

Project Risk & Supply Chain Risk

Prepared by Dr. Dalia Hosni

Lecture 3



PMG 663

Project Risk & Supply Chain Risk



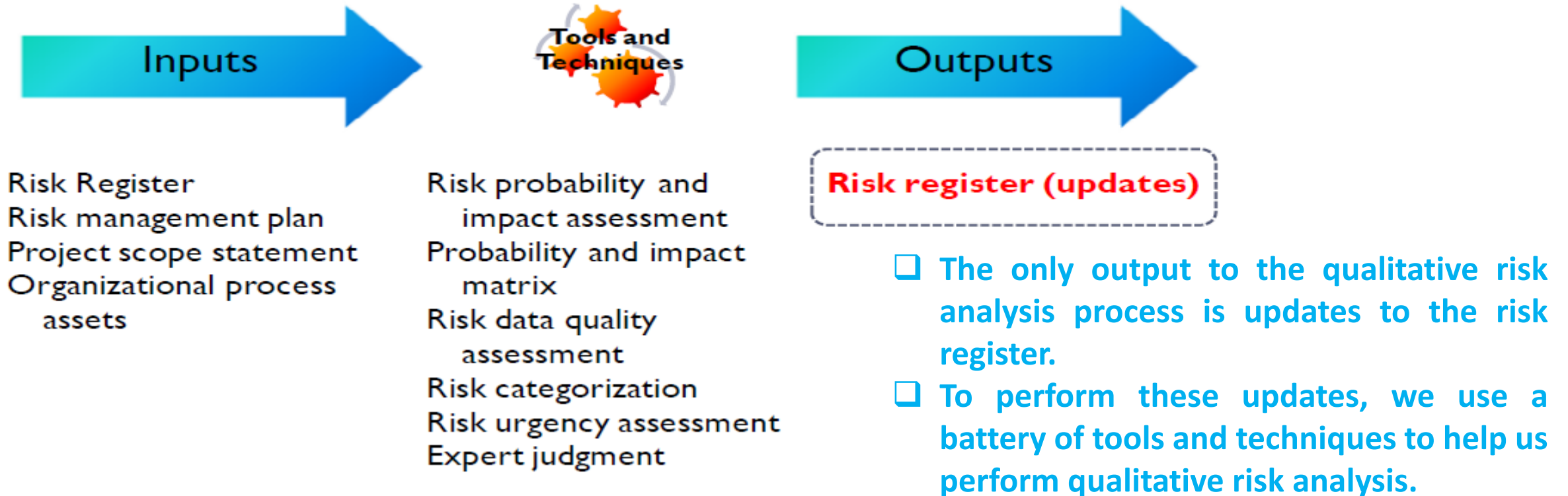
جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY



- Plan Risk Management
- Identify Risks
- Perform Qualitative Risk Analysis
- Perform Quantitative Risk Analysis
- Plan Risk Responses
- Monitor and Control Risks



Perform Qualitative Risk Analysis



Qualitative Risk Assessment Matrix

The qualitative risk assessment matrix offers a summary level of the potential impact of the risk, based on approximate percentages. Notice that this matrix shows general percentages that are not tied to specific dollar amounts or timelines. Another way of showing a qualitative impact is to rank the probabilities as high, medium or low:

Risk	Impact	Likelihood
Shipments are delayed	High	Low
Long lead times for hardware	Medium	Medium
Resource unavailability	Medium	Low
Rework issues	Low	High



Risk Register Updates

Partial List of Risk Register Updates:

- ☐ Ranking and prioritization of project risks
- ☐ Grouping risks by categories
- ☐ Risks requiring near-term response
- ☐ Risks requiring additional analysis and response
- ☐ Low priority risks to monitor
- ☐ Look for trends in results – regression analysis or trend charts



Risk Register Updates

Risk register updates will generally include the outcome of risk assessments, risk audits, and periodic risk reviews. This can include identification of new risk events or updates to risk probability, risk impact, risk priority and risk response plans

An important use of the risk register is to view the actual outcomes of the project risks and risk responses against anticipated risks. This data can help project managers plan for risk as the project moves forward



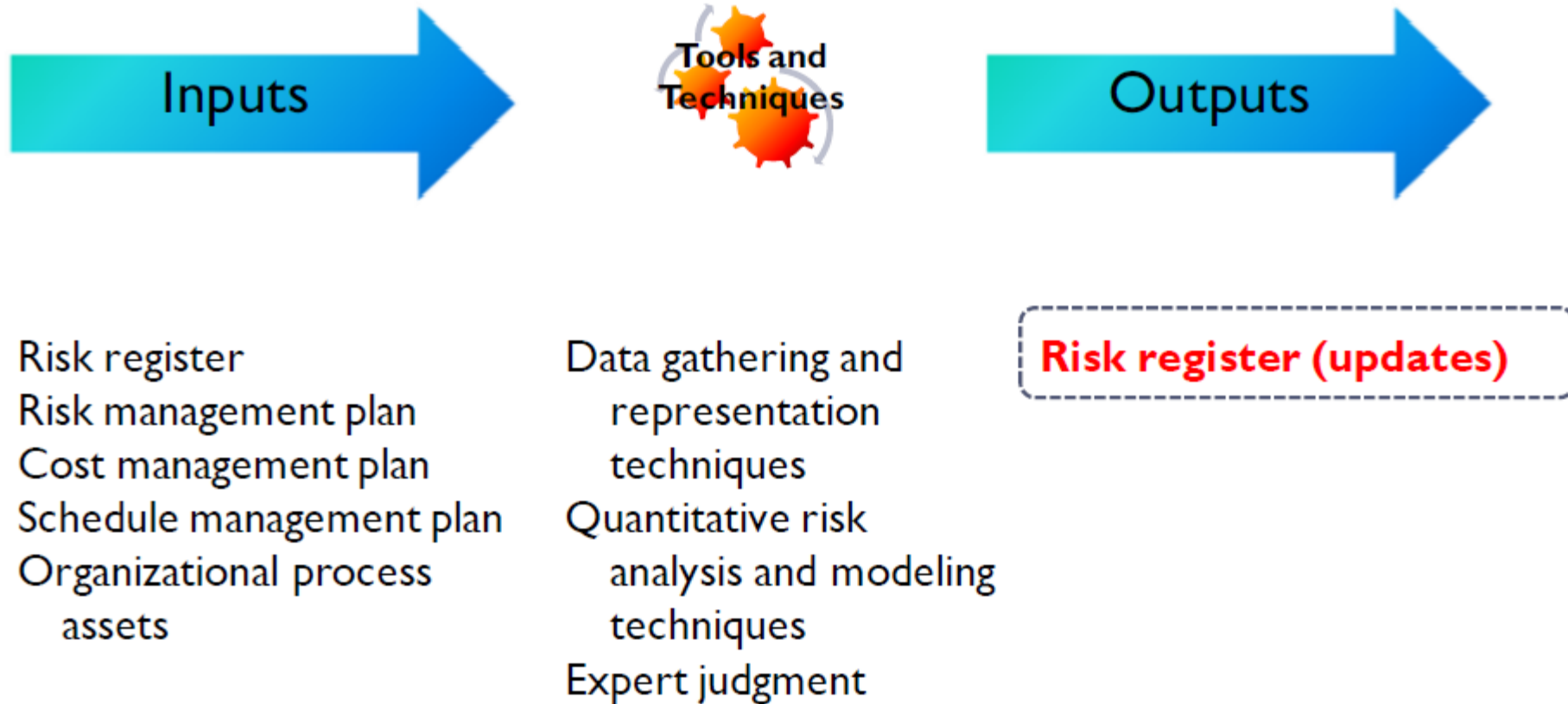
Risk Register Updates



Risk Register updates are an output of Perform Qualitative Risk Analysis, Perform Quantitative Risk Analysis, Plan Risk Responses and Monitor & Control Risks.

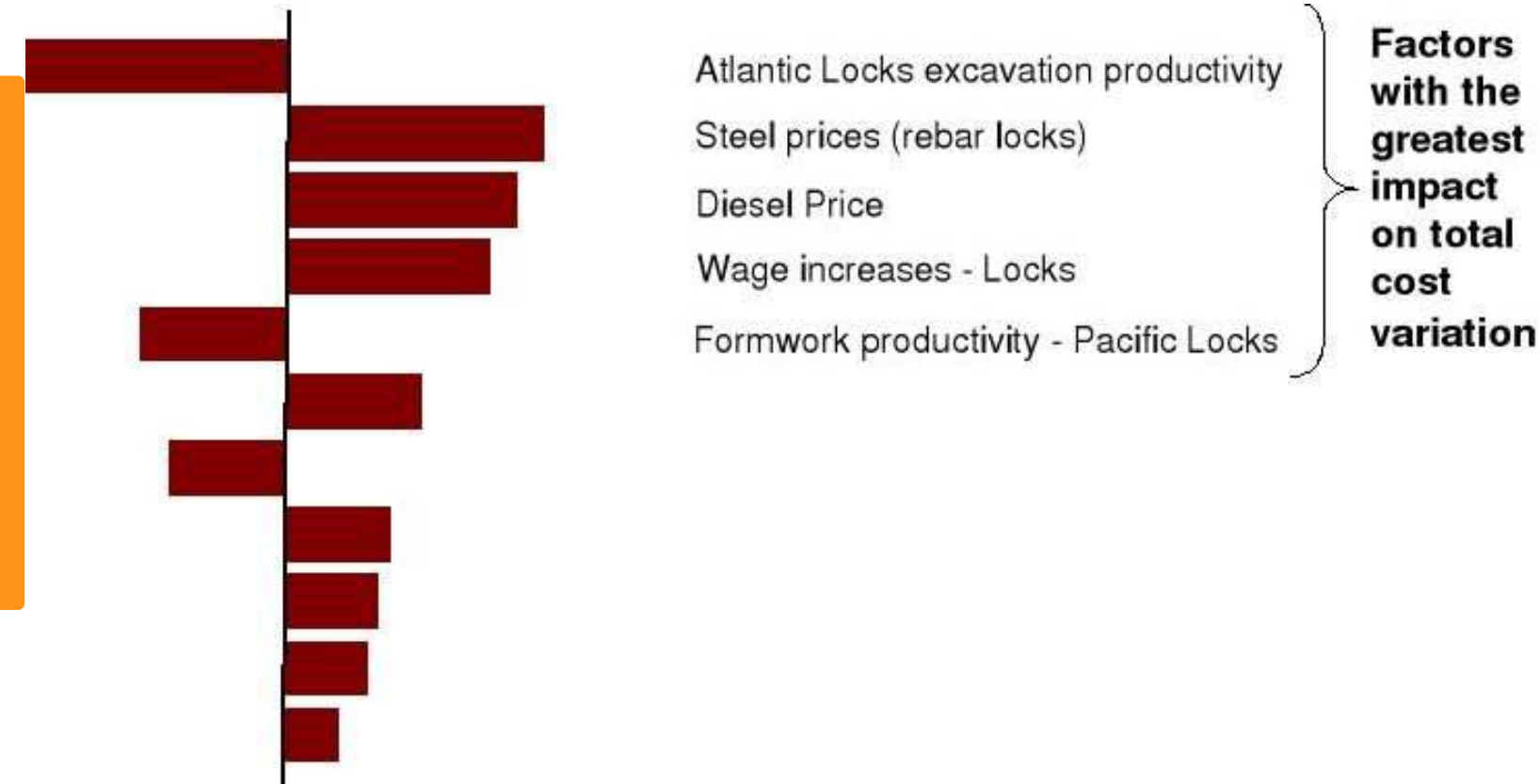


Perform Quantitative Risk Analysis



Quantitative risk analysis involves the numerical quantification and measurement of the effects of identified risks on the project. It frequently involves the use of sophisticated mathematical modeling techniques to create forecasts and trend analysis.





One of the more common analysis and modeling techniques is the sensitivity analysis, which is used to identify the risks with the largest potential impact on the project. The tornado diagram is frequently used to display the sensitivity analysis. The example shown is from the US Department of Transportation



Chapter 03

قابلية
الكشف

Perform Quantitative Risk Analysis Failure Modes Effects Analysis (FMEA)

شدة الخطر

احتمالية الحدوث

Potential Failure Mode and Effects Analysis (Design FMEA)

Item	Requirements	Potential Failure Mode	Potential Effect(s) of Failure	Severity	Potential Cause(s) / Mechanism(s) of Failure	Current Design Controls Prevention	Occurrence	Current Detection Design Controls		Detection	R.P.N.
								Cause	Failure Mode		
Name,	Requirements of function being analyzed	Manner in which system could fail:	Effects of failure as perceived by customers.		List every potential cause and/or failure mechanism:	List prevention activities		List Causes	List detection activities		0



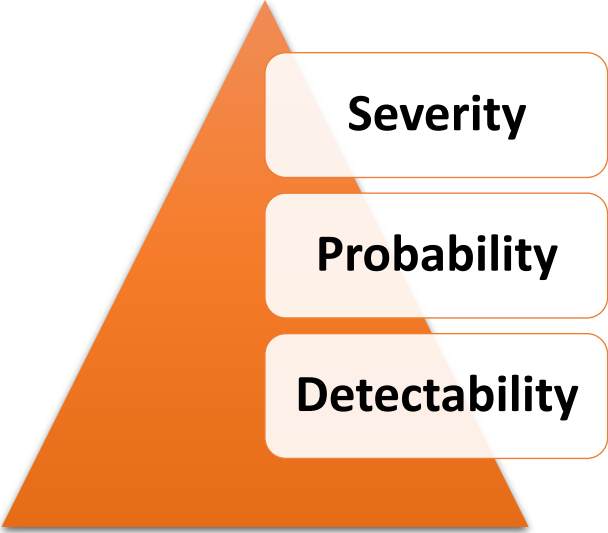
FMEA: Failure Modes Effects Analysis. The FMEA is useful for manufactured product or where risk may be undetectable:

Utilizes three measures :1) Severity, 2) Occurrence, 3) Detectability to produce the Risk Priority Number (RPN) : The higher the RPN, the greater the risk



Perform Quantitative Risk Analysis

A key aspect of the failure modes and effects analysis, or FMEA, is that it uses three measures to determine the **Risk Priority Number**:



Severity

Severity of the risk - represented on a numeric scale from 1 to 10, 1 representing no effect, to 10 representing a high hazard (unsafe without warning)

Probability

Probability of occurrence – 1 representing the current probability of less than .0007%, to 10 representing a probability of 20% (almost continuous failure) or greater

Detectability

Detectability of the risk – 1 representing a risk that is highly detectable, to 10 representing a risk that is completely undetectable (failure without warning)

Notes

The three numbers are multiplied together to produce the RPN (Risk Priority Number)



Perform Quantitative Risk Analysis

The three numbers are multiplied together to produce the RPN (Risk Priority Number)

This risk register type is particularly effective for manufactured products or for software products in which the software controls mechanical devices that could potentially cause serious injury or loss of life if the software (and therefore the device itself) were to fail.



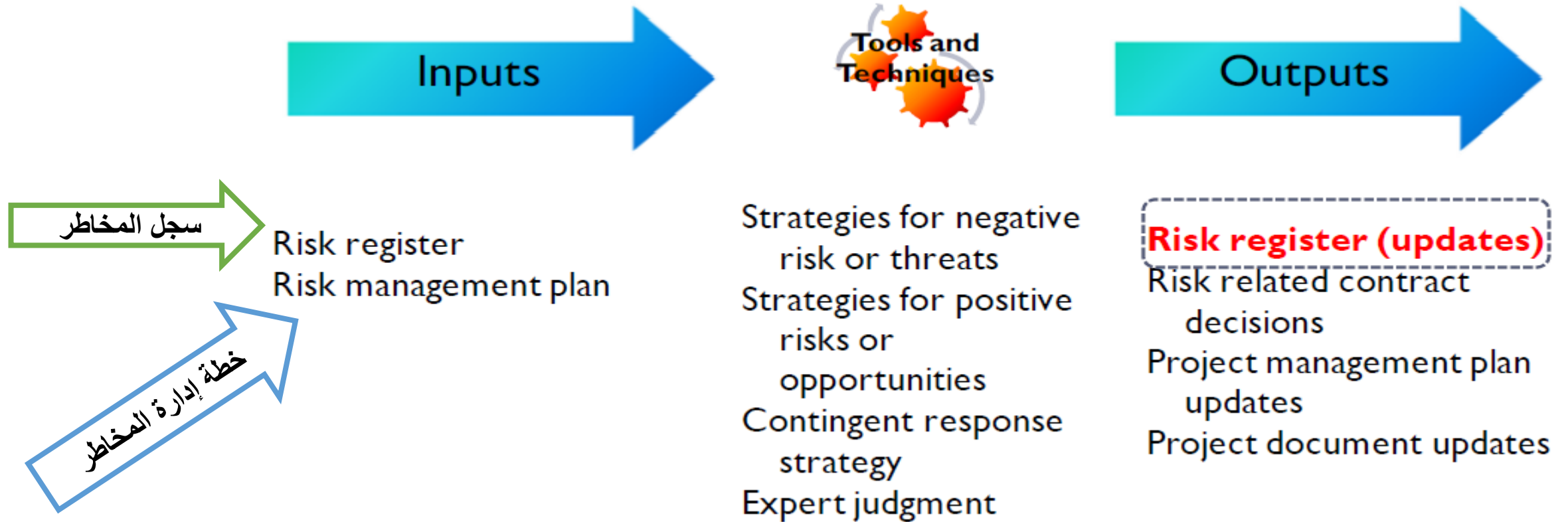
Expected Value/ Expected Monetary Value

Expected value or Expected Monetary Value (EMV) is computed by multiplying the probability of an event by its impact. Examples appear below:

المخاطره	Risk #	Probability	التأثير	Impact	القيمة المتوقعة	Expected value
	1	30%		-\$20,000		- \$6,000
	2	25%		28 Days		7 days
	3	11%		-\$95,000		-\$10,450
	4	40%		-\$38,000		-\$15,200
	5	20%		+\$40,000		+\$8,000



Plan Risk Responses



After risks are identified and evaluated from a qualitative and quantitative perspective, we can plan our responses to risk, and either to enhance opportunities, or reduce threats for the project.



Plan Risk Responses

There are a number of risk response strategies that can be employed on a project, however, all of the responses fall into the following basic categories:

- ☐ Implementing actions to prevent the risk from occurring
- ☐ Implementing actions in response to a risk occurrence
- ☐ Implementing actions to mitigate or reduce the risk occurrence
- ☐ Implementing actions to promote opportunities
- ☐ Implementing fallback or contingent responses, in the event risk response plans do not work



Examples of Risk Strategies – Negative Risks

Avoid Elimination of the potential threat. For example, you are dealing with a vendor and there is the threat of a potential major strike. Your avoidance strategy would be to switch vendors to an organization that does not have unions at all.



Transfer----- This involves shifting some or all of the negative impact of a threat, along with the ownership of the response, to a third party. Examples include purchasing insurance, performance bonds, warranties, or other forms of guarantee.



Mitigate_____ – this involves a reduction in the probability or impact of the risk. Designing fault tolerance into a system is a risk mitigation strategy. Instead of shouldering the full cost of the development of a new high risk product, you find three or four partners who can share the expense of development. In case of failure, your exposure to loss has been cut by 75-80%



Accept – Acceptance means that you cannot eliminate, transfer, or mitigate a threat, and there is no other suitable response strategy. You can actively or passively accept the threat:

- ❖ Passive acceptance means you take no action and deal with the risk if it occurs
- ❖ Active acceptance commonly means you have set aside contingency reserves to deal with any potential risk

Accept



Examples of Risk Strategies – Positive Risks

Exploit-----is used when the organization wants to ensure an opportunity is realized. Saving funds by using existing equipment or facilities is an exploit strategy



Examples of Risk Strategies – Positive Risks

Share_____ occurs when the organization transfers ownership of the opportunity, in part or altogether to a third party to ensure the opportunity occurs. Engaging a sub-contractor with specialized skill sets not available in your organization can help you capture an opportunity that may have been out of reach otherwise.



Examples of Risk Strategies – Positive Risks

Enhance___ – used to increase the impact or probability of an opportunity. Ending a project early by using highly experienced resources, or utilizing specific schedule compression techniques, is an enhancement opportunity.



Examples of Risk Strategies – Positive Risks

Accept – willing to take advantage of an opportunity without actively pursuing it.



shutterstock.com • 1253919295



Plan Risk Responses

Quick Quiz: Look at the next table and see if you can quickly identify what type of risk response strategy is being employed in each situation:

QUIZ!



Plan Risk Responses

Risk Description	Response Strategy?
There is a risk your lead architect may leave the project before her job is completed. As a result you cross-trained one of the developers to handle lead architect responsibility	mitigate
The database for your software project is expected to run into multiple terabytes. After consulting with the infrastructure team you discover there are terabytes of available storage in the data center that can be secured at a much lower cost than purchasing new equipment.	exploit
An out-of-state vendor on your project has expressed concerns about meeting delivery due dates. You engage a local vendor that can easily meet the delivery dates without issue.	Avoid
Staffing up for customer service on your project will take too long and be too expensive. You identify a vendor that will exceed your customer service requirements and will pay penalties if their service falls below stated quality levels.	transfer,



Risk Register Updates

The risk register is completed at this point and can include:

- ☐ Identified risks and descriptions
- ☐ Triggers
- ☐ Response strategy
- ☐ Specific actions taken if risk occurs

تحديد المخاطر
ووصفها

المحفزات

إستراتيجية
الإستجابة

إتخاذ إجراءات
محدده في حالة
حدوث مخاطر



Plan Risk Responses

The risk register is designed to be written to a level of detail that corresponds with the priority ranking of the risk and its associated response. Frequently, the lower level, low priority risks are placed on a 'watch list' for periodic review and monitoring.



Plan Risk Responses

Contingency Plans

Contingency plans are developed for a specific risk. Contingency plans are generally developed when you have accepted a risk and now have developed a plan 'B' or plan 'C' as a contingent response. These plans are executed only under predefined conditions, and when there is sufficient warning to implement the plan.

Fallback plans are implemented when a contingent response is not effective.



Residual and Secondary Risks

Residual risks are identified as risks that remain after a risk response strategy was implemented. It is possible that residual risks can be identified in the risk planning process, in which case they are subject to contingency and fallback planning.



Plan Risk Responses

- ❑ if you know that certain key personnel on the project might leave before the project is over, your risk response strategy may include required cross-training of other lower level resources.
 - ❖ There is a potential residual risk that even with cross-training, the lower level resources might not perform to the level expected. In this event, you may have identified a contingent or fallback plan to address the residual risk.



A secondary risk is a risk that results from implementing a risk response strategy. Secondary risks can be identified in the planning process, or they might occur as a result of discovery.



For example, you implemented a risk avoidance strategy by replacing an unreliable vendor with a highly dependable vendor on a project. However, unknown to you at the time, the dependable vendor was in negotiations to be bought out by a larger company. The secondary risk with the dependable vendor may include elements such as unexpected price changes, changes in resource availability, or a complete change in the business model.



- Plan Risk Management
- Identify Risks
- Perform Qualitative Risk Analysis
- Perform Quantitative Risk Analysis
- Plan Risk Responses
- Monitor and Control Risks

