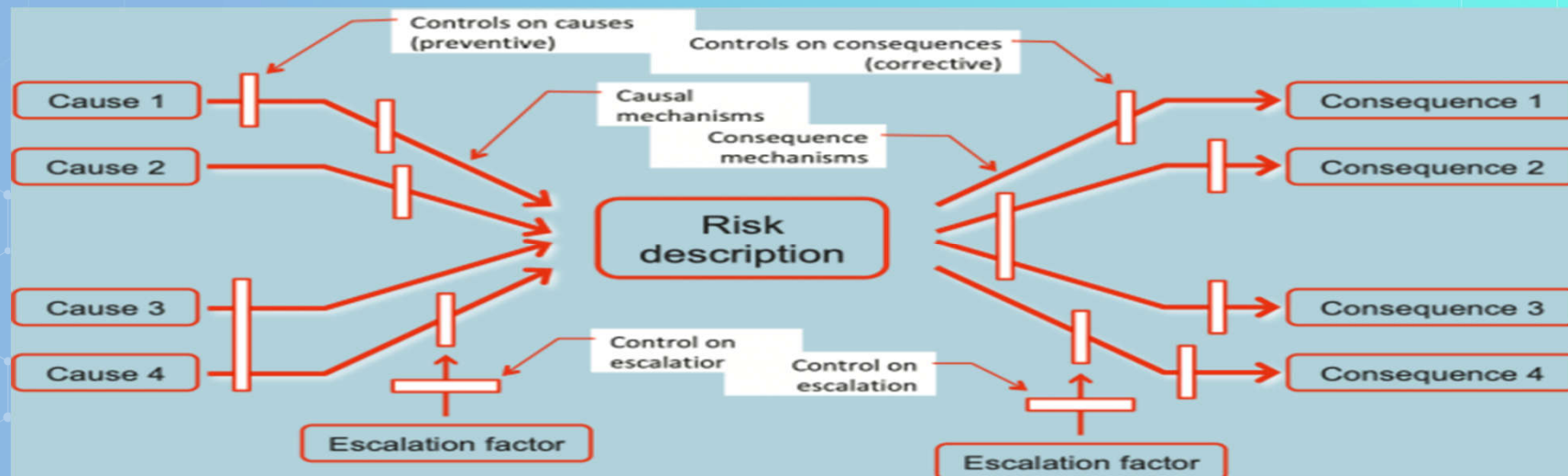
ROOT CAUSE ANALYSIS FISHBONE METHOD



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

تکنیک‌هایی برای تجزیه و تحلیل کنترل‌ها

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



تکنیک‌هایی برای فهم پیامدها و احتمالات

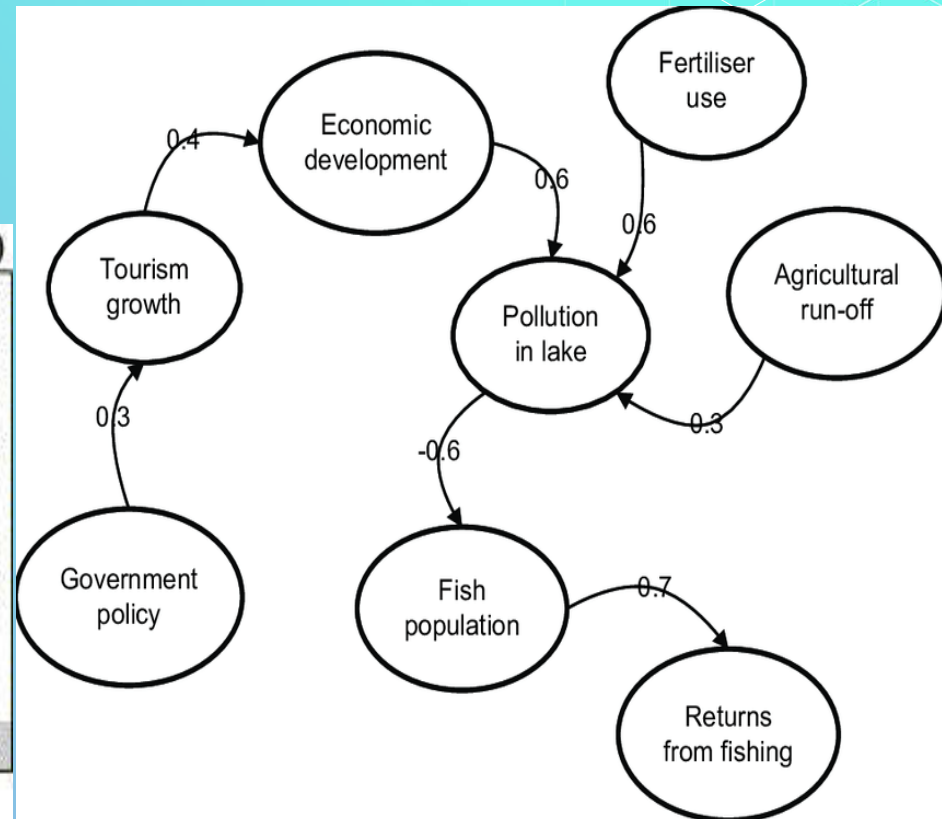
- ◆ Bayesian analysis
- ◆ Bayesian networks and influence diagrams
- ◆ Business impact analysis (BIA)
- ◆ Cause-consequence analysis (CCA)
- ◆ Event tree analysis (ETA)
- ◆ Fault tree analysis (FTA)
- ◆ Human reliability analysis (HRA)
- ◆ Markov analysis
- ◆ **Monte Carlo simulation**
- ◆ Privacy impact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

تکنیک‌هایی برای تجزیه و تحلیل وابستگی‌ها و تعاملات

- ◆ Causal mapping
- ◆ Cross impact analysis

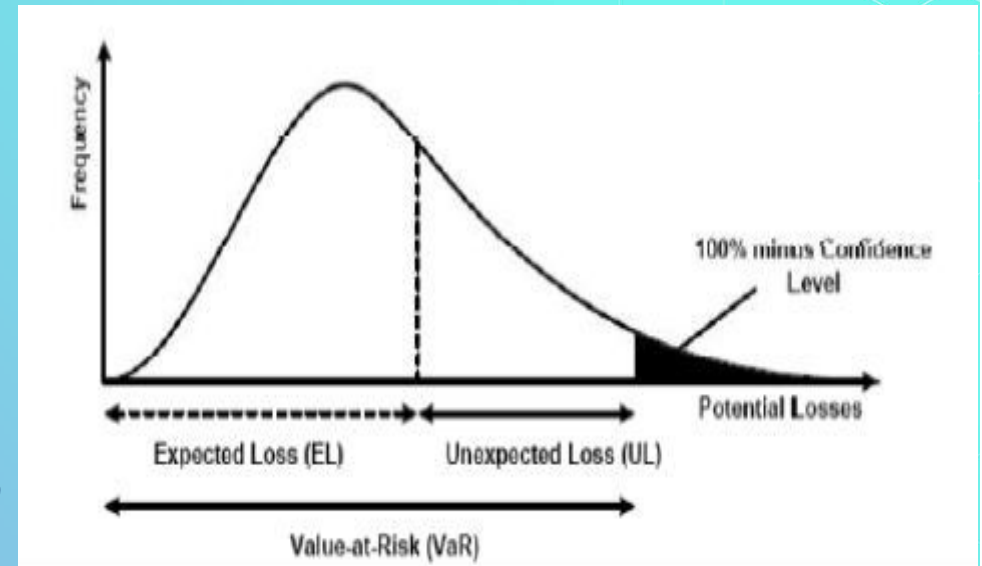
	1	2	3	4	5	6	7	8	9	10	
1. National income	1	0	2	0	0	2	3	5	0	0	2
2. Number of terrors	2	0	0	3	4	4	0	4	0	0	2
3. Deterrent power of law	3	2	0	0	0	4	0	0	0	0	0
4. Rate of violence shown in media	4	0	0	0	0	2	0	0	0	0	3
5. Rate of armament	5	0	4	0	0	0	0	0	0	0	1
6. Education level	6	4	3	0	0	3	0	4	1	0	0
7. Rate of migration	7	3	0	0	0	0	4	0	0	0	0
8. Technological and industrial development	8	3	0	0	0	1	3	3	0	0	1
9. Incorrect state policies	9	5	4	2	0	3	3	4	2	0	1
10. Market volume of security equipment	10	0	1	0	0	0	0	0	0	0	0

5: very strong, 4: strong, 3: average, 2: weak, 1: very weak, 0: no relationship



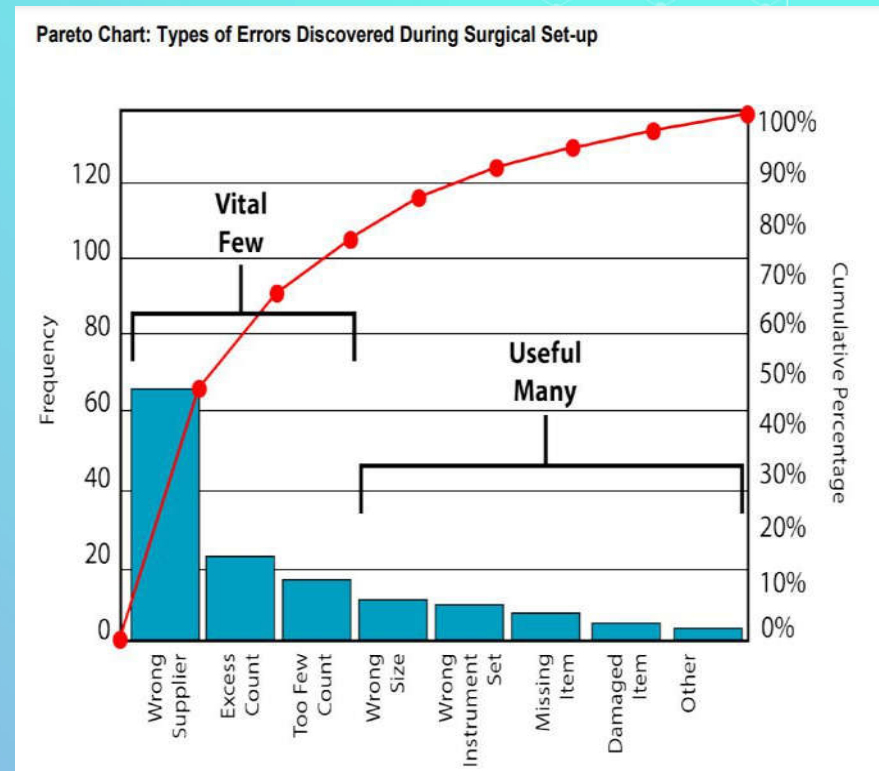
تکنیک های اندازه گیری ریسک

- ◆ 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

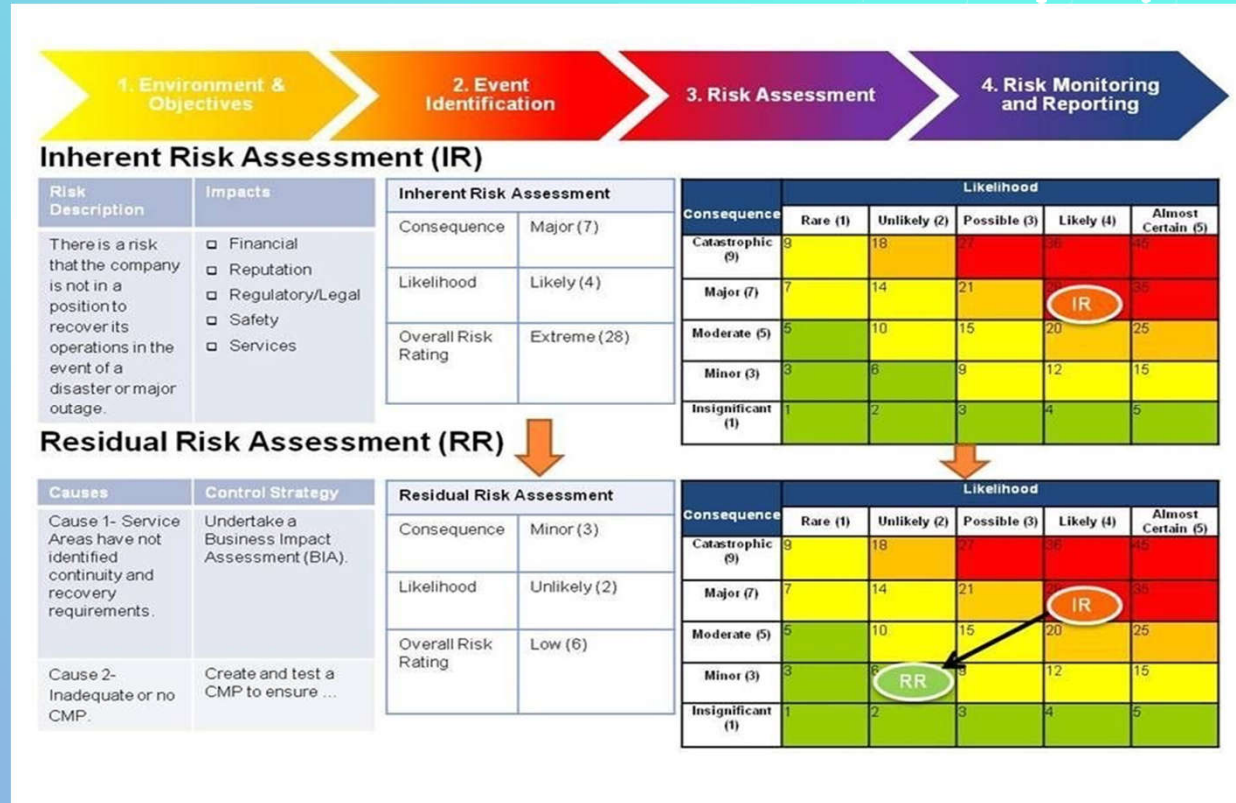
- ◆ Cost/benefit analysis (CBA)
- ◆ Decision tree analysis
- ◆ Game theory
- ◆ Multi-criteria analysis (MCA)

MCDCA Performance Matrix

	Alternative			Criterion Weights
	1	2	3	
Efficacy	##	##	##	##
Safety	##	##	##	##
Quality of Life	##	##	##	##
Functional Status	##	##	##	##
Dosing Convenience	##	##	##	##
Price	##	##	##	##
Cost-Effectiveness	##	##	##	##
Budget Impact	##	##	##	##

تکنیک هایی برای ثبت و گزارش دهی

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



روند تکنیک‌های شناسایی و ارزیابی ریسک



تکنیک های ضروری برای یادگیری و استفاده

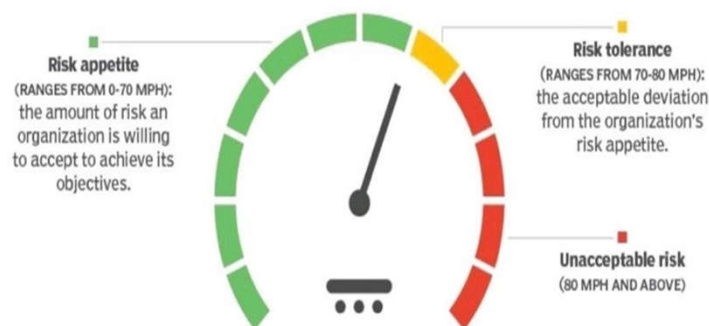
- ◆ **Monte Carlo simulation**
- ◆ Decision tree
- ◆ Risk return spectrum
- ◆ Scenario analysis
- ◆ Business impact analysis
- ◆ PERT
- ◆ Sensitivity analysis
- ◆ Lessons learned
- ◆ Data analysis
- ◆ Horizon scanning
- ◆ ...

اشتهاء و تحمل (تفرانس) ریسک

اشتهاء و حد تحمل ریسک

Risk appetite vs. risk tolerance

If risk appetite represents the official speed limit of 70, risk tolerance is how much faster you can go before likely getting a ticket.



SOURCE: MIKE CHAPPEL, SPEEDOMETER: UNXP/GETTY IMAGES

©2022 TECHTARGET. ALL RIGHTS RESERVED TechTarget

- ◆ تعیین اشتهای ریسک و تolerانس به وضوح پایه و اساس مناسبی برای مدیریت ریسک فراهم می کند
- ◆ اغلب این دو عبارت به جای هم استفاده می شوند
- ◆ 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 بیانیه های ریسک پذیری مورد تأیید هیئت مدیره اند
- ◆ هیئت مدیره از مدیریت ارشد انتظار دارند که در تعقیب اهداف استراتژیک سازمان عمل کنند

... اشتباهای ریسک و حد تحمل

بسیاری از سازمان‌ها برای انواع تصمیم‌گیری‌ها و فعالیت‌های کاری سطوح اشتباهی ریسک را مستندسازی کرده‌اند. مانند:

- ❖ تفکیک وظایف
- ❖ حدود تأمین مالی و معاملات
- ❖ معیارهای انتخاب پیمانکار
- ❖ حدود و سقف سپرده گذاری در بانک
- ❖ تفرانس 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 پروژه‌های سرمایه‌گذاری؛ و
- ❖

ملاحظات اثرگذار بر اشتباهی ریسک سازمان



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.

اشتهای ریسک چیست؟



◆ در ۱۰ درصد مواقع اشتهای ریسک توسط قانون و مقررات تعیین می‌شود. مانند:

❖ تفرانس 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 می‌کند. مثل سقف پرداخت خسارت، تخفیفات حق بیمه، ...

◆ در ۸۰ درصد مواقع بستگی به رویکرد تصمیم‌گیری 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 اشتباهی 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 اشتباهی ندارند، واحد مدیریت ریسک بایستی با واحدهای اجرایی برای تعیین و پیشنهاد سطوح اشتباه همکاری کند.

...

بازنگری سند اشتباهات 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 اشتباهات ریسک مشخص است و کاری که مدیر ریسک باید انجام دهد، تأیید و تصدیق و پایش و بازنگری انجام آنهاست

درباره اشتها و تolerانس ریسک بیشتر بدانیم ...

◆ برای اطلاعات بیشتر در خصوص اشتها و تolerانس 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

تعريف ايزو ۳۱۰۷۳ درباره مواجهه/رفتار با ريسک

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 می‌کند.

◆ معمولاً جزئیاتی را در مورد موارد زیر ارائه می‌دهد:

- ❖ اقداماتی که باید انجام شود و ریسک‌هایی که به آنها رسیدگی می‌شود
- ❖ 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 تolerانس ریسک، مستند زیر را مطالعه نمایید:

IIRM, 2015; “A Practical Guide 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 برنامه‌ریزی شده 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، اندازه‌گیری و گزارش دهی سازمان.

ایزو ۳۱۰۰۰ ویرایش ۲۰۱۸

مستندسازی و گزارش دهی

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 فعالیت‌های مدیریت ریسک دارند.

گزارش دهی 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.
- ◆ گزارش دهی موثر ریسک به استحکام حاکمیت شرکتی کمک می کند.
- ◆ 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 تفرانس 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

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.”

◆ 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)

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 ...

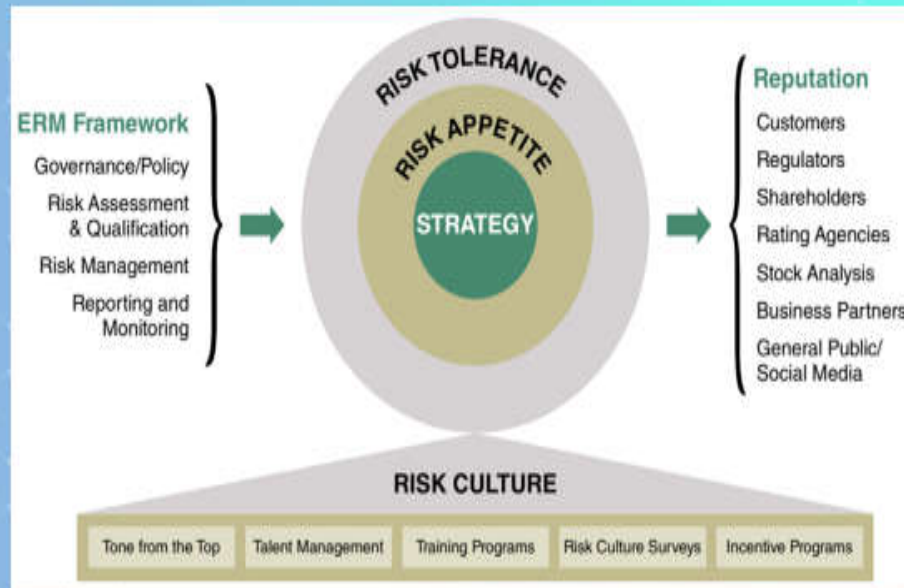
برای اطلاعات بیشتر در خصوص اشتها و تفرانس ریسک، مستند زیر را مطالعه نمایید:

[BS ISO 31000-2018.pdf](#)

توسعه فرهنگ ریسک و مدیریت تغییر سازمانی

درباره فرهنگ ریسک

ارتباط عناصر کلیدی چارچوب ERM



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

78

اثربخشی و جامعیت فرآیند مدیریت ریسک به فرهنگ ریسک سازمان بستگی دارد

اگر فرهنگ برای بحث آزاد و در نظر گرفتن ریسک به دو معنای منفی و مثبت کلمه مساعد نباشد، فرآیند مدیریت ریسک با شکست مواجه خواهد شد

سازمان ممکن است خط‌مشی‌ها و رویه‌هایی برای مدیریت ریسک داشته باشد، اما فرهنگ سمی سایه افکنده و هرگونه گفتگو یا اقدام جدی را نفی کند

سازمان‌ها ممکن است فرآیندهای پیچیده‌ای برای اندازه‌گیری و ارزیابی ریسک داشته باشند، اما فرهنگ برای مدیریت ریسک مفید نباشد

اگر تمرکز فرآیند مدیریت ریسک صرفاً علامت زدن باکس‌های چک لیست باشد، بعید است که این فرآیند به سطح بلوغ مورد انتظار برسد

گزارشات زیادی در خصوص ارتقای فرهنگ ریسک سازمان وجود دارد.

ریسک فرهنگ Culture Risk

- ❖ No resources have been allocated to expand risk management.
- ❖ Risk is viewed as "owned" by the internal audit activity and control functions.
- ❖ Scheduling interviews and receiving survey feedback timely is difficult.
- ❖ Bad news does not travel upward in the organization.
- ❖ The challenge to get whole organization on board is unanticipated or greater than anticipated.
- ❖ The organization fails to recognize how people react to change.
- ❖ The organization views risk management process as prescriptive.
- ❖ The internal audit activity fails to effectively report and explain findings and risk ratings.
- ❖ Management fears risk exposure.
- ❖ Cultural traditions are opposed to risk management goals and objectives.

Successful Risk Culture



Source: IIA; 2019 *"Assessing the Risk Management Process"*

بیشتر بدانیم ...

برای اطلاعات بیشتر در خصوص فرهنگ ریسک، مستندات زیر را مطالعه نمایید:

- ❖ The Association of Chartered Certified Accountants, 2014: "A risk challenge culture"
- ❖ Working Values, Ltd. "Is your Culture a Risk Factor?"
- ❖ Higgins, Richard, Grace Liou, Susanne Maurenbrecher, Thomas Poppensieker, and Olivia White. "Strengthening Institutional Risk and Integrity Culture," n.d.
- ❖ Watson, Cate, and David James. "Risk Management and Organisational Culture: Constructing 'Tone at the Top,'" n.d.
- ❖ ...

ابزارهای مدیریت ریسک و راه حل های نرم افزاری

معرفی چند نرم افزار مدیریت ریسک

1. **Infinity** — A Customizable Enterprise Risk Management Software
2. **Project Risk Manager** — One of the Most Adaptable Risk Management Software Solutions
3. **Acumen Risk** — The Most User-Friendly Risk Management App
4. **Pims Risk** — A Great Risk Assessment Software for All Teams
5. **TrackMyRisks** — Among the Best Risk Management Tools for Automation
6. **Opture** — A Great Enterprise Risk Management Software
7. **Resolver** — The Best Risk Management App for Medium and Large Companies
8. **IsoMetrix** — One of the Best Risk Management Applications
9. **@RISK** — A Risk Management Tool That's More Than an Add-On
10. **ProcessMAP** — A Versatile Risk Management Platform
11. **Fusion Framework System** — A Great Risk Management Software for Data Visualization
12. **StandardFusion** — A Versatile Enterprise Risk Management Software
13. **Integrum** — An Approachable and Customizable Risk Management Software
14. **Qualys** — An All-Encompassing Risk Assessment Software
15. **Reciprocity** — A Great Time-Saving Risk Management Software

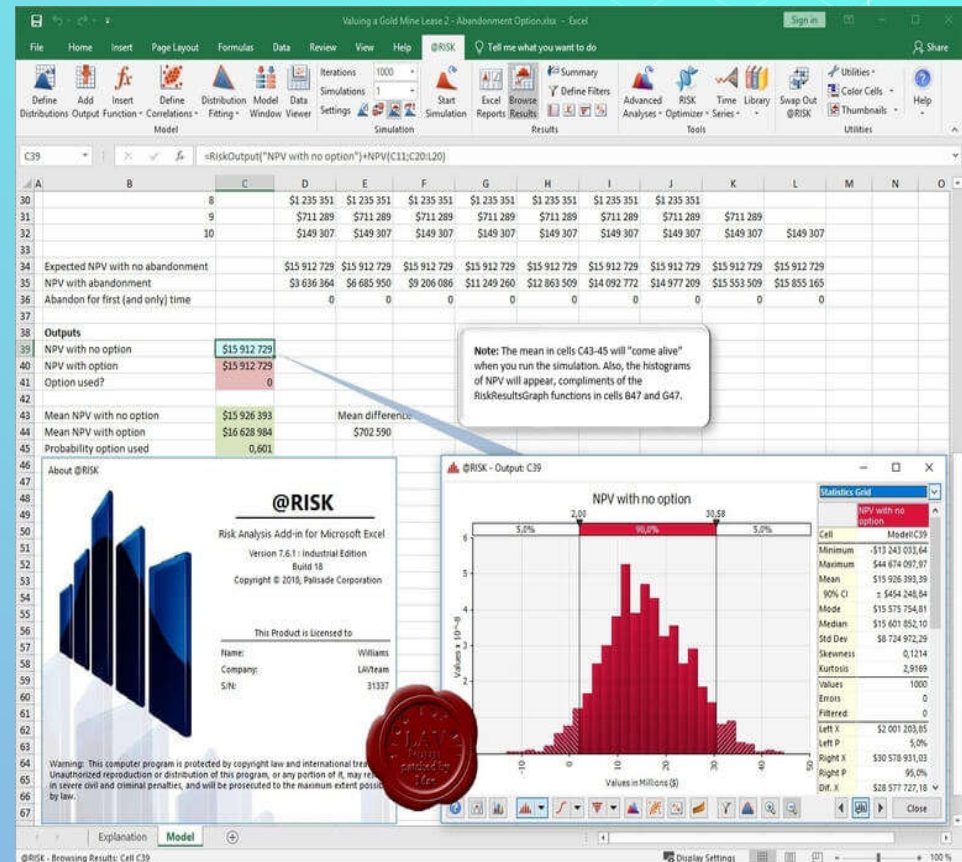
Selection Criteria:

- ❖ **Key features**
- ❖ **Price**
- ❖ ...

معیارهای انتخاب

Some Key Features for Software Selection:

- ❖ Compliance Management
- ❖ Dashboard
- ❖ Disaster Recovery
- ❖ IT Risk Management
- ❖ Incident Management
- ❖ Operational Risk Management
- ❖ Risk Assessment
- ❖ Incident Reporting
- ❖ Investigation Management
- ❖ Business Process Control
- ❖ Compliance Management
- ❖ Mobile Access
- ❖ Predictive Analytics



مسئله غامض (دشوار) مدیریت ریسک

*'I've worked in first line, second line and third line, and there is always, clearly, a healthy tension. But, from a first-line perspective, the guys just want to get on and run the business and this type of [risk management] activity can just be seen as **an administrative frustration, an overhead that doesn't actually add any value**'.*

Business Manager

پیاده سازی سیستم مدیریت ریسک دشوار و پیچیده است:

فقدان فهم، درک و زبان مشترک

گسترده‌گی ابعاد و تنوع ریسک و موضوعات مرتبط با

ERM

تعارض منافع با مدیران و کارکنان لایه اول دفاعی

طولانی بودن دوره به ثمر نشستن تصمیمات مدیریت

ریسک

اتخاذ تصمیمات برای آینده و نامشهود بودن نتیجه آنها

(معرفی محصول جدید، M&A، ...)

صعوبت آشکار شدن نتایج برنامه مدیریت ریسک

سازمانی (حتی ممکن است نتایج آشکار نشود)

سخت بودن توجیه و تأمین هزینه‌های برنامه مدیریت

ریسک سازمانی

... مسئله غامض (دشوار) مدیریت ریسک (ادامه)



Internal Control -
Integrated Framework

Expanded into
3 components



Enterprise Risk Model -
Integrated Framework



Contextual Business Model

تجسم بصری مدل کسب و کار



- ◆ نگاه ساده ولی کل نگر به فرآیندهای حاکمیتی و مدیریتی
- ◆ فرآیندهای حاکمیتی شامل: تعیین چشم انداز، مأموریت و نظارت هیأت مدیره بر برنامه ریزی و عملیات
- ◆ تعیین استراتژی توسط تیم مدیریت اجرایی (و بسته به اندازه سازمانی با همکاری هیأت مدیره) که عبارتست از یک برنامه سطح بالا برای دستیابی به یک یا چند هدف سازمانی متناسب با بیانیه مأموریت
- ◆ روی هم رفته عناصر حاکمیت و استراتژی جهت گیری سازمان و چگونگی موفقیت آن در تأمین انتظارات ذینفعان را روشن می سازد
- ◆ چارچوبهای مدیریت ریسک بایستی در این عناصر نهادینه/یکپارچه سازی شود

پیاده‌سازی اثر بخش سیستم مدیریت ریسک سازمانی

نهادینه‌سازی/یکپارچه‌سازی چارچوب‌های مدیریت

ریسک در:

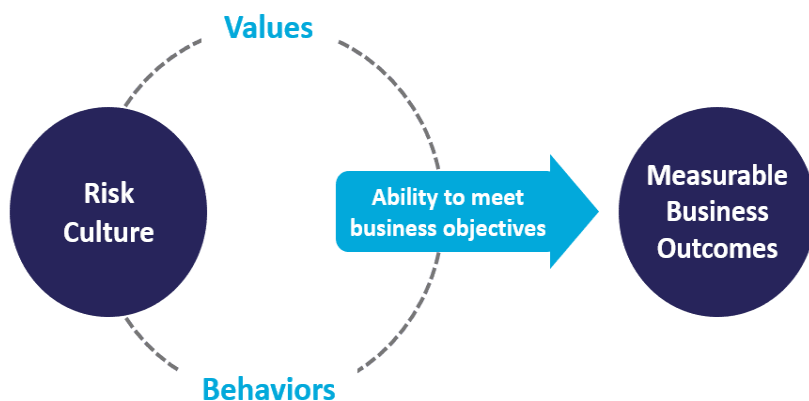
فرهنگ سازمانی (DNA Embedded)

مدل کسب و کار سازمان

بیانیه چشم انداز FERMA

بیانیه چشم انداز مرکز توسعه مدیریت ریسک

مقاومت در برابر تغییر و مدیریت آن



توجه به موضوع مهم ریسک و تغییر (Risk and Change)

غامض/دشوار بودن توجیه هزینه‌ها و پیاده‌سازی اقدامات مدیریت ریسک به مقاومت در برابر آن می‌انجامد

ضرورت ارتقاء فرهنگ سازمانی برای پشتیبانی از اقدامات مدیریت ریسک

ریسک و تغییر به مثابه دوروی یک سکه

استراتژی حل مسئله: نهادینه سازی/یکپارچه سازی مدیریت ریسک در فرهنگ سازمانی

بهترین روش توسعه برنامه ERM

برنامه ERM را می توان به چهار جزء زیر تقسیم کرد:

شناسایی ریسک

ارزیابی/سنجش ریسک

پاسخ به ریسک؛ و

ارتباطات و پایش

توسعه منحصر به فرد برنامه ERM و رویکرد سفارشی سازی متناسب با عواملی مانند:

بیانیه مأموریت

اندازه

پیچیدگی سازمانی

منابع انسانی؛ و

سرمایه

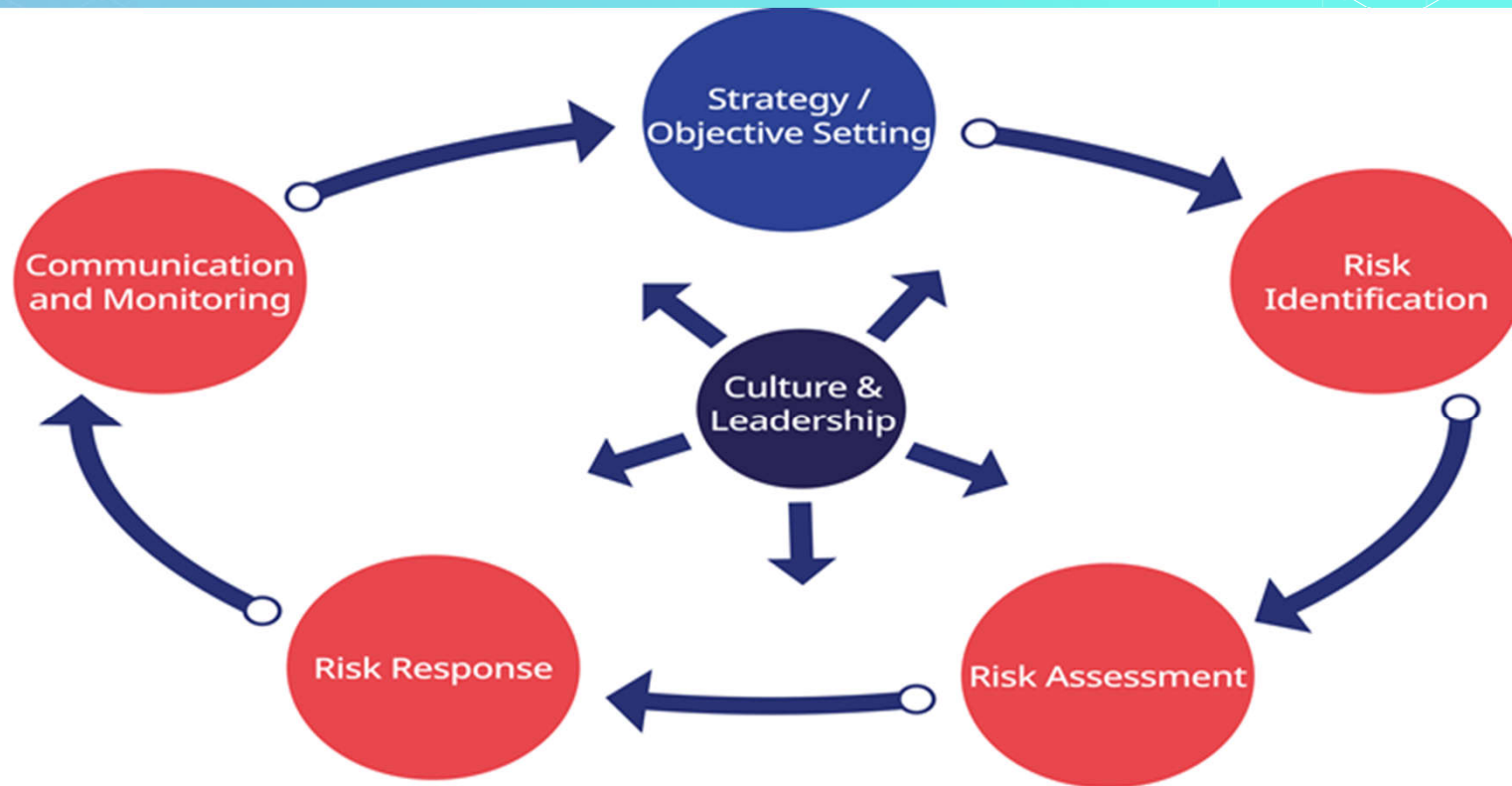
شروع استراتژی ERM با اهداف استراتژیک

Risk List ERM

VS

Objective Centric ERM

اجزای فرآیند ERM



Source: Beasley, 2020.

بعضی از ابزارها/تکنیک‌های شناسایی ریسک

- ◆ **Brainstorming**
- ◆ **Event Inventories and Loss Event Data**
- ◆ **Interviews and Self-Assessment**
- ◆ **Facilitated Workshops**
- ◆ **SWOT Analysis**
- ◆ **Risk Questionnaires and Risk Surveys**
- ◆ **Scenario Analysis**
- ◆ **Using Technology**
- ◆ **Other Techniques**

شناسایی ریسک

◆ همه سطوح سازمانی بایستی به شناسایی چشم انداز ریسک سازمان (risk landscape) کمک کنند

◆ روش مصاحبه، بازدید، جلسات توفان فکری، ...

◆ دسته بندی ریسک‌های شناسایی شده بر اساس سیستم طبقه بندی ریسک سازمان (عملیاتی، استراتژیک، مالی، ...)

◆ شناسایی ریسک به تنهایی کافی نیست و گام بعدی سنجش/ارزیابی و الویت‌بندی ریسک است

◆ معمولاً تعداد ۸ تا ۱۵ ریسک اصلی و مهم برای فاز بعدی انتخاب می‌شود

◆ مدیریت ریسک فرآیندی پیوسته و در حال تکوین با حلقه بازخورد (feedback loop) است

◆ این فرآیند با شناسایی ریسک آغاز می‌شود

◆ هدف شناسایی ریسک دستیابی به موجودی ریسک (risk inventory) سازمان است

◆ شناسایی ریسک با سنجش/ارزیابی ریسک متفاوت است، هر چند همپوشانی‌هایی نیز وجود دارد

◆ شناسایی دقیق ریسک برای موفقیت برنامه ERM حیاتی است

چشم انداز / پرتفوی / موجودی ریسک سازمانی



Source: Debra Elkins, "Managing Enterprise Risks in Global Automotive Manufacturing Operations," presentation at the University of Virginia, January 23, 2006. Permission granted for use.

نمونہ فرم شناسایی ریسک

EXHIBIT 4A: RISK IDENTIFICATION TEMPLATE

1. Please list the major strategies and/or objectives for your area of responsibility.
2. Please list the major risks your unit faces in achieving its objectives. List no more than 10 risks.
3. Please assess the overall risk management capability within your area of responsibility to seize opportunities and manage the risks you have identified.

EXHIBIT 4B: MAJOR STRATEGIES/OBJECTIVES FOR YOUR UNIT

Please list the major strategies/objectives for your unit.

EXHIBIT 4C: MAJOR RISKS FOR YOUR UNIT

Please list the major risks your unit faces in achieving your objectives. List no more than 10 risks.

نمونه فرم شناسایی، ارزیابی و مواجهه/رفتار با ریسک

Step 1 to 3
Context

Date Risk Identified: Enter date

Risk Owner: Input the stakeholder accountable for the risk

Business Area/s: Provide the primary affected business area

Risk Type: Choose an item.

Risk Category: Choose an item.

Commentary / Summary Input any details that may provide useful background/context in understanding the risk.

1 – Identify			2 - Analyse	3 – Evaluate		4 – Treat			
Risk No.	Step 4. Risk Description (What could go wrong?)	Step 5. Consequences (Why do we care?)	Step 6. Cause (Why would this risk occur?)	Step 7. Controls	Step 8. Current Risk Rating	Step 9. Risk Treatment Option (Select 'Accept' or 'Treat')	Step 10. Treatment Plan (Describe your plan)	Step 11. Treatment Due/ Review Dates & Owner	Step 12. Target Risk Rating
#	Type here - Provide a brief but clear description of the risk.	Type here - The consequences need to provide the description of what impact the risk will result in.	Type here - Input the key drivers that will result in the risk occurring.	Type here - Detail the controls mitigations currently in place that will reduce the risk. If none exist please note this	Type here - Use the 'Risk Exposure Matrix' supported with the Consequence and Likelihood Criteria to assist you in identifying the risk level. These ratings should be done after taking into account the controls currently in place.	Select 'Accept' or 'Treat'. Accept when no further treatment. Choose an item.	Type here - Input any planned mitigations (but not currently in place) that will further reduce the risk.	Type here - Record the review and/or due dates for each treatment and associated owner	Type here - These ratings should be done after taking into account the planned treatments.
Sample	Poor Partner Management - Risk that an ad-hoc approach is taken in developing RMIT's global presence	This risk may negatively impact RMIT brand and position in different countries whilst also negatively impacting financial performance	Strategy and drive to grow international revenue but without clear partner management process and policies, causing an ad-hoc approach to expand global presence	No controls are currently in place	Consequence: 3 Likelihood: C High	Option - Treat	Design and develop new Global Partnership Life-cycle Framework - Gain executive approval, assign development to staff member, and create a development and implementation plan.	October 2019 Joe Bloggs	Consequence: 3 Likelihood: B Medium

ارزیابی قابلیت مدیریت ریسک

Use the following categories* to assess the overall risk management capability within your area of responsibility to seize opportunities and manage risks using the scale at the bottom of the page.

Internal Environment	VL	L	M	H	VH
Objective Setting	VL	L	M	H	VH
Event Identification	VL	L	M	H	VH
Risk Assessment	VL	L	M	H	VH
Risk Response	VL	L	M	H	VH
Control Activities	VL	L	M	H	VH
Information/communication	VL	L	M	H	VH
Monitoring	VL	L	M	H	VH

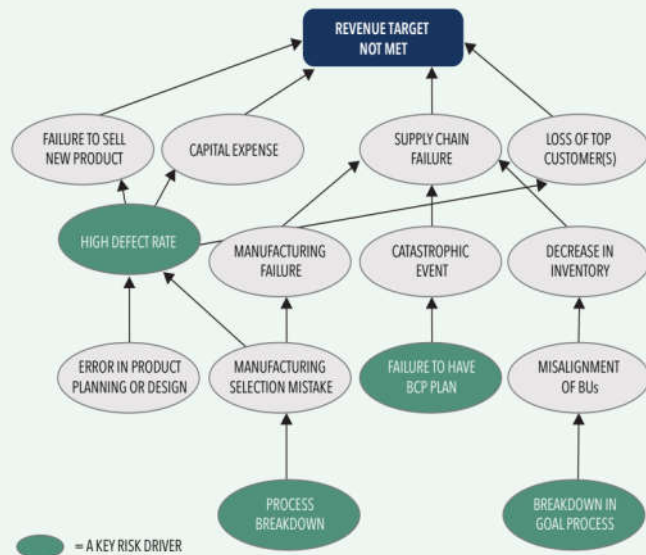
What is your level of concern with respect to the overall risk management capability of your area of responsibility to seize opportunities and manage risks? Please circle the most appropriate response:

VL = Very Low L = Low M = Medium H = High VH = Very High

*The categories are taken from COSO, *Enterprise Risk Management—Integrated Framework: Executive Summary*, AICPA, New York, N.Y., 2004.

نمودار اثرگذاری (Influence Diagram) یا تجزیه و تحلیل علل ریشه‌ای (RCA)

Develop Influence Diagram and Quantify the Risk Drivers: Define root causes and main drivers of the risks. Define the chain of events in likely scenario. Drivers should be small enough in scope that they can be quantified.

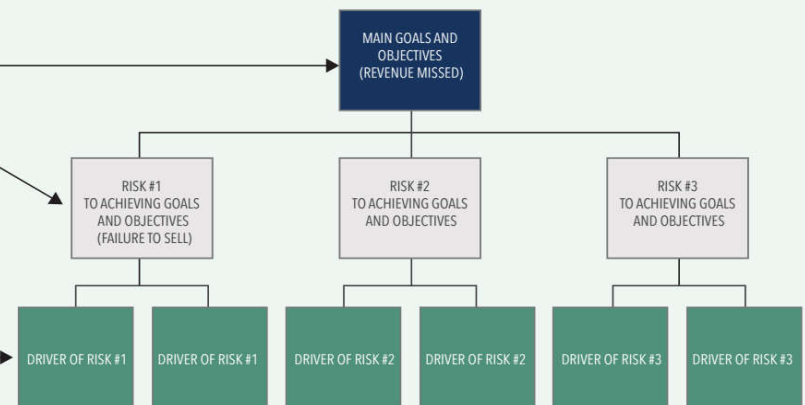


پس از شناسایی ریسک و قبل از کمی کردن آن
درک و فهم دقیق‌تر علل ریشه‌ای و بالقوه ریسک از طریق تجزیه
و تحلیل عوامل محرک

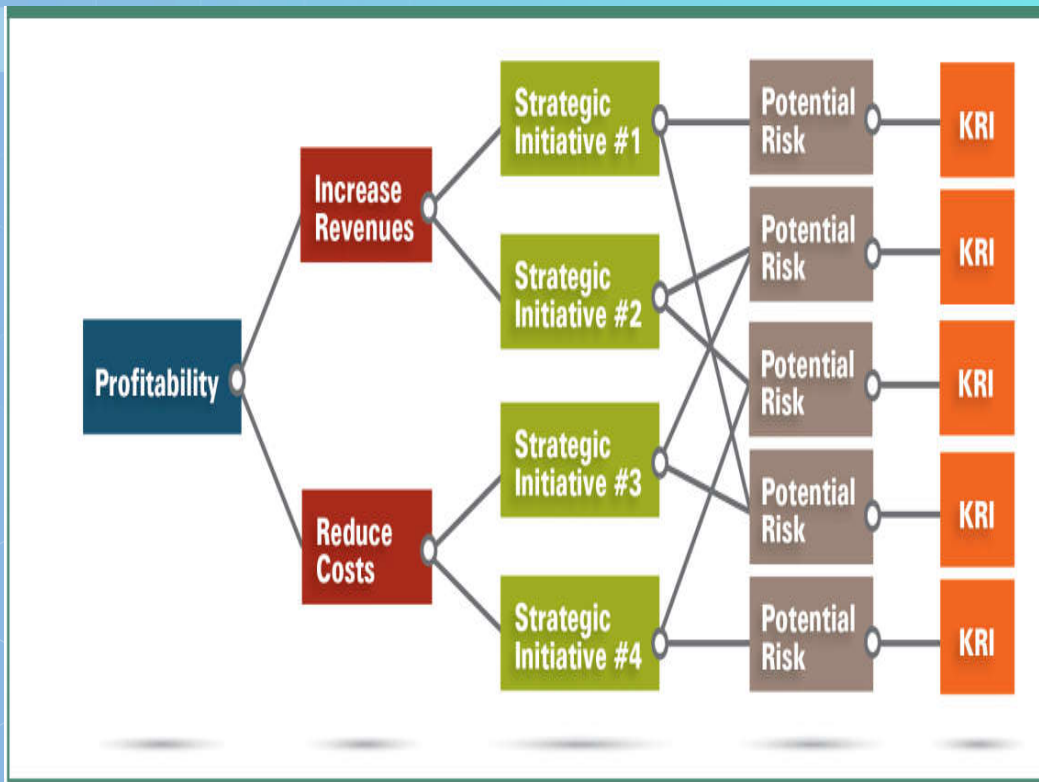
همکاری با سایر قسمت‌های سازمان مالک بخشی از ریسک
استفاده از تجزیه و تحلیل سناریو برای RCA
بررسی مستندات و مصاحبه
کاربرد برای اهداف راهبردی (شکل روبرو)

Do NOT try to quantify at these levels

Quantify risks at this level or below



ارتباط اهداف به استراتژی‌ها به ریسک‌ها و شاخص‌های کلیدی ریسک



توسعه شاخص‌های کلیدی ریسک (KRIs)

ابزارهای ارزیابی/سنجش ریسک

- ◆ Categories
- ◆ Qualitative vs. Quantitative
- ◆ Risk Rankings
- ◆ Impact and Probability
- ◆ Keys to Risk Maps
- ◆ Link to Objectives at Risk or Divisions at Risk
- ◆ Residual Risk
- ◆ Validating the Impact and Probability
- ◆ Gain/Loss Curves
- ◆ Tornado Charts
- ◆ Risk-Adjusted Revenues
- ◆ A Common Sense Approach to Risk Assessment
- ◆ Probabilistic Models Seemingly Nonquantifiable Risks

◆ شناسایی صحیح ریسک بخشی از ارزیابی و عامل

مهمی در رسیدن به نتایج ارزیابی ریسک است

◆ تلاش سازمان برای اطمینان از شناسایی درست

ریسک‌ها با استفاده از ابزارها/رویکردهای

شناسایی ریسک

◆ ایجاد زبان و فهم مشترک از واژگان ریسک

◆ عدم فهم مشترک مانع توسعه ERM

◆ دسته بندی ریسک‌ها پس از شناسایی آنها:

◆ خطر، عملیاتی، مالی و استراتژیک

◆ قابل کنترل و غیر قابل کنترل

◆ داخلی/خارجی

◆ مالی/غیر مالی

◆ بیمه‌ای/غیر بیمه‌ای

نگاهی به پرتفوی ریسک (اصل ۱۴ کوزو)

Strategy View (Portfolio)

Our strategy is to leverage product design and customer service to become the industry leader

Entity Objective View (Risk Profile)

Strengthening Balance Sheet

Enhancing Operational Excellence

Growing Market Share

Business Objective View (Risk Profile)

Improving Quality of Credit Portfolio

Optimizing Working Capital

Minimizing Losses and Inefficiencies

Investing in Best-in-Class Technology Solutions

Satisfying All Compliance Obligations

Maintaining Customer Satisfaction

Market Leader on Innovative New Products

Risk View

Risk of Counterparty Default

Risk of Funding Gap

Risk of Fraud

Risk of Technology Disruption

Risk of Compliance Breach

Risk of Product Recall

Risk of Product Obsolescence

Risk of Poor Customer Experience

Risk of Low Sales

Risk Category View

Financial Risk

Operational Risk

Compliance Risk

Customer Risk

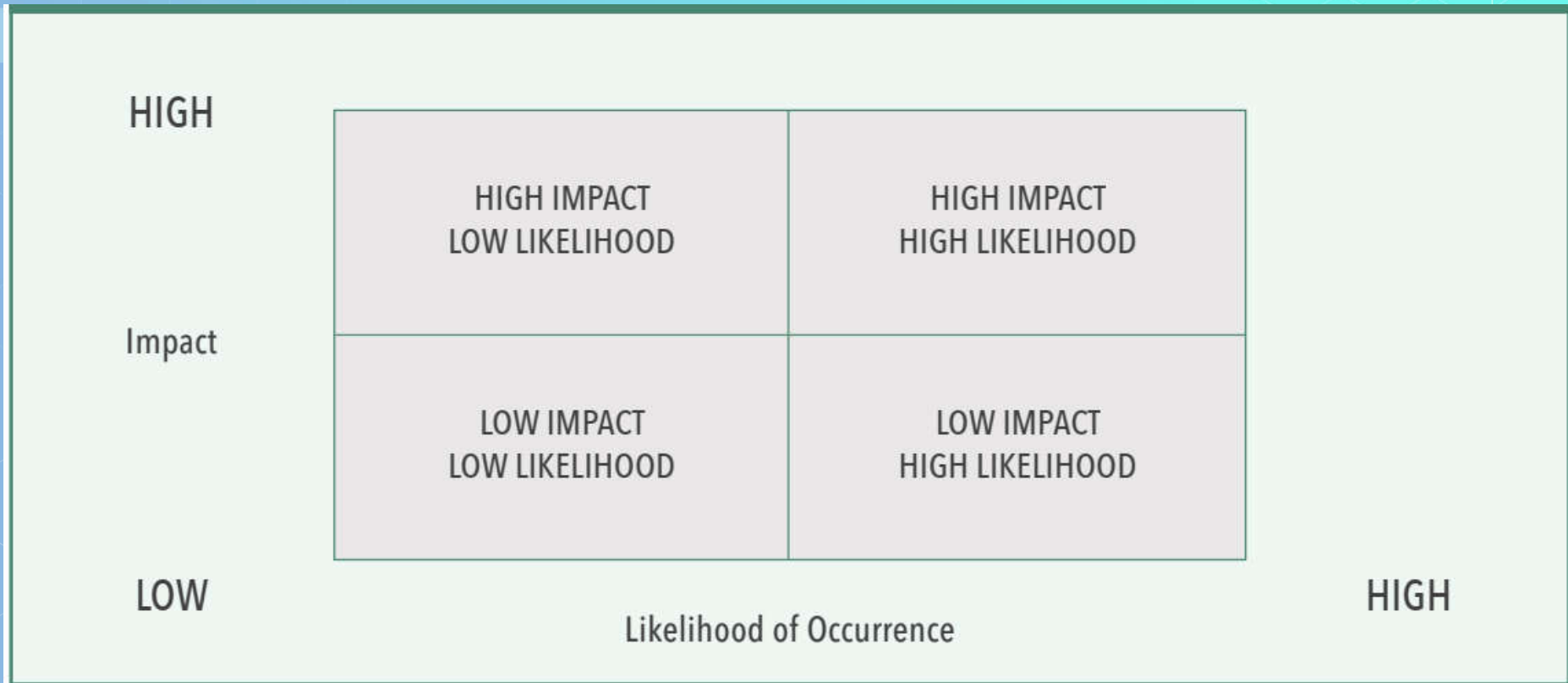
رویکردهای کمی و کیفی به ارزیابی ریسک

QUALITATIVE:	QUALITATIVE/QUANTITATIVE:	QUANTITATIVE:
Risk identification	Validation of risk impact	Probabilistic techniques:
Risk rankings	Validation of risk likelihood	Cash flow at risk
Risk maps	Validation of correlations	Earnings at risk
Risk maps with impact and likelihood	Risk-corrected revenues	Earnings distributions
Risks mapped to objectives or divisions	Gain/loss curves	EPS distributions
Identification of risk correlations	Tornado charts	
	Scenario analysis	
	Benchmarking	
	Net present value	
	Traditional measures	



- ◆ روشهای کیفی شامل: فهرست ریسکها، طبقه بندی ریسکها و ماتریس ریسک
- ◆ فهرست ریسک و دانش تحلیلی به آن نقطه شروع ارزیابی است
- ◆ بعضی از ریسکها را نمی توان کمی کرد. به عنوان مثال: ...
- ◆ دادن اولویت بالا به ریسکهای کمی ناشدنی روشی برای کمی کردن آنهاست
- ◆ ...

فراوانی، شدت و درجه بندی ریسک



ماتریس/نقشه/نقشه حرارتی ریسک

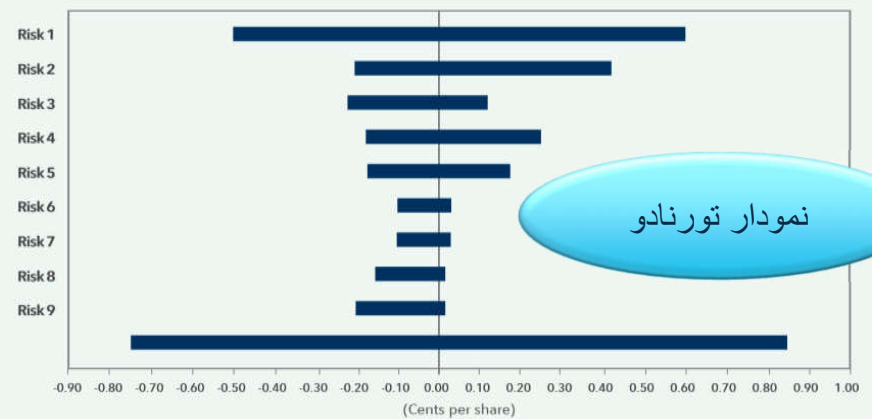
Criticality of Achievement	Level Impact	6 Yellow (Level III) Close monitoring for increased impact and/or variability	8 Red (Level IV) <ul style="list-style-type: none"> Segment commitment Reported to segment leadership Close monitoring of risk action plan 	9 Red (Level V) <ul style="list-style-type: none"> Segment commitment Reported to audit committee Reported to segment leadership Close monitoring of risk action plan
	Segment/Intersegment Level Impact	3 Green (Level II) High-level monitoring for increased impact and/or variability	5 Yellow (Level III) Close monitoring for increased impact and/or variability	7 Red (Level IV) <ul style="list-style-type: none"> Segment commitment Reported to segment leadership Close monitoring of risk action plan
	Process/Business Level Impact	1 Green (Level I) High-level monitoring for increased impact and/or variability	2 Green (Level II) High-level monitoring for increased impact and/or variability	4 Yellow (Level III) Close monitoring for increased impact and/or variability
		Low (Consistently within tolerable variance in key metric improvement or target)	Moderate (Sometimes within tolerable variance in key metric improvement or target)	High (Mostly outside of tolerable variance in key metric improvement or target)
Actual/Potential Performance Variability Around Targets				
Achievement of Objective/Execution of Process/Implementation of Change/Management of Risk				

LIKELIHOOD	High	Risk 7	Risk 6	Risk 2
	Medium	Risk 4	Risk 5 Risk 1	Risk 9
	Low			Risk 8 Risk 3
		Low	Medium	High
IMPACT				

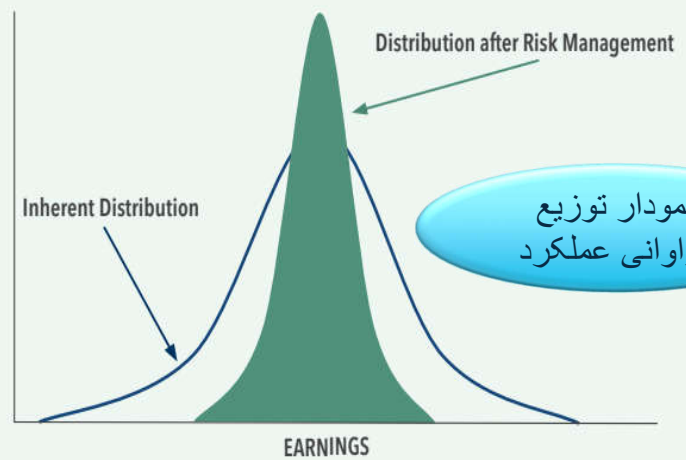
نقشه ریسک و فرصت

Likelihood	Impact									
	Opportunities					Risks				
	Extreme	Major	Moderate	Minor	Incidental	Incidental	Minor	Moderate	Major	Extreme
Frequent	Dark Blue	Dark Blue	Dark Blue	Dark Blue	Blue	Yellow	Red	Red	Red	Red
Likely	Dark Blue	Dark Blue	Dark Blue	Blue	Blue	Yellow	Yellow	Red	Red	Red
Possible	Dark Blue	Dark Blue	Blue	Blue	Light Blue	Green	Yellow	Yellow	Red	Red
Unlikely	Dark Blue	Blue	Blue	Light Blue	Light Blue	Green	Green	Yellow	Yellow	Red
Rare	Blue	Blue	Light Blue	Light Blue	Light Blue	Green	Green	Green	Yellow	Yellow

سایر ابزارهای مورد استفاده در ارزیابی ریسک



نمودار درآمد تعدیل شده با ریسک



نمونه مدل بلوغ سیستم مدیریت ریسک سازمانی

Phase I: Building a Foundation for Business Risk Management

Phase Objectives:

- Build executive-level support
- Strengthen core team and operating model
- Align expectations through a risk management commitment process
- Develop specific segment-level risk management commitments

Stage Objectives:

Stage 1: Awareness Build risk management vision, strategy, and awareness	Stage 2: Capability Build initial risk management foundation of structure, resources, and operating model	Stage 3: Alignment Align expectations through a risk management commitment
--	---	--

Phase II: Segment-Level Business Risk Management

- Execution of a consistent risk management approach across all segments
- Engagement in specific areas to help the business remediate significant risk issues and fulfill their segment risk management commitment
- Segment-level personnel at appropriate levels engaged in the risk management process
- Demonstrating the tangible value of a disciplined risk management process within each segment

Stage 4: Engagement Engagement in specific risk issues to help fulfill the risk management commitment	Stage 5: Value Demonstrating tangible value from a disciplined risk management process	Stage 6: Operationalize Segment-level personnel at all levels fully engaged in and operationalizing the risk management process
---	--	---

Phase III: Enterprise-Level Business Risk Management

- Evolve to an enterprise risk commitment and accountability model by "connecting" the segment risk commitments to consider cross-segment risk issues and interdependencies
- Enhance coordination and integration among segment business risk services (BRS) teams to help the enterprise remediate significant risk issues and fulfill the enterprise risk commitment
- Deepen risk management focus on potential risk issues applicable to all business segments
- Enhance coordination with other components of the enterprise risk management operating model that focus on specific areas of risk exposure

Stage 7: Collaborate Enhance BRM collaboration across other segment teams to consider cross-segment risk issues and interdependencies	Stage 8: Coordinate Enhance BRM coordination with other areas	Stage 9: Integrate BRM is fully integrated with business planning, performance management, quality, and other key management processes
---	---	--

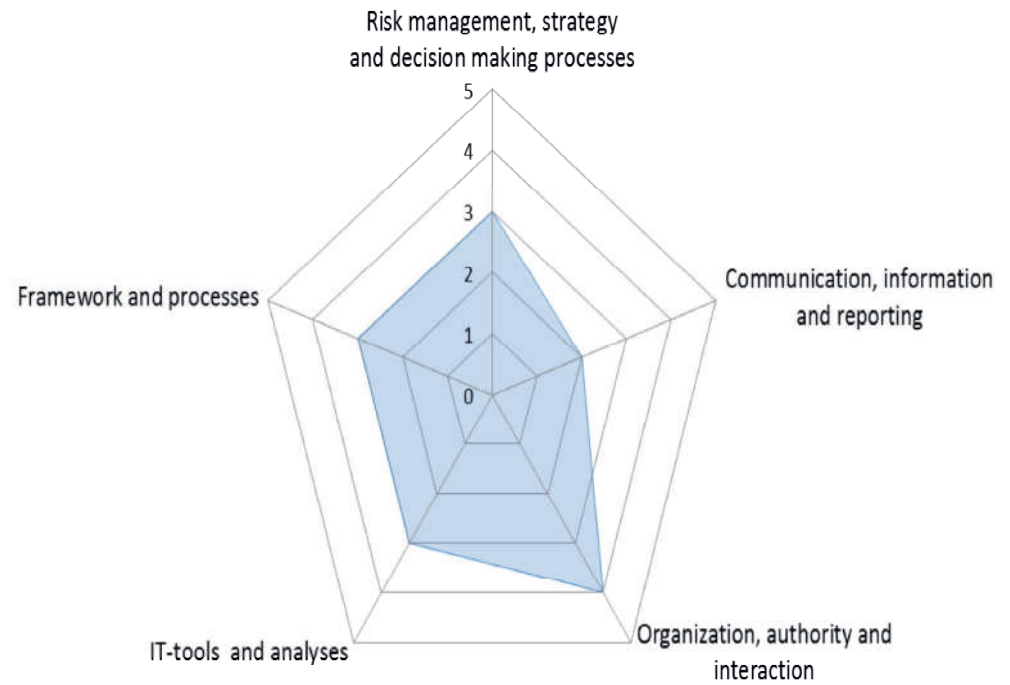
1. Ad hoc

2. Initial

3. Repeatable

4. Managed

5. Leadership



مطالعات موردی و نمونه هایی از اجرای مدیریت ریسک

هوش مصنوعی، یادگیری ماشینی و یادگیری عمیق



McKinsey
& Company

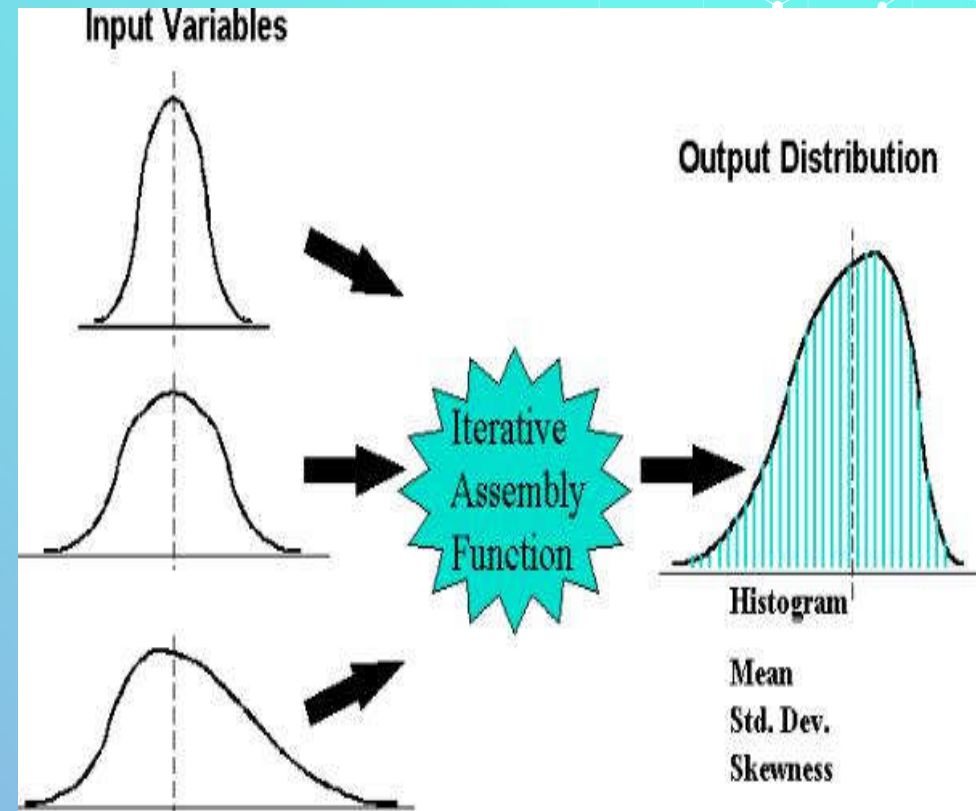
Insurance Practice

Insurance 2030— The impact of AI on the future of insurance

The industry is on the verge of a seismic, tech-driven shift. A focus on four areas can position carriers to embrace this change.

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
- ❖ ...



شبیه سازی مونت کارلو

Non-financial risks: Why quantify?

1. To assess the **total potential exposure** of single risk (risks can lead to several consequences, like safety, reputational, compliance, operational disruption, etc.)
2. To **aggregate risks** and find the combined exposure of multiple risks
3. To **compare** and **prioritise** risks using on the basis of total exposure
4. To run more **insightful analyses** (e.g., sensitivity studies, control cost-effectiveness analyses)
5. To help calculate the **ROI** of your risk program

Quantifying non-financial risks is common in certain industries...

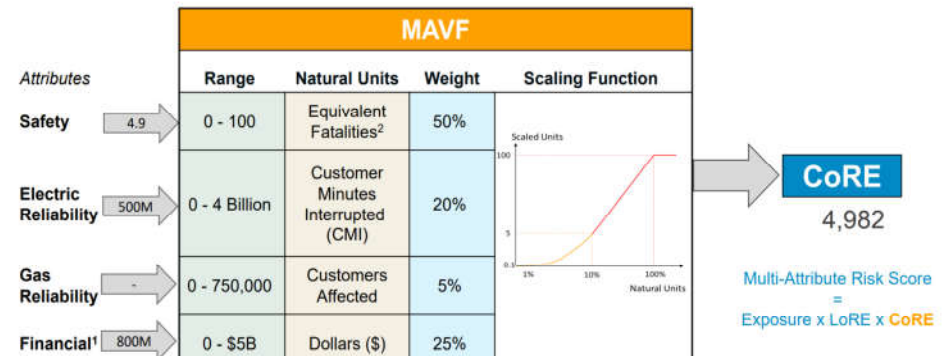
For example...

After a series of disasters, the **California Public Utilities Commission** now requires utility companies to:

- Implement a risk-based decision-making framework
- Use a **Multi-Attribute Value Function**: for combining all potential consequences of a risk event and create a single measurement of value/score
 - **Attribute**: An observable aspect of a risky situation that has value or reflects a utility objective
 - Attributes considered: **Safety, Reliability and Financial**
- Apply MAVF to calculate **mitigation cost-effectiveness** (Risk-Spend Efficiency)

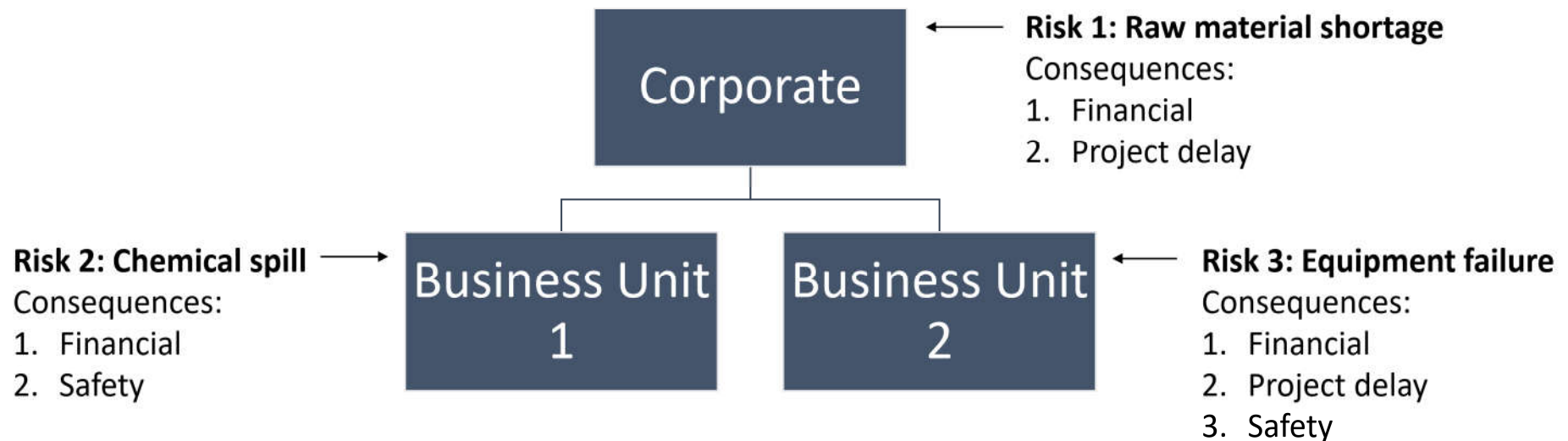


San Bruno pipeline explosion, 9/11/2010



Case study

- A corporate entity has two business units
- The corporate board wants to aggregate and compare three key risks, each with different consequences



Set up a risk scoring framework

- Entity specific utility scale
- Corporate utility scale

Risk score ranges from 0 – 5

Consequence	Entity	Nil (Score = 0)	Insignificant (Score = 1)	Minor (Score = 2)	Moderate (Score = 3)	Major (Score = 4)	Severe (Score = 5)
Financial (USD)	Corporate	No loss	50,000	200,000	700,000	3,000,000	10,000,000
	Business Unit 1		20,000	80,000	300,000	1,000,000	5,000,000
	Business Unit 2		10,000	30,000	100,000	250,000	1,000,000
Project delay	Corporate	No delay	1 month	3 months	6 months	12 months	24 months
	Business Unit 1		2 weeks	1 month	3 months	6 months	12 months
	Business Unit 2		1 week	2 weeks	1 month	3 months	6 months
Safety	Corporate	No injury	First Aid	Medically treated injury	Hospitalisation	Single fatality	Multiple fatalities
	Business Unit 1						
	Business Unit 2						

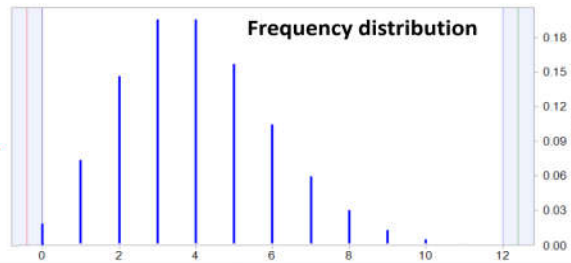
Assess risk likelihood and consequence(s)

1)	Corporate Risk	Financial consequence			Min	Most likely	Max	
	Raw material shortage	Revenue loss			500,000	1,000,000	5,000,000	
	Likelihood	Non-financial consequence	Nil (0)	Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Severe (5)
	30%	Project delay*	50%	5%	10%	25%	5%	5%
2)	BU1 Risk	Financial consequence			Min	Most likely	Max	
	Chemical spill	Fines, clean up costs			1,000	50,000	10,000,000	
	Likelihood	Non-financial consequence	Nil (0)	Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Severe (5)
	20 - 50%	Safety	80%	5%	10%	5%	0.1%	0.001%
3)	BU2 Risk	Financial consequence			Min	Most likely	Max	
	Equipment failure	Repairs			2,000	10,000	1,000,000	
	Average frequency	Non-financial consequences	Nil (0)	Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Severe (5)
	4 per year	Project delay*	70%	10%	10%	5%	3%	2%
		Safety	60%	25%	8%	4%	2%	1%

* For simplicity, project delays were modelled using a discrete distribution but we could also have used continuous distributions

Run a Monte Carlo simulation

BU2 Risk	
Equipment failure	
Average frequency	
4 per year	



For example, in trial #30 out of 5,000...

Simulated frequency
5 failures

Financial impact Business Unit 2 Scale	
Parameters	Values
Min	2,000
Most likely	10,000
Max	1,000,000
Simulated value *	77,340

Project delay Business Unit 2 Scale			
Consequence	Probability	No. events	Utility value
0	70%	2	-
1	10%	1	10,000
2	10%	1	30,000
3	5%	1	100,000
4	3%	0	-
5	2%	0	-
Simulated utility			140,000

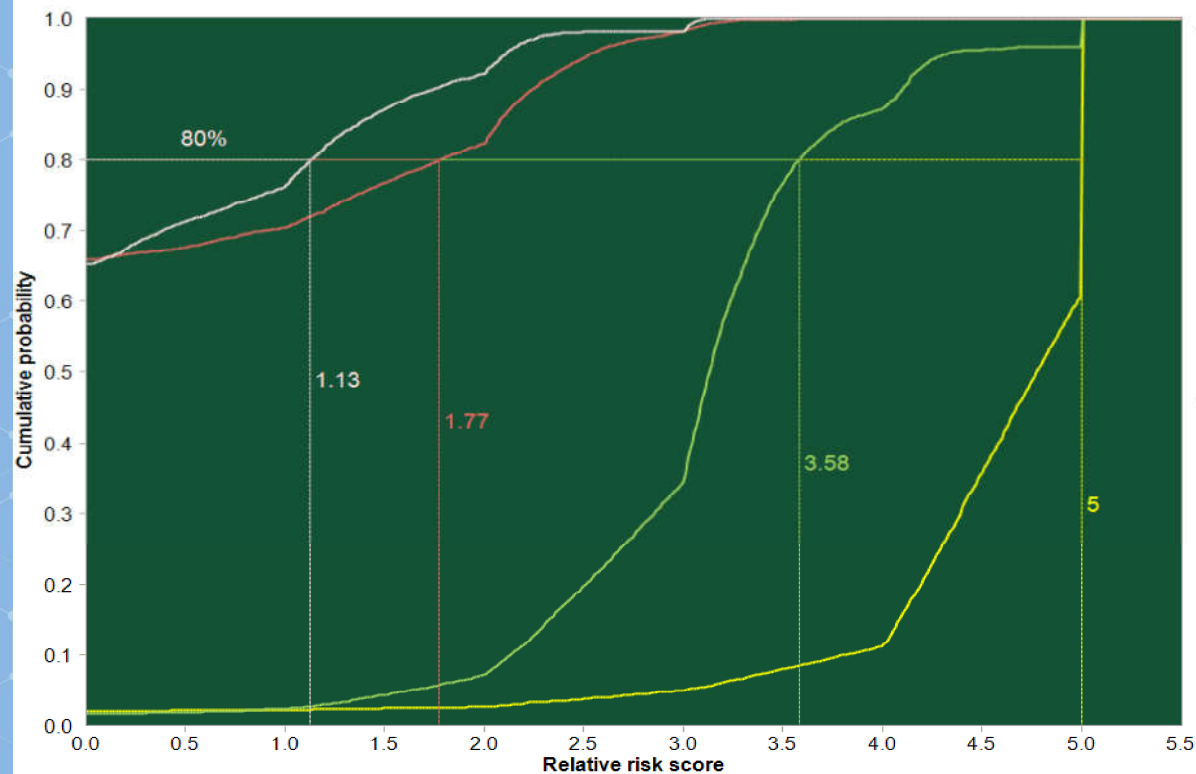
Safety Corporate Scale			
Consequence	Probability	No. events	Utility value
0	60%	3	-
1	25%	1	50,000
2	8%	1	200,000
3	4%	0	-
4	2%	0	-
5	1%	0	-
Simulated utility **			250,000

= Simulated total utility: **467,340** — Interpolation —> Risk score: **4.29**

* Calculates the aggregated distribution given the simulated risk event frequency of 5 equipment failures

** There are pros and cons in 'putting numbers' on the utility of injuries, fatalities, etc. However, this is common practice as seen in the use of such concepts as the 'value of statistical life'.

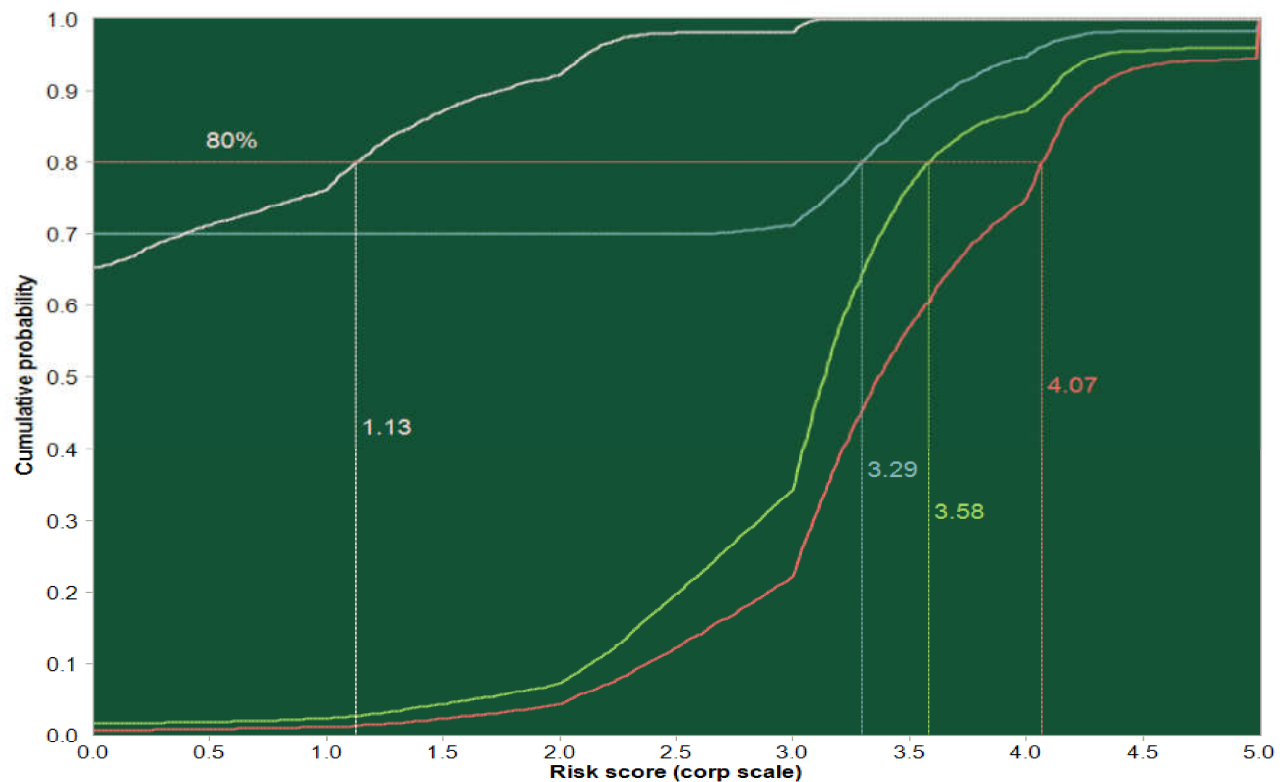
Quantifying risks: Business Unit vs Corporate scale



- The same risk scores **higher** in the **Business Unit scale** than in the **Corporate scale** because:
 - BUs have **lower risk thresholds**
 - Safety consequences **carry more weight** as they are linked to the Corporate utility scale (making these consequences more important)
- In other words, risks are **'more damaging'** at the BU level, typically because of their more restricted capacity to absorb risk relative to the corporate entity

- 1. Equipment failure (BU scale)
- 1. Equipment failure (corp scale)
- 3. Chemical spill (BU scale)
- 3. Chemical spill (corp scale)

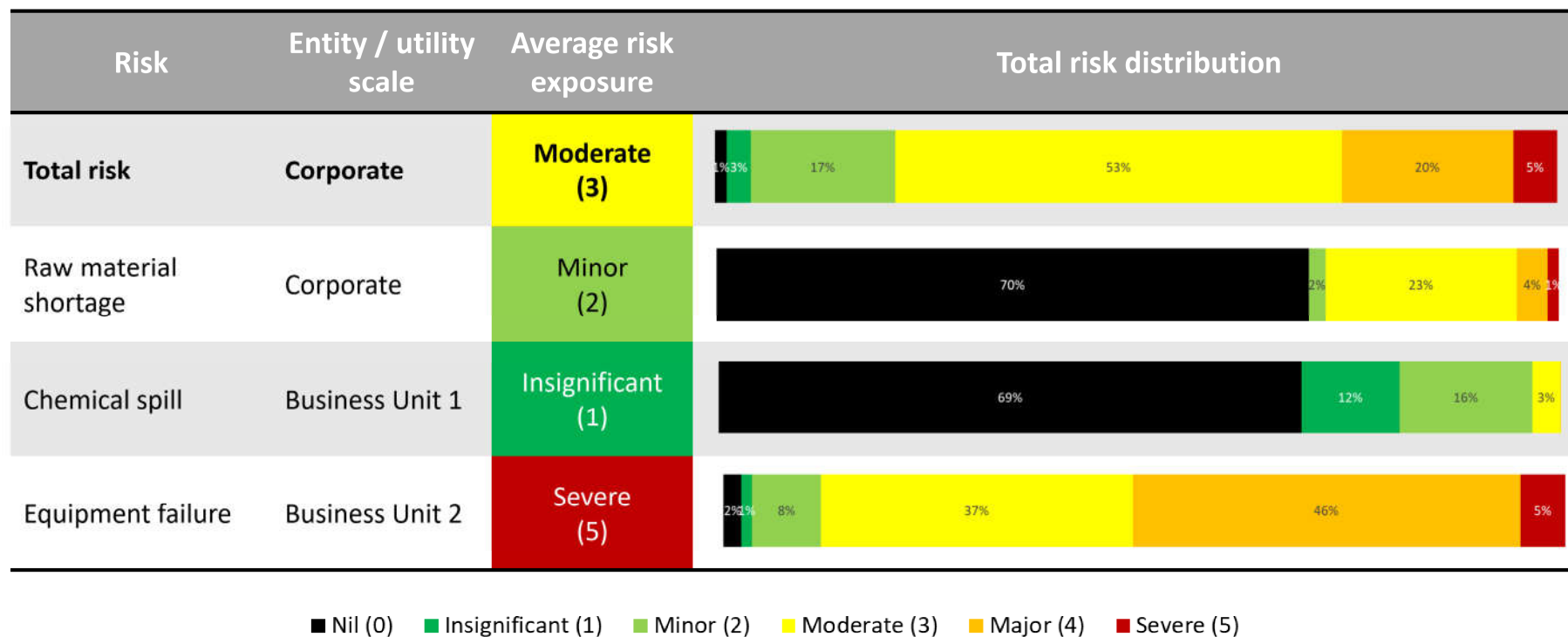
Aggregating risks at the corporate level



- Risks can be properly **compared** and **prioritised** when aggregated at the corporate level (this is what 'Enterprise Risk Management' is supposed to be about)
- The **total amount of risk** carried at the corporate entity can also be calculated

- 1. Equipment failure (corp scale)
- 2. Raw material shortage (corp scale)
- 3. Chemical spill (corp scale)
- Total risk

Another way to visualise what we've done



خطرات و روندهای نوظهور در مدیریت ریسک

جنبه های نظارتی و انطباقی مدیریت ریسک

مقررات گذاری برای ریسک و مدیریت ریسک

❖ شروع مقررات گذاری از دهه ۱۹۹۰

❖ ایجاد مدل‌های داخلی مدیریت ریسک و فرمول‌های محاسبه سرمایه مورد نیاز برای حفاظت از مؤسسات مالی (از جمله بانک‌ها و بیمه‌ها) به منظور حفاظت از ایشان در برابر ریسک‌ها و کاهش سرمایه قانونی مورد نیاز:

❖ MCR

❖ SCR

❖ Stress and Scenario Test

❖ توسعه مفهوم حاکمیت ریسک (Risk Governance) در همین دهه؛

❖ توسعه استانداردهای مدیریت ریسک؛

Sarbanes-Oxley Act (2002)

❖ وضع قانون SOX در آمریکا (بحران ورشکستگی شرکت ها ناشی از ضعف حاکمیت مدیریت ریسک):

❖ شرکت Enron؛

❖ شرکت Worldcom؛

❖ ...

❖ این قانون، اصول حاکمیت شرکتی (Corporate Governance) را ارائه می‌دهد؛

❖ الزام شرکت های مندرج در فهرست بازار سهام نیویورک (NYSE) به رعایت قانون SOX و برخورداری از حاکمیت مدیریت ریسک؛

❖ ناتوانی این مجموعه از قوانین، مقررات و اقدامات احتیاطی در جلوگیری از فروپاشی و بحران بازارهای مالی جهانی (2007 تا

۲۰۰۹)



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 بین‌المللی مواجهند
- ◆ ترکیبی از رژیم‌های 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
- ◆ همه‌کدها 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

ورشکستگی سازمانهای بزرگ	بحرانهای مالی	عوامل بیولوژیک
وضع قانون SOX در آمریکا (۲۰۰۲)	بحران مالی جهانی (۲۰۰۸)	پاندمی COVID-19

◆ تغییرات جوی (Climate Change)
◆ فناوریهای نوآورانه و تحول آفرین (Disruptive Innovative Technologies):

- ◆ هوش مصنوعی
- ◆ یادگیری ماشینی
- ◆ اینترنت اشیا
- ◆ بلاک چین
- ◆ ...

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.

با تشکر از توجه شما