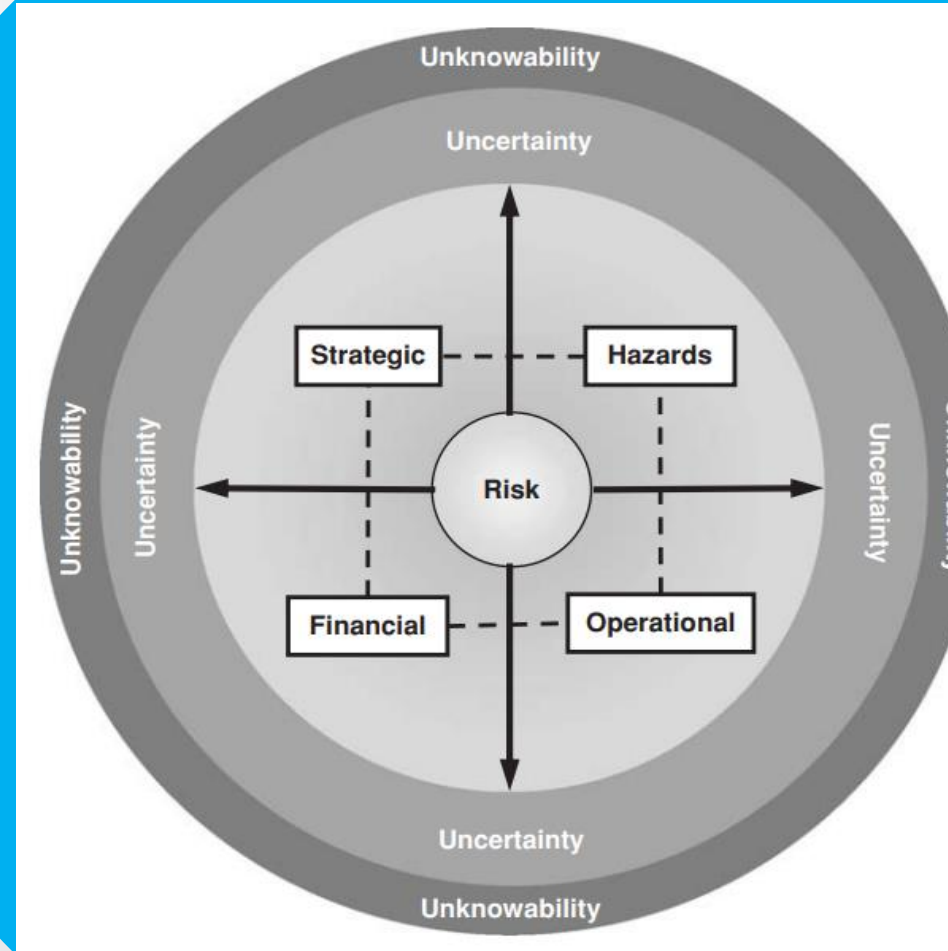


Strategic And Operational Risk Management

PMG630

Prepared by

Dr. Ayman Hassan



Lecture .9 “Risk Monitoring, Reporting, and Review”

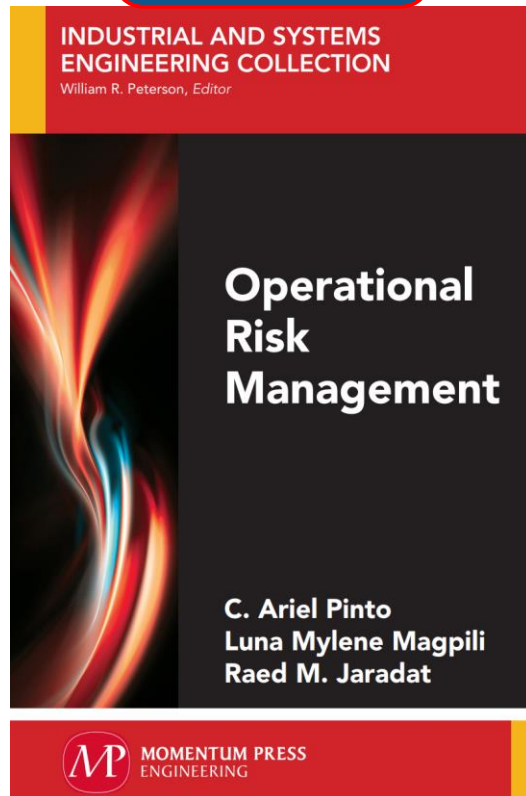
Chapter 5

Risk Monitoring, Reporting, and Review

Prepared by

Dr. Ayman Hassan

Chapter 5



REF, 1



REF,2

1. Summary of the previous lecture
2. Introduction
3. Risk response strategies " treatment "
4. General Risk Strategies
5. Risk Monitoring, Reporting, and Review
6. Risk Monitoring Objectives
7. Tracking : Risk Database
8. What Is A risk register?
9. Risk Review And Audit
10. Performance Mentoring
11. Summary
12. References & Resources

Previously,

we discussed the process of identifying risks, analysing their causes, and assessing their impact, and we discussed the four basic strategies for dealing with them, then we developed an action plan, and we identified who is responsible for approving and implementing it. In this section, it is important to discuss Risk Monitoring, Reporting, and Review

- Depending on the nature of a risk, project teams define an appropriate response strategy to it.
- ✓ There are four common risk response strategies:



- There are four general strategies for dealing with risk, depending on whether they are negative risks (threats) or positive risks (opportunities).
- Which strategy to use depends on two factors: the probability of the risk occurring and the impact that it would have on the project if it were to occur.
- For the sake of simplicity, let's categorize both the probability and impact of a risk into high and low categories.
- Then we have the following matrix for negative risks and positive risks

<u>Probability</u>	<u>Impact</u>	<u>Strategy</u>
L	L	<u>Accept</u>
H	H	<u>Avoid</u>
L	H	<u>Transfer</u>
H	L	<u>Mitigate</u>



Dr. Ayman Hassan

1- Accept

- As can be seen, if the risk is low in terms of probability and impact, you can simply accept it.
- Accepting a risk does not mean ignoring it: risks in these categories that are accepted are put in a watch list.
- During the course of the project, this watch list should be reviewed to see if the probability and/or impact of the risk has increased.
- It means , after analyzing all the variables, you'll inevitably decide to simply accept some risks. In certain cases, the potential impact may be so small that it's negligible.
- In other cases, the risk may be so low that it doesn't make sense to spend money trying to avoid or mitigate it.

- Whatever the case, make sure your executive sponsors sign off on any risk acceptance.
- You want to make sure they know you anticipated the risks and considered strategies for avoidance, transfer, or mitigation before going down the acceptance route.
- Airlines often overbook flights knowing that a certain number of people will cancel, but what if they don't, some of those flights will inevitably end up with too many passengers on board—at which point airlines start offering incentives (such as flight credits) to entice people off the plane.
- If that doesn't work, airlines are forced to kick some people off the flight. They know that this will create unhappy customers, but they accept the risk.

- Why do they accept the consequences? Airlines have done their math, and they know that in order to compete in a price-sensitive market, they need to fill their flights with as many passengers as possible.
- If they don't fill as many seats as possible, their profits will drop, and they won't be able to offer those low fares we all love. In short, they can't compete without overbooking, so they're willing to accept the occasional angry tweet in exchange for overbooked flights.

2- Avoiding

- Avoiding a risk means to completely eliminate it.
- Not all risks can be eliminated, and some can only be eliminated at great cost, so you'll want to analyze the costs and benefits of eliminating a given risk.
- Only then can you decide whether it's worth the time, money, and effort.
- On the opposite end of the scale, if the probability and impact are high, you should do all you can to avoid that risk.
- Some ways of avoiding risk are by clarifying requirements so that the potentially high-risk portions of the scope are excluded, or if the risk is to the schedule, by extending the schedule.

- An electronics manufacturer is set to go with a new, cheaper supplier for a key component of a product they sell.
 - There is no prior experience with the new supplier, so there is some concern that they may not deliver on time, potentially causing the company to lose money. This is a risk, and this risk can essentially be eliminated by going with the old (more expensive) supplier to meet the initial deadline, and reserving the cheaper supplier for future deadlines.
 - This is something the project team should discuss with their managers and/or executive sponsors, and weigh the level of risk they are willing to accept.
 - They may decide that going with the old supplier would destroy their profit margins because the new supplier is a retail giant that has negotiated very cheap prices.
 - So... you either accept the cost with the old supplier, and avoid the risk of going with a supplier you have never dealt with before, even though their prices are lower than the old supplier.
- ❖ What do you suggest?

3- Transfer

- Now, if the impact is high and the probability is low, you may want to transfer the risk to a third party.
- It means Transfer: These risk response strategies aim to transfer responsibility for a risk to a third party.
- This third party then bears the consequences of the risk occurring

- At the start of the Great Depression of the 1920s, Americans rushed the banks to withdraw their life savings because they knew their financial institutions were about to collapse., Since the banks didn't have any kind of risk transference in place, only a handful of their customers could withdraw their money before the banks ran out of capital.

- Today, all respected U.S. banks are members of the Federal Deposit Insurance Corporation (FDIC), which insures each account up to \$250,000. This transfer of risk allows customers to trust banks. In turn, that trust allows banks to earn people's business and prosper.
- The banks pay to be members of the FDIC. By doing so they transfer the risk of losing their clients' money to the FDIC, which is strong enough financially to avoid a repeat of 1929.
- If they didn't do that, nobody would trust banks and their entire business model would fail.

4- Mitigate

- A fourth strategy occurs when either the impact or the probability is high, and that is to mitigate the risk by lowering the probability of it occurring, or reducing the impact on the project if it occurs.
- The most common strategy for handling risk is to reduce that risk to an acceptable level. Since completely eliminating risk is often impossible or too costly, risk-mitigation is a key strategy for most project managers.

- Risk mitigation is pre-emptive.
- A great example of this is when an organization practices regular and proper maintenance of its equipment.
- This way, there's a smaller chance that their equipment breaks down.
- If the equipment breaks down for unavoidable reasons, regular maintenance can ensure that the damage isn't too bad.
- It also makes sure that the repairs won't be as costly compared to if the organization didn't practice regular maintenance.

- Risk mitigation is the process of understanding certain risks and threats, accepting that they exist, and taking the appropriate measures to reduce their effects in case they happen. It is a part of the risk management process and is necessary to prepare an organization for any threats to its operations and processes.
- Instead of eliminating threats, risk mitigation focuses on the unavoidable threats and reducing their impact.
- This can include natural disasters and other threats that may cause issues in production and other processes.
- These are threats that cannot be eliminated and are completely out of the company's control.
- Risk mitigation is there so that if these events occur, the company has the right measures to ensure that the damage the organization sustains is kept to the bare minimum.

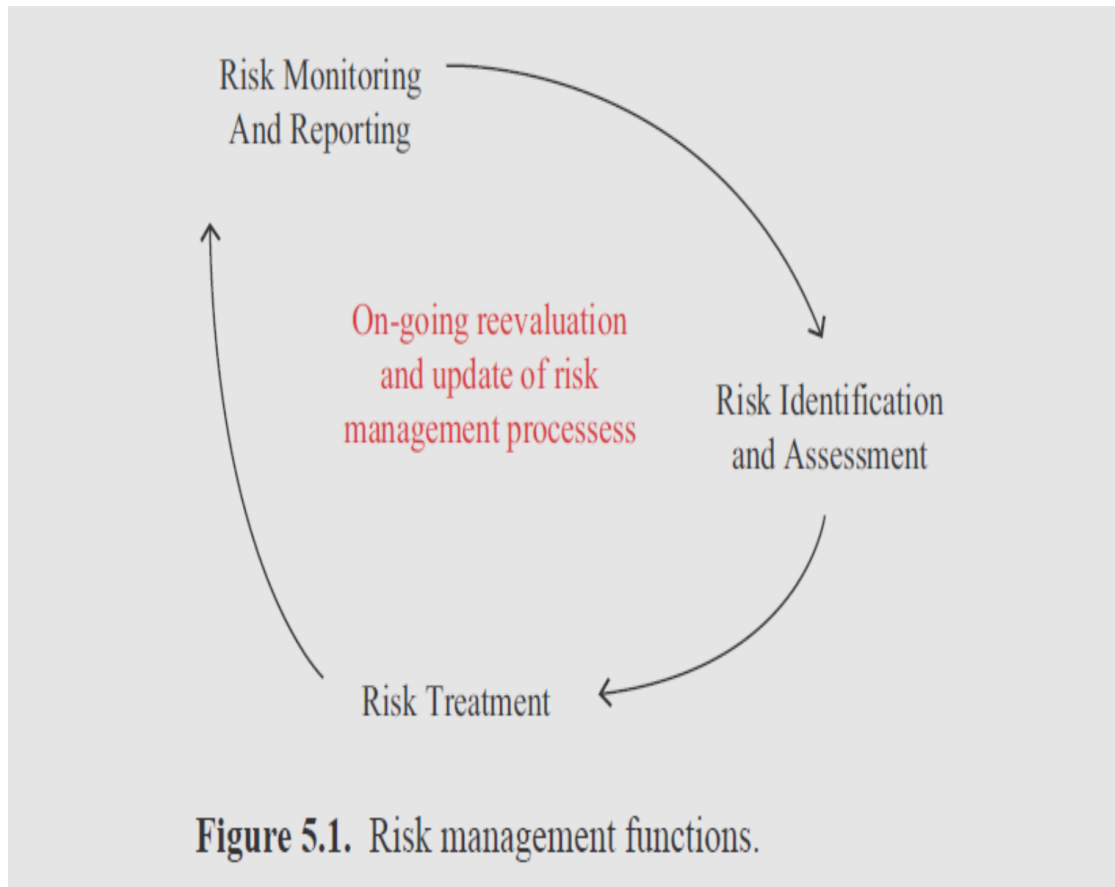
About techniques and tools**what is better qualitative or quantitative methods for risk analysis?**

- Whether you employ qualitative or quantitative methods for risk analysis, the analysis itself should consider two main factors: probability and impact.
- Probability is the likelihood of an event occurring; impact is the operational, reputational, or financial damage of that event to your organization.
- Together, these two elements will help you determine the severity of each potential risk so that you can develop strategies for each in accordance with your security posture and risk tolerance.

Risk Monitoring, Reporting, and Review

- After identifying and assessing risks and selecting response plans to address them, the next important function is to monitor, report and review risks, as shown in Figure 5.1.
- The purpose here is to monitor the implementation of risk response plans and procedures and to assess the effectiveness of current risk management processes.
- A key part of this function is to assess how current risk management plans and processes can be improved to respond to current and emerging environments.

• **Figure 5.1.**



- Determine whether identified operational risks (and their causal chain of events) are under control.
- This includes tracking identified risks and verifying that significant risks remain within acceptable risk levels.
- Evaluate the effectiveness of risk management, response plans, and procedures in addressing identified risks.
- This includes obtaining relevant information during the monitoring and review process to assess, control, and eliminate critical events.

- Evaluate the strength of risk controls over time as the system evolves.¹
- This also includes monitoring residual risks, identifying gaps and new risks, and eliminating invalid or outdated risks.
- Track evolving system needs and requirements.
- Remember that new needs and requirements often bring with them new risks that need to be controlled.

- Monitoring and management of risks is one of the main elements in the risk treatment and risk management process.
- There is no one specific methodology or process that can be applied to monitor operational risks in all systems.
- For example, monitoring operational risks in a bank is different from monitoring operational risks in a production system.
- For a reliable monitoring process, comprehensive treatment and assessment of risk events are necessary.
- It is essential to have a clear set of definitions of the operational risk under monitor.

- This includes identifying the appropriate risk indicators.
- The development of flexible methodology to accommodate any adjustment or changes in the system.
- It is naive to consider that the operation environment is always static, and therefore, operational risk can be controlled or avoided in the systems all at once.
- With increasing consumer demand and expectations resulting from advancing technologies, many systems are dealing with shifting dynamic environments.
- Therefore, it is necessary to adopt a flexible methodology to mitigate and control operational risk to the minimum.

- Full appreciation of the surrounding environments where systems operate.
- It is essential to understand the nature of the operations' environment.
- There are two types of environments: static and dynamic.
- In the static environment, the system is bounded apart from the environment, which means that there is no or minimal interaction between the system and the environment.
- In the dynamic environment, there is continuous interaction between the system and the environment.
- While it is relatively easy to monitor the operational risk in a static environment, it is a much more difficult task in a turbulent shifting environment.

- In general, the report should include the following parts.
- Description of the scope of the risk management plan
- Risk identification and assessment
- Risk treatment, response, and action plan
- The risk management plan is essentially a compilation of the broader system's risk profile or risk portfolio.

- Note that the report should cover the 6 + 1 questions
- It defines the scope of the risks being tracked and quantifies or measures the risks in terms of their estimated likelihood and impacts.
- It should further describe established acceptable risk level (i.e., As Low as Reasonably Practicable [ALARP] and detail the treatment response plans and actions for each identified risks.
- Included in the plan are the processes established for detecting, tracking, and documenting risks, as well as persons responsible for each risk response and actions.

- The forms discussed in Chapter 3 can be used to document the particulars of the risk management plan for each part, subsystem, or process.
- The report can also include the risk matrix discussed
- It offers a good overview and summary of the comparative risks.
- The summary of the risk management plan should include a list of risks requiring immediate response, a list of risks requiring response in the near term, a list of risks for additional analysis and response, and a watch list of low-priority risk.
- The report should also highlight any developments and trends from the risk data and risk assessment including an analysis of new and emerging risks.

The most common database compiled for risk is what is known as the risk register or risk log.

The database and information requirements are extracted from the risk management plan.

It often replicates or digitizes the tabular forms in Chapter 3. Though, more importantly, the risk register tracks the actual occurrences of the risk events.

Further, the risk register can document conditions leading up to the risk event, the response and actions taken, as well as the actual outcomes.

SIMPLE SAFETY RISK REGISTER TEMPLATE

RISK DESCRIPTION	IMPACT DESCRIPTION	IMPACT LEVEL	PROBABILITY LEVEL	PRIORITY LEVEL	MITIGATION NOTES	OWNER
Brief summary of the risk.	What will happen if the risk is not mitigated or eliminated?	Rate 1 (LOW) to 5 (HIGH)	Rate 1 (LOW) to 5 (HIGH)	(IMPACT X PROBABILITY) Address highest first.	What can be done to lower or eliminate the impact or probability.	Who's responsible?
Leads from roof during rain make the floor slippery	Slips and falls	3	5	15	- Order "slippery when wet" signs - Have mops on hand - Fix roof	Allen
Shortage of eye protection	Increase in injuries Production delayed Increased insurance premiums	5	1	5	- Increase supply - Low inventory warnings - Find alternative suppliers	Linda
		4	5	20		
		5	5	25		
		2	1	2		
		3	4	12		
		1	1	1		
		2	4	8		
		4	4	16		

PROBABILITY

5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5
	1	2	3	4	5

IMPACT

It is a document used as a risk management tool and to fulfill regulatory compliance acting as a repository for all risks identified and includes additional information about each risk, e.g., nature of the risk, reference and owner, mitigation measures. It can be displayed as a scatterplot or as a table.

[ISO](#) 73:2009 Risk management—Vocabulary defines a risk register to be a "record of information about identified risks".

A typical risk register contains:

- A risk category to group similar risks
- The risk breakdown structure identification number
- A brief description or name of the risk to make the risk easy to discuss
- The impact (or consequence) if event actually occurs rated on an integer scale
- The probability or likelihood of its occurrence rated on an integer scale
- The Risk Score (or Risk Rating) is the multiplication of Probability and Impact and is often used to rank the risks.

- Common mitigation steps (e.g. within IT projects) are Identify, Analyze, Plan Response, Monitor and Control.

The risk register is called "**qualitative**" if the probabilities are estimated by ranking them, as "high" to "low" impact. It is called "**quantitative**" both the impact and the probability is put into numbers, e.g. a risk might have a "\$1m" impact and a "50%" probability.

Contingent response - the actions to be taken should the risk event actually occur.

Contingency - the budget allocated to the contingent response

Trigger - an event that itself results in the risk event occurring (for example the risk event might be "flooding" and "heavy rainfall" the trigger)

The risk review examines both intended and documented results of the risk response and action plans in dealing with identified risks. Included in the risk review is an evaluation of the residual risk against established risk levels.

Residual risk assessment considers both the risks as previously identified and the resulting risk from the response mechanisms and the control activities implemented.

The process evaluates the effectiveness, cost, and efficiency of the activities and its adequacy in providing reasonable assurance that the likelihood and impacts of the risk events are brought down to the established acceptable risk level (i.e., ALARP).

- It is critical that the risk review evaluates the significant risks that fall outside of the acceptable risk levels.
- This may happen due to changing systems and policies or changing conditions and environments.
- These risks should be addressed with appropriate action plans to bring the risk within established levels. Risk treatment and response plans should be updated accordingly.

- An important oversight role in confirming that management is monitoring and managing all known risks in accordance with established levels can be done through a risk audit.
- When possible, the audit committee should consist of both internal and external members.
- A risk audit is a more comprehensive evaluation of the entire risk management system and processes.
- Thus it is conducted less often than risk reviews.

EFFECTIVE PERFORMANCE MONITORING To be effective, it is emphasized that the performance monitoring processes should be treated as an integrated component in the system.

There are two key elements in achieving an effective risk monitoring and review process.

First, clear communication channels between the members of the system increase the level of awareness with regards to the implementation of risk treatment and controls.

All stakeholders in the system must know specifically why particular risk controls or safeguards have been implemented.

Clear communication creates an environment where every member knows precisely his or her responsibilities toward addressing the risk.

Communication is important especially in large systems that have a high level of interaction, ambiguity, emergence, huge data collection, and complexity.

Second, it is necessary to establish a flexible monitoring process.

The design of risk monitoring procedures should be flexible so that they can adapt and respond in a cost-effective manner to threats arising from emergence, turbulent environments, uncertainty, and contextual issues of a dynamic nature.

Flexibility is the ability to add, adjust, or remove both physical components and functions. The level of flexibility should not cause the monitoring process to lose its identity; rather, it should provide an environment of trust where members of the system can share their proposed changes and strategies.

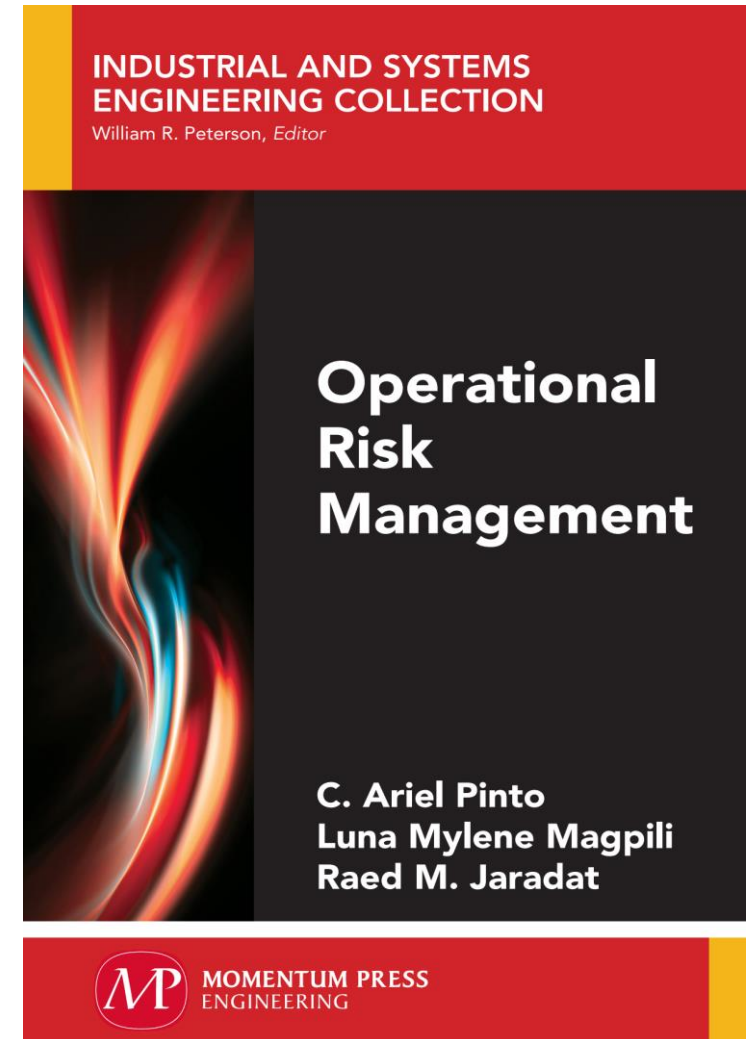
- ❖ Performance monitoring should be implemented to control and manage risks at established levels and to ensure the appropriateness and effectiveness of the risk treatment and response over time.
- ❖ These are done by using information from sources such as risk management plan and risk databases.

[5th Edition PMBOK® Guide—Chapter 11: Risk Strategies | 4squarereviews](#)

[4 Risk Response Strategies for Project Management Success | \(mrmcentral.com\)](#)

[What is Risk Mitigation & Why is it Important? | SafetyCulture](#)

❑ [Causal Chain - Tool/Concept/Definition \(thwink.org\)](#)





كل التوفيق لكم

My Best Wishes ...
* Dr. Ayman Hassan *

