IT Security and Risk Management

Risk management Identification

ا.د. حنان الطاهر الداقيز

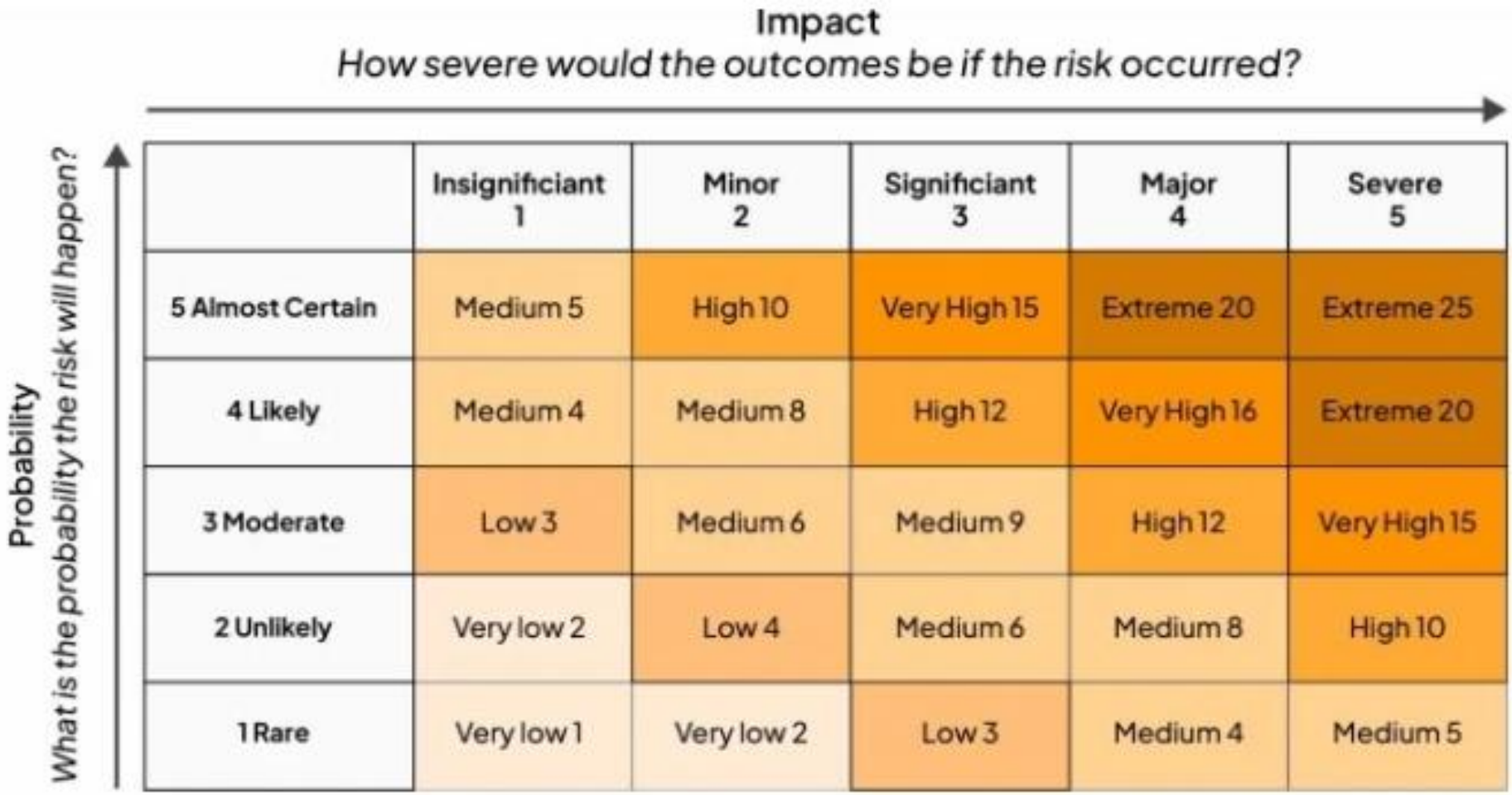
h.dagez@uot.edu.ly

ربيع 2024

https://t.me/+xavNMXu7DyM5Yjc0

Risk Register

- The main output of the risk identification process is a list of identified risks and other information needed to begin creating a risk register
- A **risk register** is:
  - A document that contains the results of various risk management processes and that is often displayed in a table or spreadsheet format
  - A tool for documenting potential risk events and related information
- **Risk events** refer to specific, uncertain events that may occur to the detriment or enhancement of the project.



	Insignificiant 1	Minor 2	Significiant 3	Major 4	Severe 5
5 Almost Certain	Medium 5	High 10	Very High 15	Extreme 20	Extreme 25
4 Likely	Medium 4	Medium 8	High 12	Very High 16	Extreme 20
3 Moderate	Low 3	Medium 6	Medium 9	High 12	Very High 15
2 Unlikely	Very low 2	Low 4	Medium 6	Medium 8	High 10
1 Rare	Very low 1	Very low 2	Low 3	Medium 4	Medium 5

Risk Register Contents, Part 1

- An identification number for each risk event
- A rank for each risk event
- The name of each risk event
- A description of each risk event
- The category under which each risk event falls
- The root cause of each risk

Risk Register Contents, Part 2

- Triggers for each risk; **triggers** are indicators or symptoms of actual risk events.
- Potential responses to each risk
- The **risk owner** or person who will own or take responsibility for each risk
- The probability and impact of each risk occurring.
- The status of each risk

Sample Risk Register

No.	Rank	Risk	Description	Category	Root Cause	Triggers	Potential Responses	Risk owner	Probability	Impacts	Status
R44	1										
R21	2										
R7	3										

- No.: R44
- Rank: 1
- Risk: New customer
- Description: We have never done a project for this organization before and don't know too much about them. One of our company's strengths is building good customer relationships, which often leads to further projects with that customer. We might have trouble working with this customer because they are new to us.
- Category: People risk.
- Etc.

Performing Qualitative Risk Analysis

- Assess the likelihood and impact of identified risks to determine their priority.
- Risk quantification tools and techniques include:
  - Probability/impact matrixes
  - The Top Ten Risk Item Tracking
  - Expert judgment

Probability/Impact Matrix

- A **probability/impact matrix** or **chart** lists the relative probability of a risk occurring on one side of a matrix or axis on a chart and the relative impact of the risk occurring on the other.
- List the risks and then label each one as high, medium, or low in terms of its probability of occurrence and its impact if it did occur
- Can also calculate **risk factors**:
  - Numbers that represent the overall risk of specific events based on their probability of occurring and the consequences to the project if they do occur.

Sample Probability/Impact Matrix

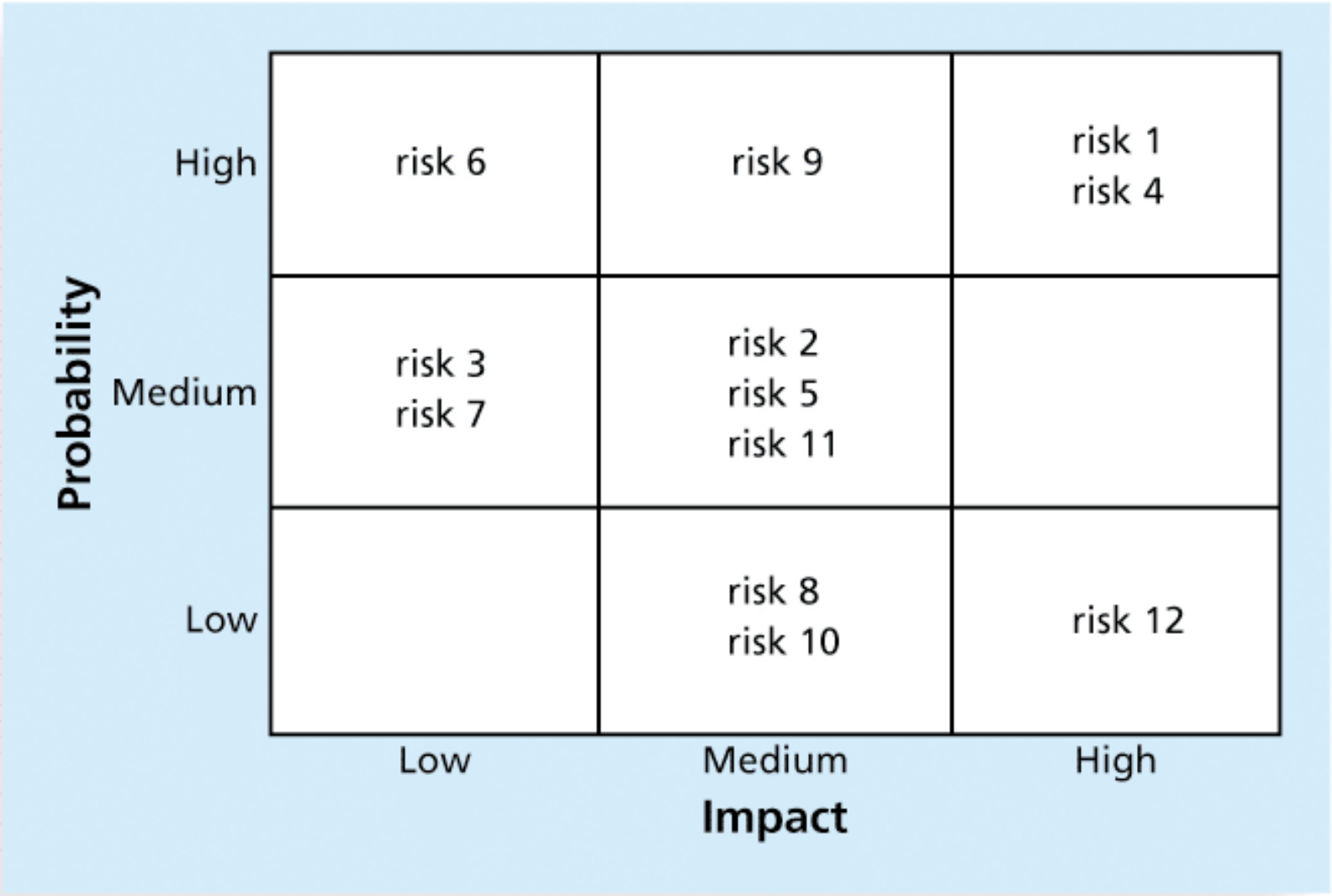
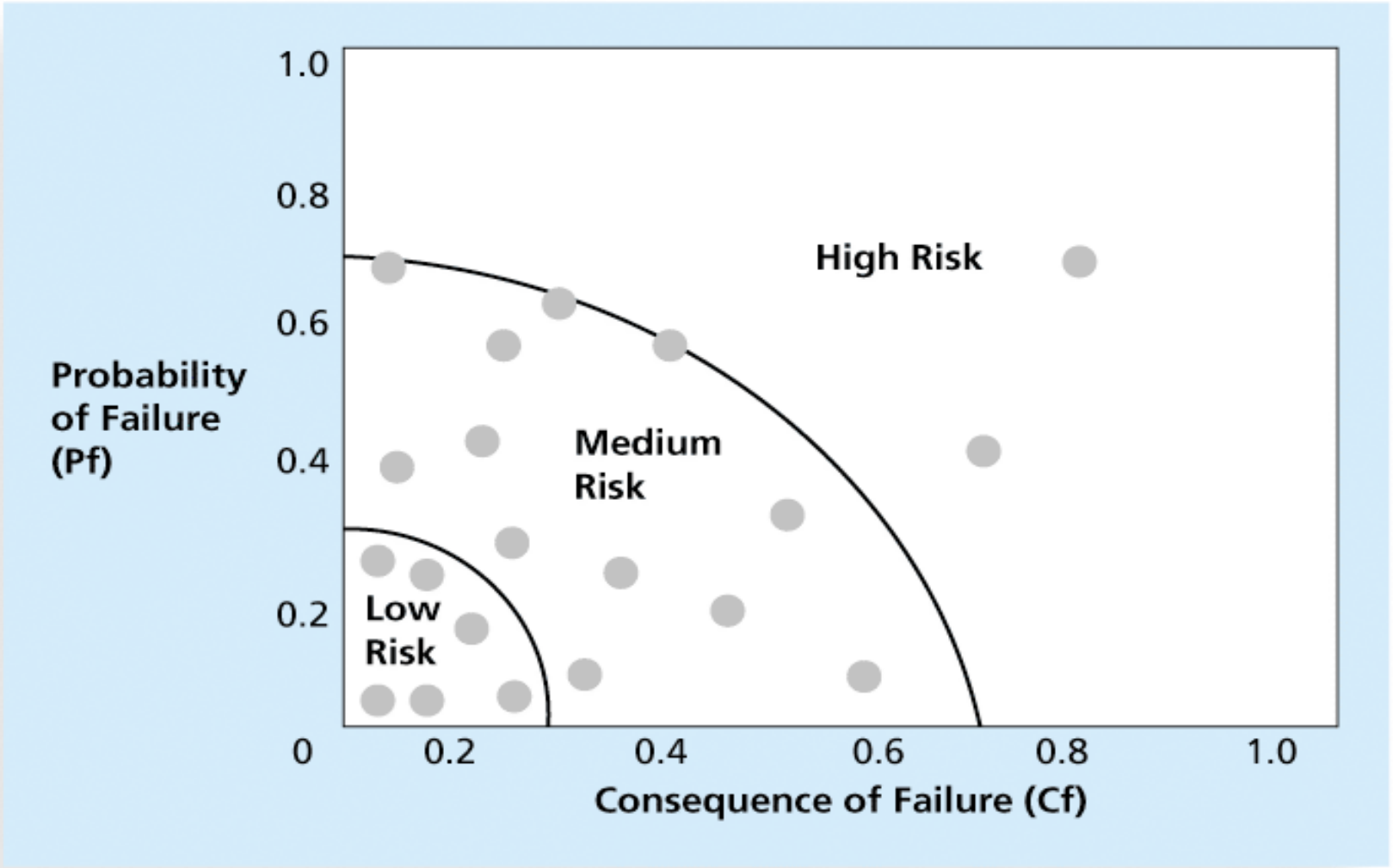


Chart Showing High-, Medium-, and Low-Risk Technologies



Top Ten Risk Item Tracking

- **Top Ten Risk Item Tracking** is a qualitative risk analysis tool that helps to identify risks and maintain an awareness of risks throughout the life of a project.
- Establish a periodic review of the top ten project risk items.
- List the current ranking, previous ranking, number of times the risk appears on the list over a period of time, and a summary of progress made in resolving the risk item.

Example of Top Ten Risk Item Tracking

Risk Event	Rank this month	Rank last month	Number of months in top ten	Risk resolution progress
Inadequate planning	1	2	4	Working on revising the entire project management plan
Poor definition	2	3	3	Holding meetings with project customer and sponsor to clarify scope
Absence of leadership	3	1	2	After previous project manager quit, assigned a new one to lead the project
Poor cost estimates	4	4	3	Revising cost estimates
Poor time estimates	5	5	3	Revising schedule estimates

Watch List

- A **watch list** is a list of risks that are low priority, but are still identified as potential risks.
- Qualitative analysis can also identify risks that should be evaluated on a quantitative basis.

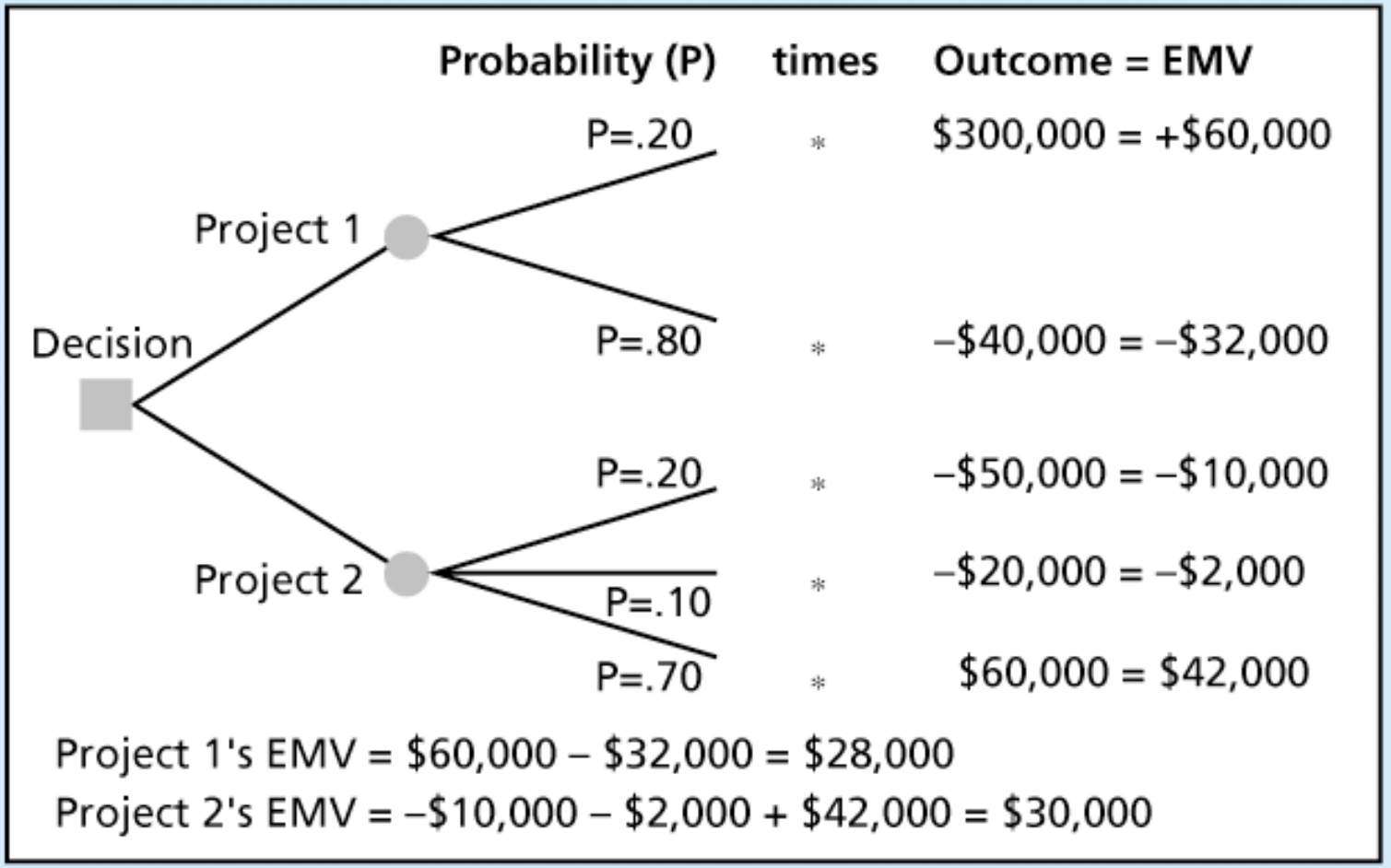
Performing Quantitative Risk Analysis

- Often follows qualitative risk analysis, but both can be done together.
- Large, complex projects involving leading edge technologies often require extensive quantitative risk analysis.
- Main techniques include:
  - Decision tree analysis
  - Simulation
  - Sensitivity analysis

Decision Trees and Expected Monetary Value (EMV)

- A **decision tree** is a diagramming analysis technique used to help select the best course of action in situations in which future outcomes are uncertain
- **Estimated monetary value (EMV)** is the product of a risk event probability and the risk event's monetary value.
- You can draw a decision tree to help find the EMV.

Expected Monetary Value (EMV) Example



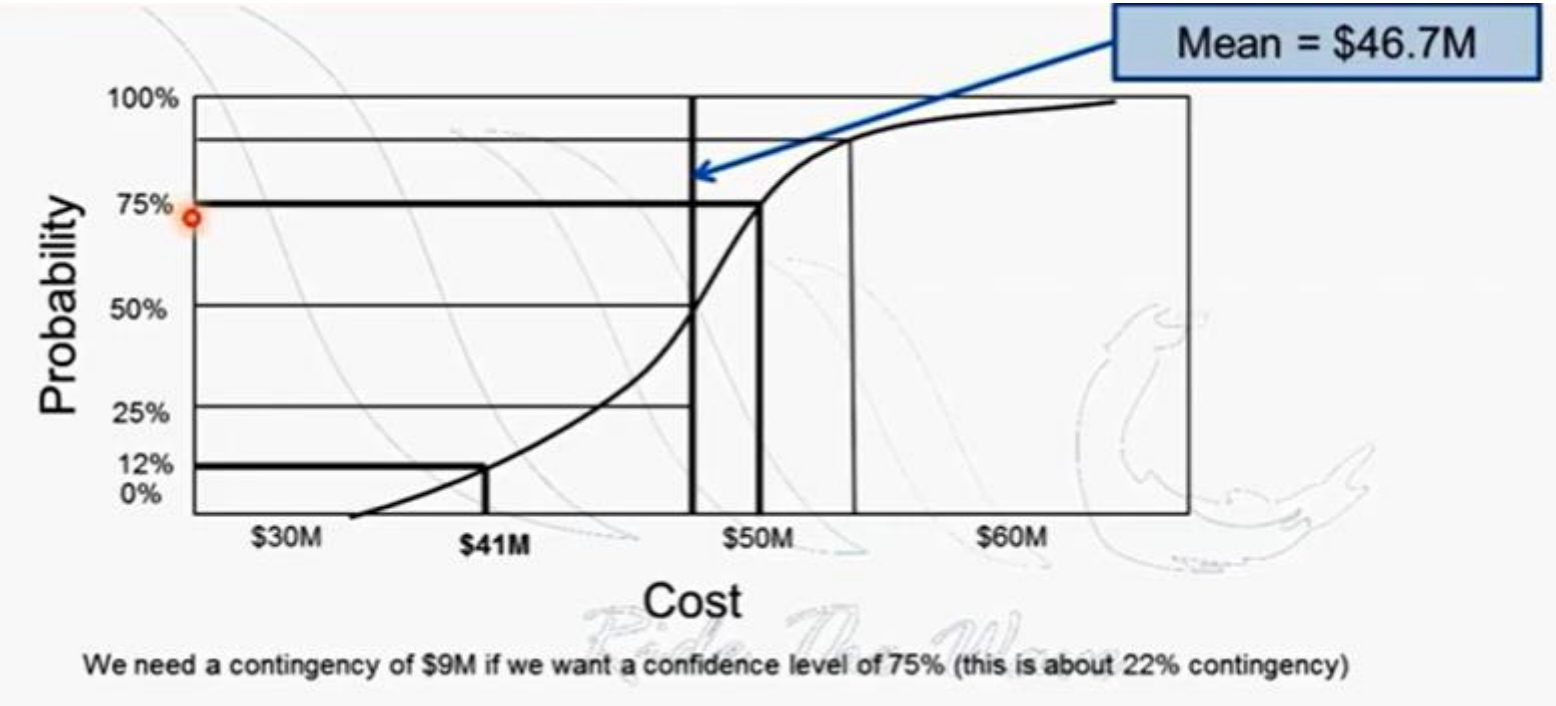
Simulation

- Simulation uses a representation or model of a system to analyze the expected behavior or performance of the system.
- **Monte Carlo analysis** simulates a model's outcome many times to provide a statistical distribution of the calculated results.
- To use a Monte Carlo simulation, you must have three estimates (most likely, pessimistic, and optimistic) plus an estimate of the likelihood of the estimate being between the most likely and optimistic values.

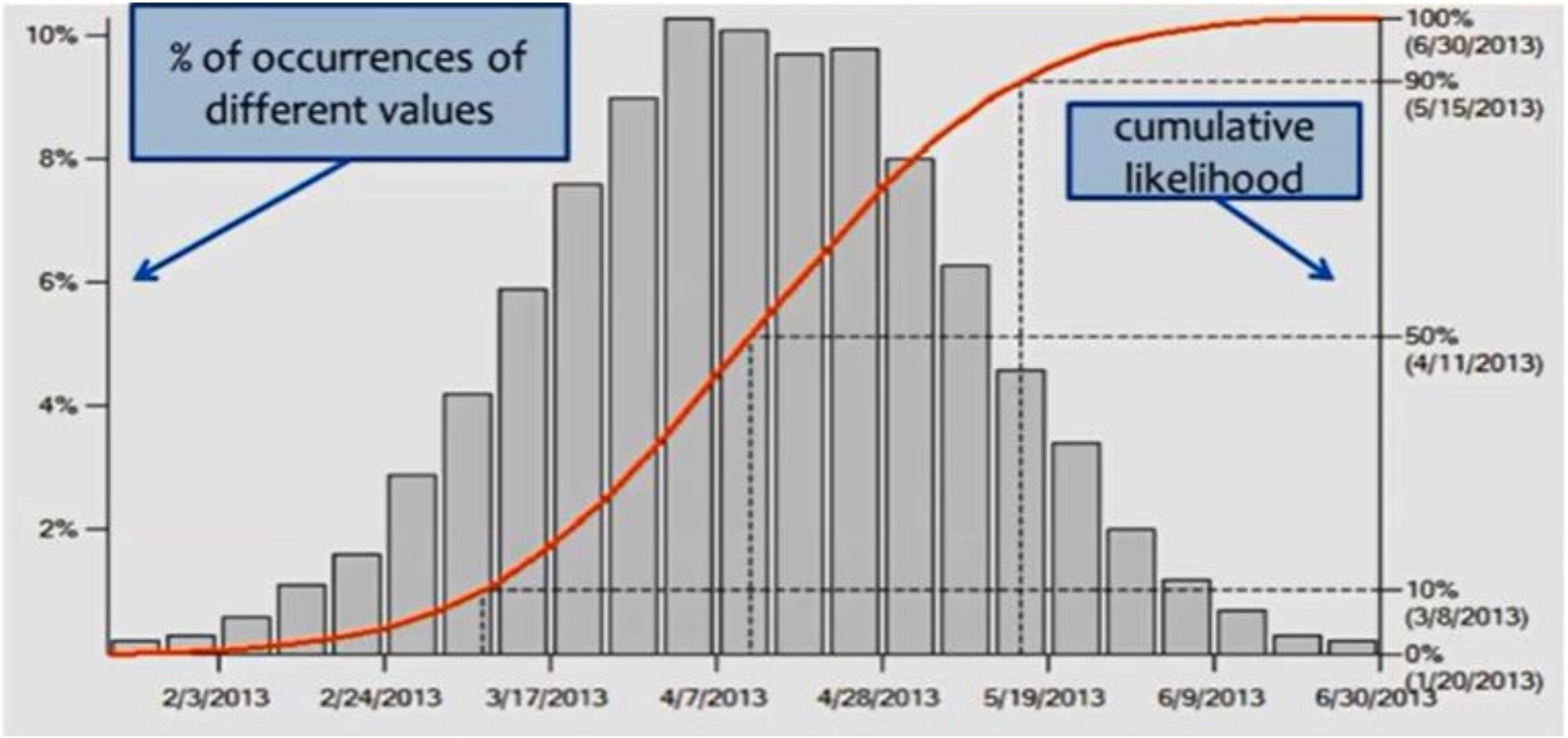
Steps of a Monte Carlo Analysis

1. Assess the range for the variables being considered.
2. Determine the probability distribution of each variable.
3. For each variable, select a random value based on the probability distribution.
4. Run a deterministic analysis or one pass through the model
5. Repeat steps 3 and 4 many times to obtain the probability distribution of the model's results.

Sample Monte Carlo Simulation Results for Project Schedule



Sample Monte Carlo Simulation Results for Project Schedule



Planning Risk Responses

- After identifying and quantifying risks, you must decide how to respond to them.
- Four main response strategies for negative risks:
  - Risk avoidance
  - Risk acceptance
  - Risk transference
  - Risk mitigation

General Risk Mitigation Strategies for Technical, Cost, and Schedule Risks

Technical Risks	Cost Risks	Schedule Risks
Emphasize team support and avoid stand-alone project structure	Increase the frequency of project monitoring	Increase the frequency of project monitoring
Increase project manager authority	Use WBS and CPM	Use WBS and CPM
Improve problem handing and communication	Improve communication, project goals understanding, and team support	Select the most experienced project manager
Increase the frequency of project monitoring	Increase project manager authority	
Use WBS and CPM		

Response Strategies for Positive Risks

- Risk exploitation استغلال الخطر
- Risk sharing مشاركة الخطر
- Risk enhancement تعزيز الخطر
- Risk acceptance قبول الخطر

Residual and Secondary Risks

- It’s also important to identify residual and secondary risks
- **Residual risks** (المخاطر المتبقية) are risks that remain after all of the response strategies have been implemented
- **Secondary risks** (المخاطر الثانوية) are a direct result of implementing a risk response

Controlling Risks

- Involves executing the risk management process to respond to risk events and ensuring that risk awareness is an ongoing activity performed by the entire project team throughout the entire project.
- **Workarounds** are unplanned responses to risk events that must be done when there are no contingency plans.
- **Main outputs of risk control are**:
  - Work performance information.
  - change requests.
  - updates to the project management plan, other project documents, and organizational process assets.

Using Software to Assist in Project Risk Management

- Risk registers can be created in a simple Word or Excel file or as part of a database.
- More sophisticated risk management software, such as Monte Carlo simulation tools, help in analyzing project risks.

THANK YOU

ANY QUESTION?