بسمه تعالی

مدیریت امنیت اطلاعات

ISMS

بخش دوم

مقدمه ی بر مدیریت و تحلیل ریسک



دکتر سیدرضا کامل

دکتری مهندسی شبکه و ارتباطات

دانشیار و عضو هیات علمی گروه کامپیوتر

دانشگاه آزاد اسلامی واحد مشهد

بهار ۱۴۰۵

سرفصل ها ...

سرفصل ها ... یادآوری ...

- پدافند غیرعامل (Passive Defence)

سرفصل ها ... یادآوری ...

- پدافند غیرعامل (Passive Defence) ☑
- مدیریت ریسک (Risk Management - RM)

مدیریت ریسک (Risk Management - RM)

مدیریت ریسک (Risk Management - RM)

تعاریف مهم و اصطلاحات ...

Asset: A system resource or capability of value to its owner that requires protection.

Threat: A potential for a threat source to exploit a vulnerability in some asset, which if it occurs may compromise the security of the asset and cause harm to the asset's owner.

Vulnerability: A flaw or weakness in an asset's design, implementation, or operation and management that could be exploited by some threat.

Risk: The potential for loss computed as the combination of the likelihood that a given threat exploits some vulnerability to an asset, and the magnitude of harmful consequence that results to the asset's owner.

مدیریت ریسک (Risk Management - RM)

Asset: A system resource or capability of value to its owner that requires protection.

Threat: A potential for a threat source to exploit a vulnerability in some asset, which if it occurs may compromise the security of the asset and cause harm to the asset's owner.

Vulnerability: A flaw or weakness in an asset's design, implementation, or operation and management that could be exploited by some threat.

Risk: The potential for loss computed as the combination of the likelihood that a given threat exploits some vulnerability to an asset, and the magnitude of harmful consequence that results to the asset's owner.



تعاریف مهم و اصطلاحات ...

- **دارایی (Asset):** یک منبع سیستم یا قابلیتی ارزشمند برای مالک آن که نیاز به حفاظت دارد.

مدیریت ریسک (Risk Management - RM)

Asset: A system resource or capability of value to its owner that requires protection.

Threat: A potential for a threat source to exploit a vulnerability in some asset, which if it occurs may compromise the security of the asset and cause harm to the asset's owner.

Vulnerability: A flaw or weakness in an asset's design, implementation, or operation and management that could be exploited by some threat.

Risk: The potential for loss computed as the combination of the likelihood that a given threat exploits some vulnerability to an asset, and the magnitude of harmful consequence that results to the asset's owner.





تعاریف مهم و اصطلاحات ...

- **دارایی (Asset):** یک منبع سیستم یا قابلیتی ارزشمند برای مالک آن که نیاز به حفاظت دارد.
- **تهدید (Threat):** پتانسیل و احتمال این‌که یک منبع تهدید از یک آسیب‌پذیری در دارایی سوءاستفاده کند؛ که در صورت وقوع، ممکن است امنیت دارایی را به خطر انداخته و به مالک دارایی آسیب برساند.

مدیریت ریسک (Risk Management - RM)

Asset: A system resource or capability of value to its owner that requires protection.

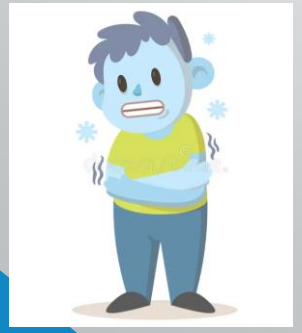
Threat: A potential for a threat source to exploit a vulnerability in some asset, which if it occurs may compromise the security of the asset and cause harm to the asset's owner.

Vulnerability: A flaw or weakness in an asset's design, implementation, or operation and management that could be exploited by some threat.

Risk: The potential for loss computed as the combination of the likelihood that a given threat exploits some vulnerability to an asset, and the magnitude of harmful consequence that results to the asset's owner.







تعاریف مهم و اصطلاحات ...

- **دارایی (Asset):** یک منبع سیستم یا قابلیتی ارزشمند برای مالک آن که نیاز به حفاظت دارد.
- **تهدید (Threat):** پتانسیل و احتمال این‌که یک منبع تهدید از یک آسیب‌پذیری در دارایی سوءاستفاده کند؛ که در صورت وقوع، ممکن است امنیت دارایی را به خطر انداخته و به مالک دارایی آسیب برساند.
- **آسیب‌پذیری (Vulnerability):** یک نقص یا نقطه ضعف در طراحی، پیاده‌سازی، یا عملکرد و مدیریت یک دارایی که می‌تواند مورد سوءاستفاده یک تهدید قرار گیرد.

مدیریت ریسک (Risk Management - RM)

Asset: A system resource or capability of value to its owner that requires protection.

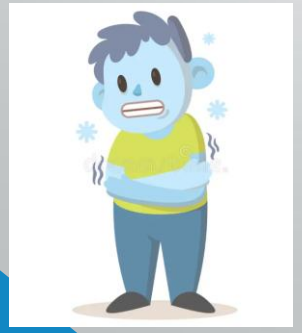
Threat: A potential for a threat source to exploit a vulnerability in some asset, which if it occurs may compromise the security of the asset and cause harm to the asset's owner.

Vulnerability: A flaw or weakness in an asset's design, implementation, or operation and management that could be exploited by some threat.

Risk: The potential for loss computed as the combination of the likelihood that a given threat exploits some vulnerability to an asset, and the magnitude of harmful consequence that results to the asset's owner.







تعاریف مهم و اصطلاحات ...

- **دارایی (Asset):** یک منبع سیستم یا قابلیتی ارزشمند برای مالک آن که نیاز به حفاظت دارد.
- **تهدید (Threat):** پتانسیل و احتمال این‌که یک منبع تهدید از یک آسیب‌پذیری در دارایی سوءاستفاده کند؛ که در صورت وقوع، ممکن است امنیت دارایی را به خطر انداخته و به مالک دارایی آسیب برساند.
- **آسیب‌پذیری (Vulnerability):** یک نقص یا نقطه ضعف در طراحی، پیاده‌سازی، یا عملکرد و مدیریت یک دارایی که می‌تواند مورد سوءاستفاده یک تهدید قرار گیرد.
- **ریسک (Risk):** پتانسیل و احتمال بروز خسارت که از ترکیب دو عامل محاسبه می‌شود :میزان احتمال این‌که یک تهدید مشخص از آسیب‌پذیری یک دارایی سوءاستفاده کند، و میزان شدت عواقب زیان‌باری که برای مالک دارایی به همراه دارد.

مدیریت ریسک (Risk Management - RM)





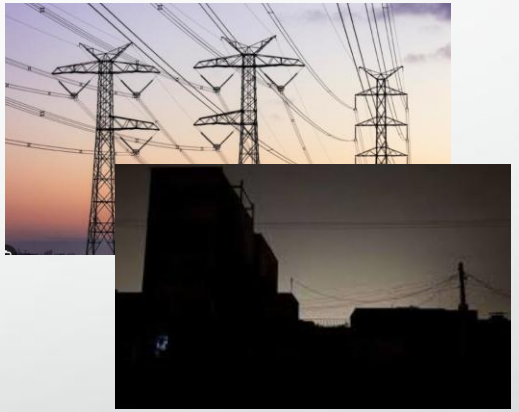


تعریف ریسک ...

- **عدم قطعیت**
- **آنچه ما از اتفاق افتادن / نیفتادن آن اطمینان نداریم**















مدیریت ریسک (Risk Management - RM)

منابع اصلی تهدیدها و ریسک ها را باید در نظر گرفت ...

مدیریت ریسک (Risk Management - RM)









منابع اصلی تهدیدها و ریسک ها را باید در نظر گرفت ...

- **تهدیدها ممکن است شامل موارد زیر باشند:**
  - طبیعی: حوادث قهری یا بلایای طبیعی

مدیریت ریسک (Risk Management - RM)











منابع اصلی تهدیدها و ریسک ها را باید در نظر گرفت ...

- **تهدیدها ممکن است شامل موارد زیر باشند:**
  - طبیعی: حوادث قهری یا بلایای طبیعی
  - ساخت انسان: خواه تصادفی باشد یا عمدی

مدیریت ریسک (Risk Management - RM)

















منابع اصلی تهدیدها و ریسک ها را باید در نظر گرفت ...

- **تهدیدها ممکن است شامل موارد زیر باشند:**
  - طبیعی: حوادث قهری یا بلایای طبیعی
  - ساخت انسان: خواه تصادفی باشد یا عمدی
- **باید مهاجمان انسانی را مد نظر قرار داد:**
  - انگیزه
  - توانایی /قابلیت
  - منابع
  - احتمال وقوع حمله
  - بازدارندگی

مدیریت ریسک (Risk Management - RM)





منابع اصلی تهدیدها و ریسک ها را باید در نظر گرفت ...

- **تهدیدها ممکن است شامل موارد زیر باشند:**
  - طبیعی: حوادث قهری یا بلایای طبیعی
  - ساخت انسان: خواه تصادفی باشد یا عمدی





- **باید مهاجمان انسانی را مد نظر قرار داد:**
  - انگیزه
  - توانایی /قابلیت
  - منابع
  - احتمال وقوع حمله
  - بازدارندگی









- **باید سوابق سازمان را در نظر گرفت**







مدیریت ریسک (Risk Management - RM)



اهمیت شناخت ریسک ها برای مدیران ...

مدیریت ریسک (Risk Management - RM)





اهمیت شناخت ریسک ها برای مدیران ...

- مدیر برای تصمیم گیری باید منابع خود را بشناسد (مانند دارایی ها / نیروی انسانی)

مدیریت ریسک (Risk Management - RM)







اهمیت شناخت ریسک ها برای مدیران ...

- مدیر برای تصمیم گیری باید منابع خود را بشناسد (مانند دارایی ها / نیروی انسانی)
- برای تصمیم گیری درست مدیر باید ریسک ها را هم بشناسد

(جزئی از دارایی های جدایی ناپذیر هر سازمان یا کسب و کار)

مدیریت ریسک (Risk Management - RM)









اهمیت شناخت ریسک ها برای مدیران ...

- مدیر برای تصمیم گیری باید منابع خود را بشناسد (مانند دارایی ها / نیروی انسانی)
- برای تصمیم گیری درست مدیر باید ریسک ها را هم بشناسد

  (جزئی از دارایی های جدایی ناپذیر هر سازمان یا کسب و کار)
- (مهم) مدیر ارشد سازمان / مدیرامنیت اطلاعات (هیچگاه ... هیچگاه ...) نباید غافلگیر بشود

  (یا تصمیمات عجولانه در هنگام وقوع بحران بگیرد)

مدیریت ریسک (Risk Management - RM)









اهمیت شناخت ریسک ها برای مدیران ...

- مدیر برای تصمیم گیری باید منابع خود را بشناسد (مانند دارایی ها / نیروی انسانی)
- برای تصمیم گیری درست مدیر باید ریسک ها را هم بشناسد

  (جزئی از دارایی های جدایی ناپذیر هر سازمان یا کسب و کار)
- (مهم) مدیر ارشد سازمان / مدیرامنیت اطلاعات (هیچگاه ... هیچگاه ...) نباید غافلگیر بشود

  (یا تصمیمات عجولانه در هنگام وقوع بحران بگیرد)

در واقع ...

مدیریت ریسک (Risk Management - RM)











اهمیت شناخت ریسک ها برای مدیران ...

- مدیر برای تصمیم گیری باید منابع خود را بشناسد (مانند دارایی ها / نیروی انسانی)
- برای تصمیم گیری درست مدیر باید ریسک ها را هم بشناسد

  (جزئی از دارایی های جدایی ناپذیر هر سازمان یا کسب و کار)
- (مهم) مدیر ارشد سازمان / مدیرامنیت اطلاعات (هیچگاه ... هیچگاه ...) نباید غافلگیر بشود

  (یا تصمیمات عجولانه در هنگام وقوع بحران بگیرد)

در واقع ...

- هوشیاری و آمادگی

مدیریت ریسک (Risk Management - RM)













اهمیت شناخت ریسک ها برای مدیران ...

- مدیر برای تصمیم گیری باید منابع خود را بشناسد (مانند دارایی ها / نیروی انسانی)
- برای تصمیم گیری درست مدیر باید ریسک ها را هم بشناسد

  (جزئی از دارایی های جدایی ناپذیر هر سازمان یا کسب و کار)
- (مهم) مدیر ارشد سازمان / مدیرامنیت اطلاعات (هیچگاه ... هیچگاه ...) نباید غافلگیر بشود

  (یا تصمیمات عجولانه در هنگام وقوع بحران بگیرد)

در واقع ...

- هوشیاری و آمادگی
- فرصت تصمیم برای اینکه اولویت های چیست و سبک و سنگین کردن هزینه های راهکردهای تعامل ریسک (trade-off)

مدیریت ریسک (Risk Management - RM)















اهمیت شناخت ریسک ها برای مدیران ...

- مدیر برای تصمیم گیری باید منابع خود را بشناسد (مانند دارایی ها / نیروی انسانی)
- برای تصمیم گیری درست مدیر باید ریسک ها را هم بشناسد

  (جزئی از دارایی های جدایی ناپذیر هر سازمان یا کسب و کار)
- (مهم) مدیر ارشد سازمان / مدیرامنیت اطلاعات (هیچگاه ... هیچگاه ...) نباید غافلگیر بشود

  (یا تصمیمات عجولانه در هنگام وقوع بحران بگیرد)

در واقع ...

- هوشیاری و آمادگی
- فرصت تصمیم برای اینکه اولویت های چیست و سبک و سنگین کردن هزینه های راهکردهای تعامل ریسک (trade-off)
- چاره اندیشی و تامین منابع

مدیریت ریسک (Risk Management - RM)







سوالات کلیدی ...

مدیریت ریسک (Risk Management - RM)



سوالات کلیدی ...

- منابع و دارایی های مهمی که نیاز به محافظت دارند چه چیزهایی هستند؟

مدیریت ریسک (Risk Management - RM)





سوالات کلیدی ...

- منابع و دارایی های مهمی که نیاز به محافظت دارند چه چیزهایی هستند؟
- تهدیدهایی که برای این دارایی ها وجود دارند چه هستند؟

مدیریت ریسک (Risk Management - RM)







سوالات کلیدی ...

- منابع و دارایی های مهمی که نیاز به محافظت دارند چه چیزهایی هستند؟
- تهدیدهایی که برای این دارایی ها وجود دارند چه هستند؟
- ما چه کارهایی می توانیم انجام بدهیم؟



تحلیل ریسک (Risk Analysis - RA)

تحلیل ریسک (Risk Analysis - RA)



تحلیل ریسک (Risk Analysis)

فرایندی سیستماتیک و منظم برای شناسایی، ارزیابی و درک مخاطراتی است که می‌توانند بر اهداف، دارایی‌ها یا پروژه‌های یک سازمان تاثیر منفی بگذارند

تحلیل ریسک (Risk Analysis - RA)









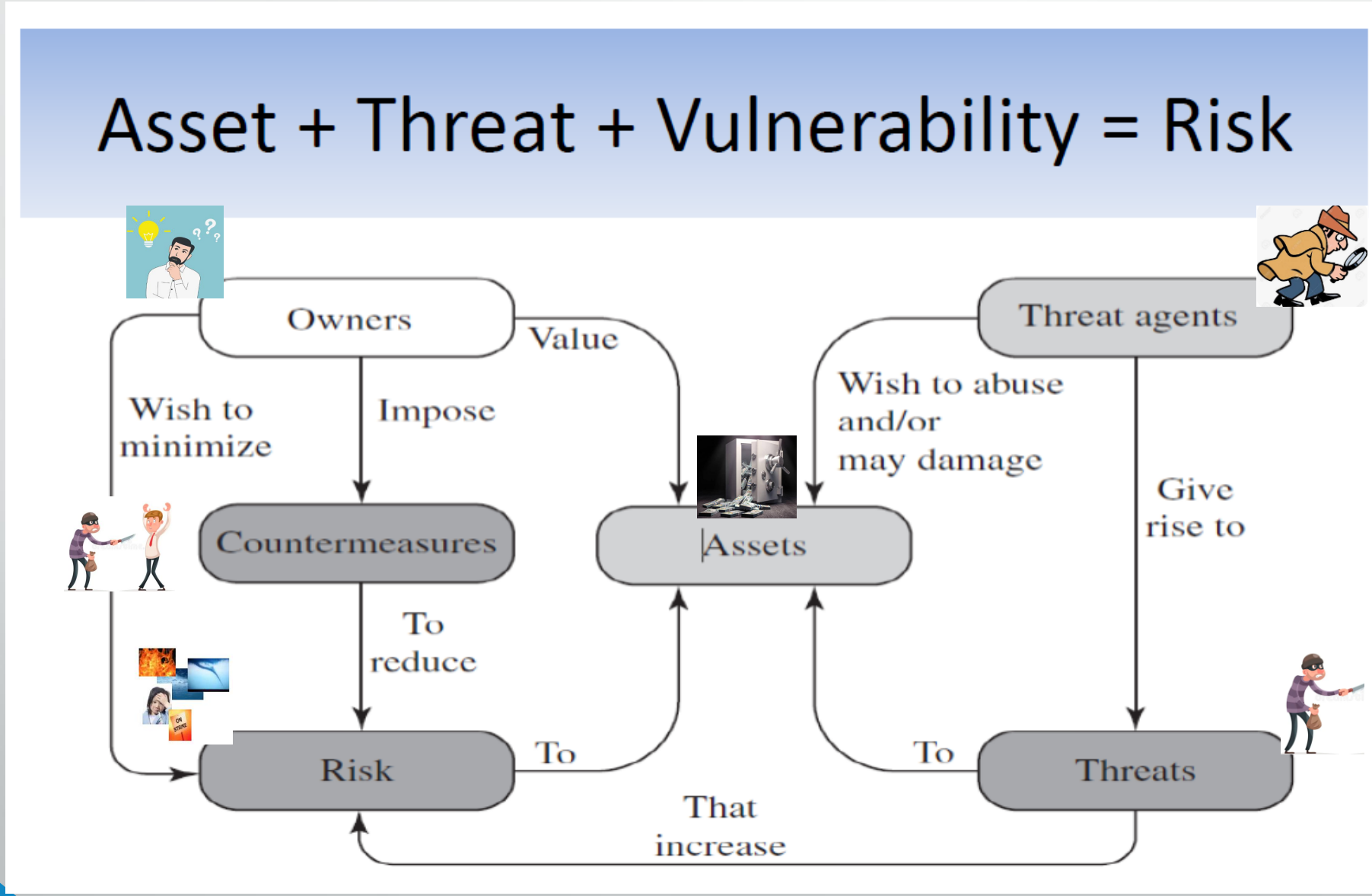
تحلیل ریسک (Risk Analysis)

فرایندی سیستماتیک و منظم برای شناسایی، ارزیابی و درک مخاطراتی است که می‌توانند بر اهداف، دارایی‌ها یا پروژه‌های یک سازمان تاثیر منفی بگذارند

در یک تعریف جامع‌تر، تحلیل ریسک پاسخ به این سه پرسش اصلی است:

- **چه اتفاقی ممکن است بیفتد؟** شناسایی تهدیدها و آسیب‌پذیری‌ها
- **احتمال وقوع آن چقدر است؟** ارزیابی احتمال وقوع
- **در صورت وقوع، چه میزان خسارت وارد می‌شود؟**

مدیریت ریسک (Risk Management - RM)



فرایند کلی مدیریت ریسک (Risk Management - RM)



- چرا تحلیل ریسک انجام می دهیم؟

فرایند کلی مدیریت ریسک (Risk Management - RM)





- چرا تحلیل ریسک انجام می دهیم؟
  - فیلتر کردن و مشخص کردن ریسک هایی که می تواند روی سرویس های ما تاثیر بگذارد

فرایند کلی مدیریت ریسک (Risk Management - RM)



- چرا تحلیل ریسک انجام می دهیم؟
  - فیلتر کردن و مشخص کردن ریسک هایی که می تواند روی سرویس های ما تاثیر بگذارد



جهت شناسایی /برای تشخیص ...

- نقاط ضعف و تهدیدها، عواقب و پیامدها اگر ...
- راهکارهای جایگزین اگر ...



فرایند کلی مدیریت ریسک (Risk Management - RM)



- چرا تحلیل ریسک انجام می دهیم؟
  - فیلتر کردن و مشخص کردن ریسک هایی که می تواند روی سرویس های ما تاثیر بگذارد



جهت شناسایی /برای تشخیص ...

- نقاط ضعف و تهدیدها، عواقب و پیامدها اگر ...
- راهکارهای جایگزین اگر ...
- هزینه‌ها برای:
  - مدیریت و مواجهه با ریسک
  - از دست رفتن کسب‌وکار
  - فرصت‌های شغلی
  - از دست رفتن اعتماد





فرایند کلی مدیریت ریسک (Risk Management - RM)

- چه وقت تحلیل ریسک ها را انجام می دهیم؟



فرایند کلی مدیریت ریسک (Risk Management - RM)

- چه وقت تحلیل ریسک ها را انجام می دهیم؟

- TG 0. Initiating a pre study
- TG 1. Initiating feasibility study
- TG 2. Initiating project execution
- TG 3. Shall the project continue with original or revised plans?
- TG 4. Initiating release of result
- TG 5. Initiating project approval and closure



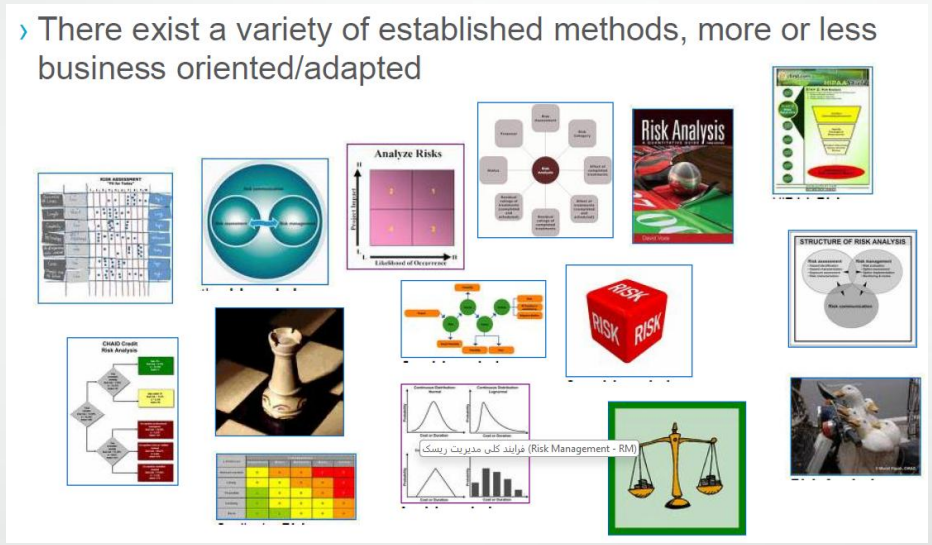
فرایند کلی مدیریت ریسک (Risk Management - RM)

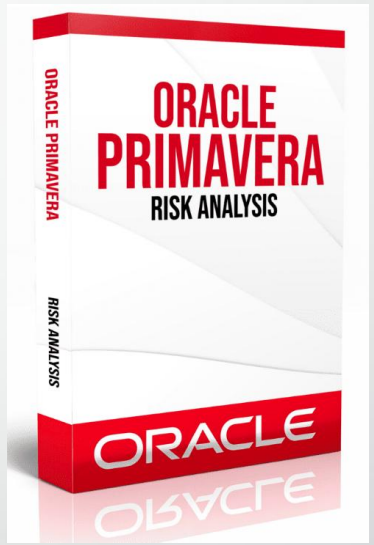
- ابزارها و روش های تحلیل ریسک؟

فرایند کلی مدیریت ریسک (Risk Management - RM)

- ابزارها و روش های تحلیل ریسک؟

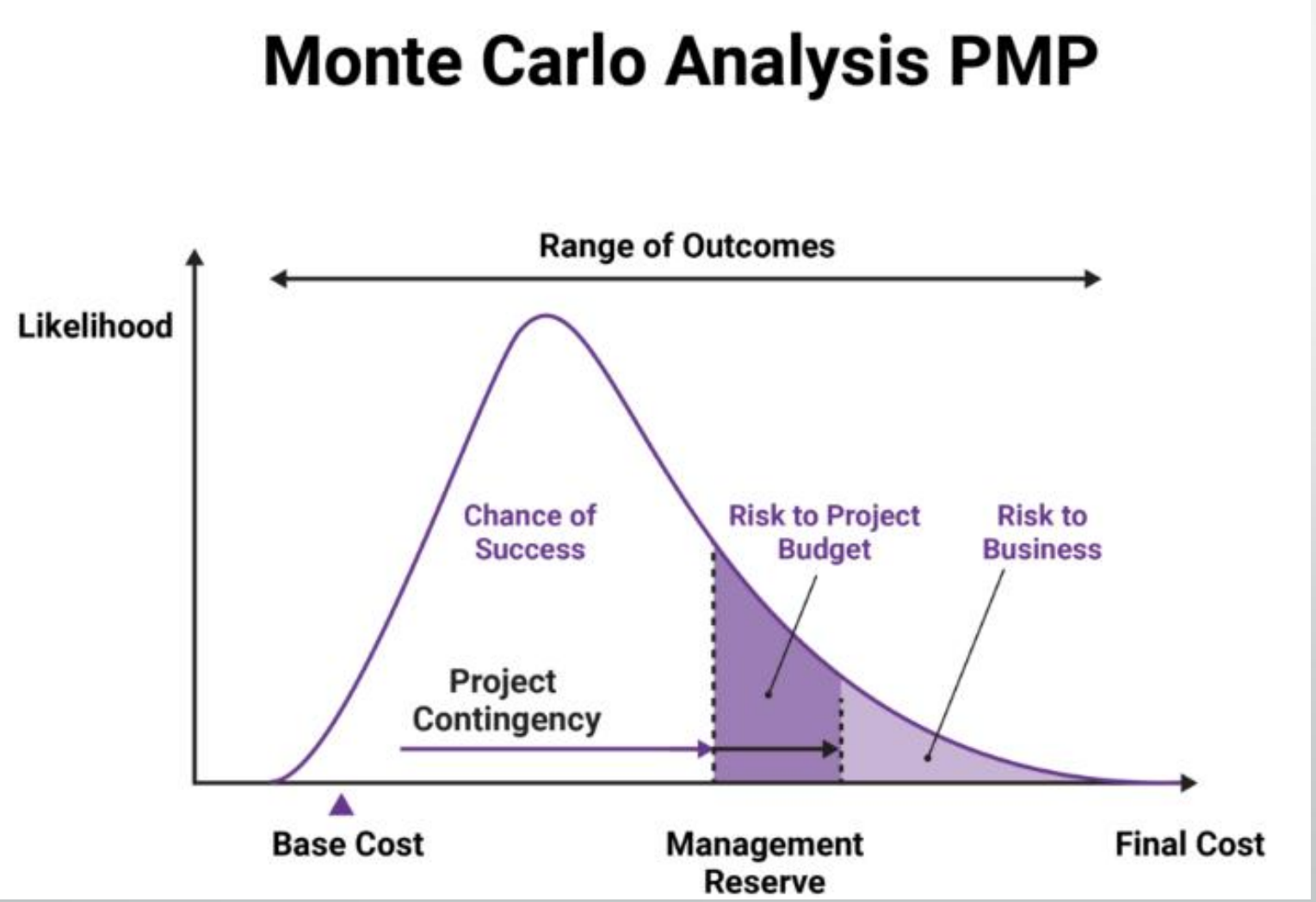






فرایند کلی مدیریت ریسک (Risk Management - RM)

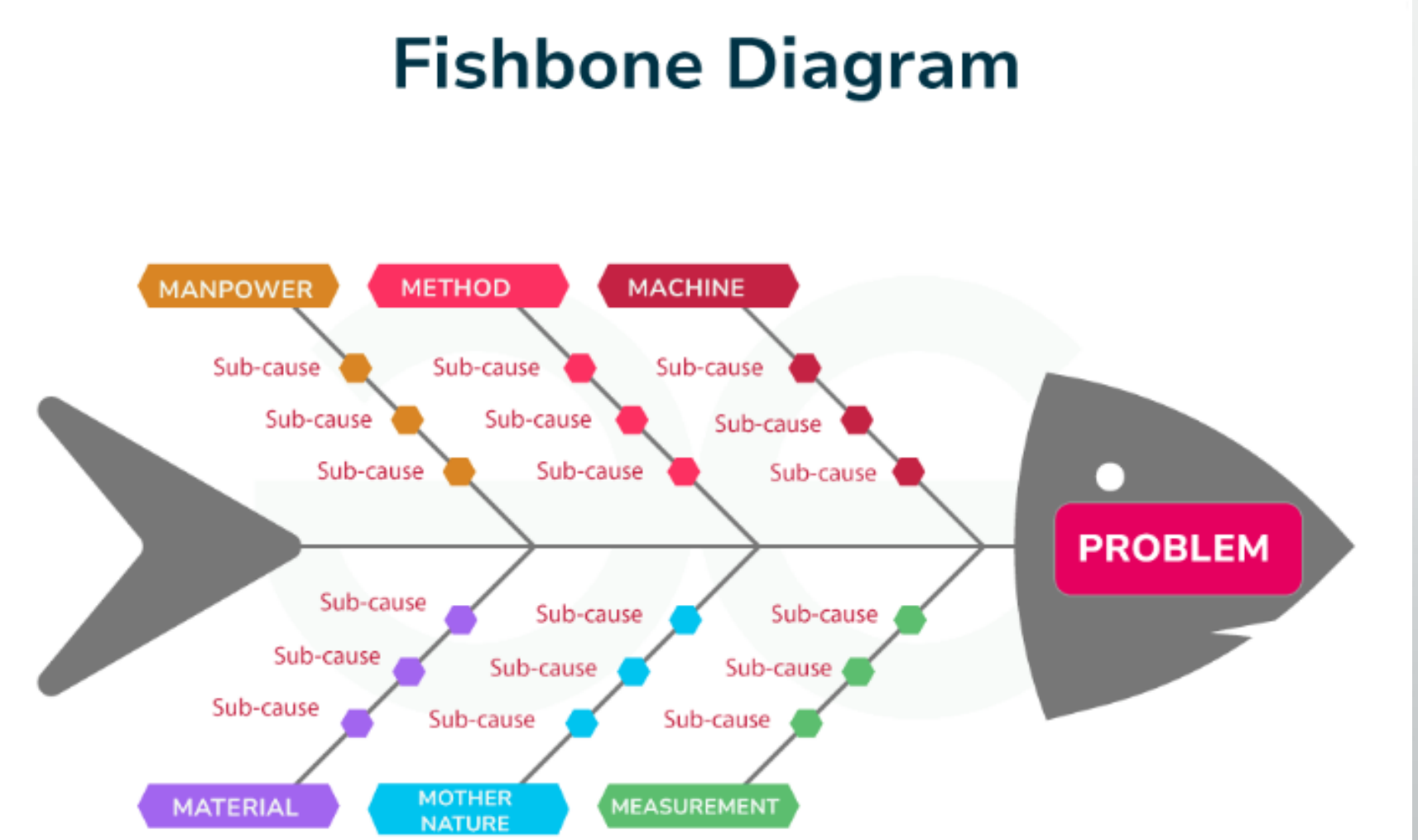
- ابزارها و روش های تحلیل ریسک؟



فرایند کلی مدیریت ریسک (Risk Management - RM)

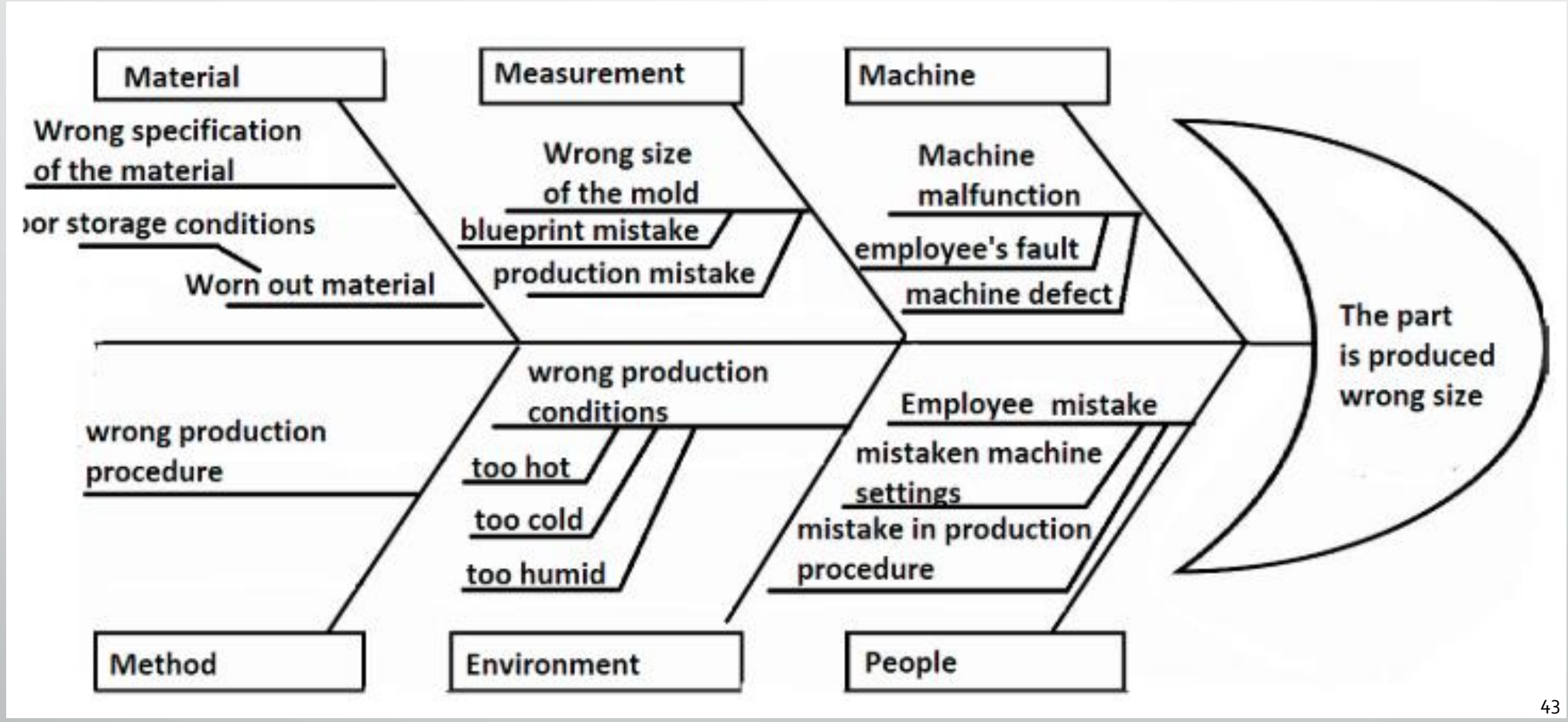
- ابزارها و روش های تحلیل ریسک؟

Ishikawa diagram



فرایند کلی مدیریت ریسک (Risk Management - RM)

- مثالی از استفاده از نمودار استخوان ماهی Ishikawa diagram



فرایند کلی مدیریت ریسک (Risk Management - RM)

- ابزارها و روش های تحلیل ریسک؟

Enterprise Risk Management (ERM) & GRC Platforms

These heavy-duty enterprise systems unify operational risk, internal audits, policy management, and regulatory compliance into a centralized company dashboard. Logical Commander +1

- Archer **(formerly RSA Archer):** One of the most long-standing names in corporate governance. It is highly favored by mature enterprises that need structured control libraries and rigorous cross-functional data modeling. Logical Commander
- Mitratech Alyne**:** Widely recognized for its modern, no-code configuration. It utilizes an AI engine to map operational documents against global regulatory frameworks like ISO 27001 and NIST. Mitratech
- MetricStream**:** Known for its deep risk assessment scoring, automated compliance workflows, and real-time risk intelligence driven by AI analytics.
- **LogicGate Risk Cloud:** An incredibly flexible, user-friendly, no-code alternative. It allows expanding businesses to build custom risk pathways without requiring extensive IT implementation. Mitratech
- **ServiceNow GRC:** The go-to option for large enterprises already using the ServiceNow operational ecosystem, allowing teams to route risk reporting over existing IT workflows. Mitratech

فرایند کلی مدیریت ریسک (Risk Management - RM)

- ابزارها و روش های تحلیل ریسک؟

🔐 Cybersecurity, Trust, & Privacy Compliance

These platforms continuously scan an organization's digital perimeter to detect data vulnerabilities, manage third-party vendor exposures, and automate security frameworks.

- **OneTrust:** The market leader in privacy data mapping. It is primarily used to ensure large-scale business operations strictly follow global privacy legal frameworks like GDPR and CCPA.
- **Vanta & Drata:** Both are automated "Trust Management" tools highly popular with tech companies and startups. They offer automated evidence collection to continuously prove compliance for audits like SOC 2.
- **SecurityScorecard:** Focuses explicitly on vendor and supply chain risk. It assigns continuous cybersecurity posture scores to outside vendors so organizations can block third-party data breaches. Vanta

فرایند کلی مدیریت ریسک (Risk Management - RM)

- ابزارها و روش های تحلیل ریسک؟

🗓 Project & Schedule Quantitative Risk Analysis

Unlike qualitative compliance dashboards, these desktop and cloud utilities rely on mathematical simulations to assess the odds of project failure or cost overruns. Invensis Learning

- Safran Risk: A premier tool for massive industrial and construction mega-projects. It features probabilistic schedule analytics natively integrated with scheduling software like Primavera P6.
- **Active Risk Manager (ARM):** A comprehensive system built specifically for program management offices (PMOs) to manage complex corporate project portfolios.
- **Predict!:** A direct, cost-effective Microsoft Project add-in that allows teams to run quick Monte Carlo risk simulations directly within their baseline project schedules. Invensis Learning



فرایند کلی مدیریت ریسک (Risk Management - RM)

- رابطه "مدیریت ریسک" و "تحلیل ریسک"



فرایند کلی مدیریت ریسک (Risk Management - RM)

- رابطه "مدیریت ریسک" و "تحلیل ریسک"
  - این دو بخش هایی جدایی ناپذیر هستند



فرایند کلی مدیریت ریسک (Risk Management - RM)

- رابطه "مدیریت ریسک" و "تحلیل ریسک"
  - این دو بخش هایی جدایی ناپذیر هستند
  - اگر تحلیل درست انجام نشود ... مدیریت ریسک فایده ی ندارد



فرایند کلی مدیریت ریسک (Risk Management - RM)

- رابطه "مدیریت ریسک" و "تحلیل ریسک"
  - این دو بخش هایی جدایی ناپذیر هستند
  - اگر تحلیل درست انجام نشود ... مدیریت ریسک فایده ی ندارد
  - اگر مدیریت درست انجام نشود ... تحلیل درست فایده ی ندارد



فرایند کلی مدیریت ریسک (Risk Management - RM)

- رابطه "مدیریت ریسک" و "تحلیل ریسک"
  - این دو بخش هایی جدایی ناپذیر هستند
  - اگر تحلیل درست انجام نشود ... مدیریت ریسک فایده ی ندارد
  - اگر مدیریت درست انجام نشود ... تحلیل درست فایده ی ندارد
  - تحلیل درست ریسک ... تصمیم گیری در مدیریت ریسک را ساده تر می کند



فرایند کلی مدیریت ریسک (Risk Management - RM)

- رابطه "مدیریت ریسک" و "تحلیل ریسک"
  - این دو بخش هایی جدایی ناپذیر هستند
  - اگر تحلیل درست انجام نشود ... مدیریت ریسک فایده ی ندارد
  - اگر مدیریت درست انجام نشود ... تحلیل درست فایده ی ندارد
  - تحلیل درست ریسک ... تصمیم گیری در مدیریت ریسک را ساده تر می کند
  - تحلیل درست و دقیق ریسک ... می تواند ما را به پیش بینی واقعیت نزدیک تر کند



فرایند کلی مدیریت ریسک (Risk Management - RM)

- رابطه "مدیریت ریسک" و "تحلیل ریسک"
  - این دو بخش هایی جدایی ناپذیر هستند
  - اگر تحلیل درست انجام نشود ... مدیریت ریسک فایده ی ندارد
  - اگر مدیریت درست انجام نشود ... تحلیل درست فایده ی ندارد
  - تحلیل درست ریسک ... تصمیم گیری در مدیریت ریسک را ساده تر می کند
  - تحلیل درست و دقیق ریسک ... می تواند ما را به پیش بینی واقعیت نزدیک تر کند
  - هر نوع مدیریتی ... نیاز به مدیریت ریسک دارد ... و مدیریت ریسک به تحلیل ریسک



فرایند کلی مدیریت ریسک (Risk Management - RM)

- رابطه "مدیریت ریسک" و "تحلیل ریسک" ادامه ...



فرایند کلی مدیریت ریسک (Risk Management - RM)

- رابطه "مدیریت ریسک" و "تحلیل ریسک" ادامه ...
  - مدیریت صحیح ریسک ... می تواند به تصمیمات صحیح استراتژیک سازمان کمک کند



فرایند کلی مدیریت ریسک (Risk Management - RM)

- رابطه "مدیریت ریسک" و "تحلیل ریسک" ادامه ...
  - مدیریت صحیح ریسک ... می تواند به تصمیمات صحیح استراتژیک سازمان کمک کند
  - مدیریت ریسک ... بخشی جدایی ناپذیر از هر مدیریتی می باشد

فرایند کلی مدیریت ریسک (Risk Management - RM)

- و اما ... فرهنگ سازی / همراهی نیروهای سازمان (ایمان نه اجبار)

فرایند کلی مدیریت ریسک (Risk Management - RM)







- و اما ... فرهنگ سازی / همراهی نیروهای سازمان (ایمان نه اجبار)

› Key to success in all Risk Management is
  - To encourage the organization to take initiative, i.e.:
    - People should always ask “what can I contribute with”
    - People should not wait for “somebody else to come with a solution or directive”
  - To encourage people to step out of “fire fighting mode”, i.e. search and identify the not obvious risks

i.e. “If it’s to be… it’s up to me” -mentality

فرایند کلی مدیریت ریسک (Risk Management - RM)

- و اما ... ارتباط صحیح و موثر ...
- و اما ... لحن سخن گفتن ...

فرایند کلی مدیریت ریسک (Risk Management - RM)







- و اما ... ارتباط صحیح و موثر ...
- و اما ... لحن سخن گفتن ...

› How to communicate risks to steering groups?
  – Mgmt / sponsors seldom like to hear bad news
  – They like to hear:
    › Good Progress
    › Opportunities where they can contribute

› When presenting risks, give management / sponsors options to choose between.
› Quantify needed actions and resources that make the difference between failure and success:

  – The risk is that …….will/can happened



  – If we do …. or this…we can mitigate…. and by that minimize ….consequence



با تشکر







