

Project Risk Management

Prepared by Dr. Usama Al-Fendi

PMG 510
Project Risk Management

Lecture 2



Lecture Outlines

- Levels of risk
- Impact of risk on organizations
- Risk Reward Relationship
- Scope of risk management
- Bow Tie Model for Risk Analysis

Level of risk

- By taking a **proactive approach to risk and risk management**, organizations will be able to achieve the following **four areas of improvement**:
 1. **Strategy**
 2. **Tactics**
 3. **Operations**
 4. **Compliance**

Level of risk

- Strategy, because the risks associated with **different strategic options** will be fully analyzed and **better strategic decisions** will be reached.
- Strategic risk refers to the internal and external events that may make it difficult, or even impossible, for an organization to achieve their objectives and strategic goals. These risks can have severe consequences that impact organizations in the long term.

Level of risk

- Tactics, because consideration will have been given **to selection of the tactics** and the risks involved in the alternatives that may be available.
- Tactical risks is the chance of loss due to changes in business conditions on a real time basis. Tactics differ from strategy in that they handle real time conditions.

Level of risk

- Operations, because **events that can cause disruption** will be identified **in advance** and actions taken to reduce the likelihood of these events occurring, limit the damage caused by these events and contain the cost of the events.
- Operational risks is the inadequate or failed internal procedures, employee errors, cybersecurity events, or external events such as weather disasters.

Level of risk

Strategic Planning

- A high-level overview of the organization.
- Long term plan (typically 5 year)
- Forward looking

Tactical Planning

- Tactics used to achieve the strategy
- Short term plan (typically 1 year or less)
- Includes specific goals, budget, resources

Operational Planning

- Plan for day to day running of the organization
- Controlled via daily/weekly/monthly reports

Level of risk

- Compliance will be enhanced because the risks associated with failure to achieve compliance with statutory and customer obligations will be recognized
- Compliance risk is an organization's legal, financial and criminal exposure if it does not follow industry laws and regulations.

The goal of many regulations is to protect people and sensitive data.

Impact of risk on organizations

- **Stakeholders** now expect that organizations will take full account of the risks that may cause disruption within operations, late delivery of projects or failure to deliver strategy, incompliance with the adapted rules, regulations, and policies.

Impact of risk on organizations

Inherent risk vs residual risk

- **Inherent Risk** is typically defined as the level of risk in place in order to achieve an entity's objectives and before actions are taken to alter the risk's impact or likelihood (risk controlling techniques).

Impact of risk on organizations

Inherent risk vs residual risk

- **Residual Risk** is the remaining level of risk following the development and implementation of the entity's response (risk controlling techniques).

Lecture

2

Impact of risk on organizations



Impact of risk on organizations

- The risk level should be compared with the risk attitude or **risk appetite** or **risk tolerance** of the organization for the said risks of that type.
- Catastrophic and unacceptable level of risk for some organizations can be normal and acceptable level for other organizations.

Impact of risk on organizations

- **Risk appetite** is best described as the amount of different types of risk a firm is **willing** to accept to achieve its objectives.
- Organizations recognize that they cannot remove all risks from their business. Achieving our business goals requires accepting some of those risks while taking actions to mitigate, avoid or transfer other risks.
- Governing body who set risk appetite.

Impact of risk on organizations

- **Risk tolerance** is the amount of acceptable deviation from an organization's risk appetite.
- While risk appetite is a broad, strategic philosophy that guides an organization's risk management efforts, risk tolerance is a much more tactical concept that identifies the risk associated with a specific initiative and compares it to the organization's risk appetite.

Impact of risk on organizations

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.



Lecture

2

Impact of risk on organizations

Risk Appetite Example	Risk Tolerance Example
"We place patient safety as our top priority. We also recognize the need to balance the level of immediate response to all patient needs with the cost of providing such service."	"We plan our staffing to treat all patients within 5 minutes of their appointment time, and emergency walk-in patients within 15 minutes. However, management accepts that in rare situations (5% of the time) patients in need of non-life-threatening attention may not receive that attention for up to 4 hours."
Difference: Strategic, Aggregate, Qualitative This demonstrates a strategic philosophy for the organization about risk taking: low appetite for risk that might impact patient safety balanced with a higher appetite related to response to patient care and customer service.	Difference: Tactical, Specific, Quantitative This demonstrates the amount of variation in the parameters to be used to measure performance and assess fit within risk tolerance limits for a specific business process. Also, the risk tolerance is expressed in quantifiable terms.

Impact of risk on organizations

- **Risk attitude** indicates the long-term view of the organization to risk and risk appetite indicates the short-term willingness to take risk.
- This is similar to the difference between the long-term or established attitude of an individual towards the food they eat and their appetite for food at a particular moment in time.

Impact of risk on organizations

Example on inherent risk

- Lack of security software or device – Standardizing the employee's guidelines and creating password rules for how the employees should cater to their devices are quite examples of controls that can assist in securing the company software and hardware. If these controls are nonexistent or too lax, data breaches will likely happen.

Impact of risk on organizations

Example on residual risk

- Third-party cyber-attack – Such cyber-attacks usually happen when there is an external intent within the organization's company network to disable, disrupt or control the stored information. As the attacks are carried out by third parties, it is highly impossible to know if and when an attack is bound to happen. Even with proper controls and checks in order, this still remains a residual risk.

Risk Reward Relationship

It is impossible for organizations or projects to achieve their goals without taking any risk.

Zero risk means zero return, “No Pain – No Gain”

You can balance your position at the level that suits your risk appetite

Lecture

2

Risk Reward Relationship



Risk Reward Relationship

- In launching a new product, the organization will put resources at risk because it has decided that a certain amount of risk taking is appropriate.
- Penetrating new market through opening new branches is putting resources at risk intentionally, hoping this will generate profits later on.

Lecture

2

Risk Reward Relationship



Lecture

2

Risk Reward Relationship



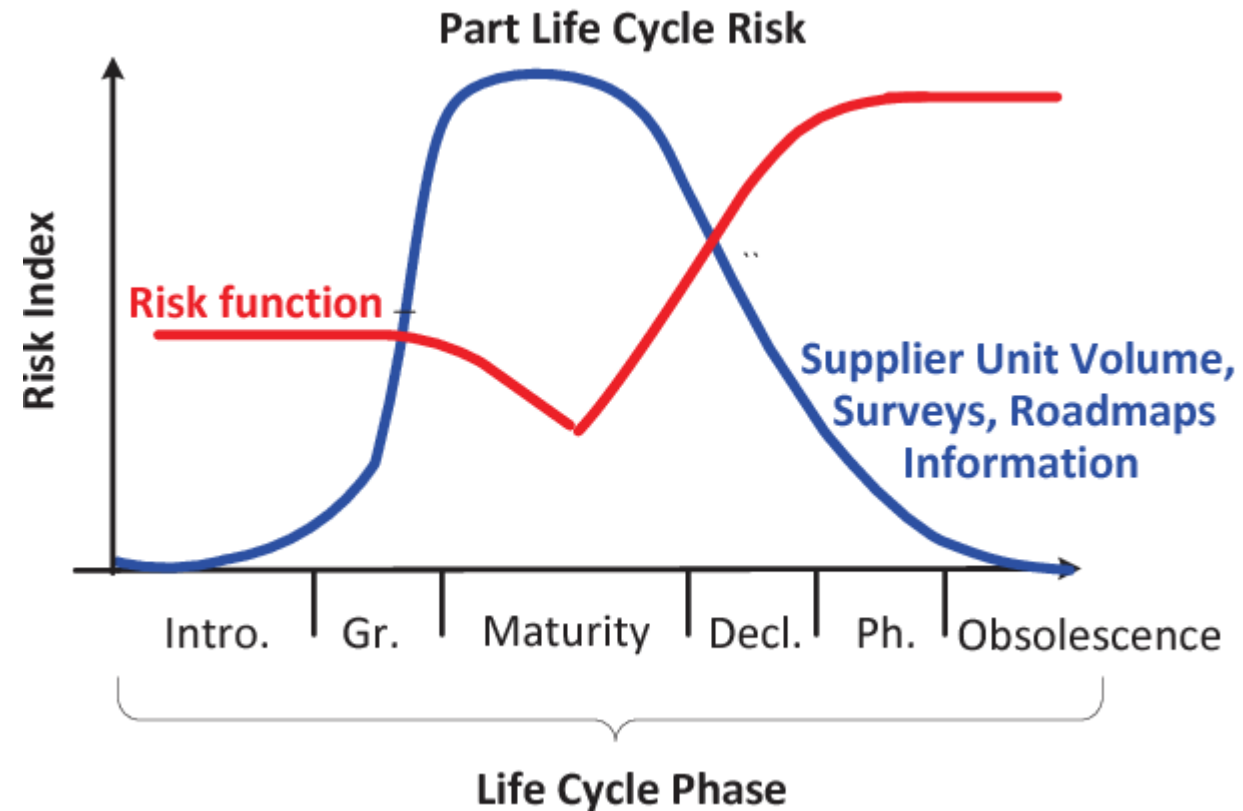
Risk Reward Relationship

- Investment process is nothing but putting the organization's assets and resources at risk in order to generate returns.

Risk Reward Relationship



Risk Reward Relationship



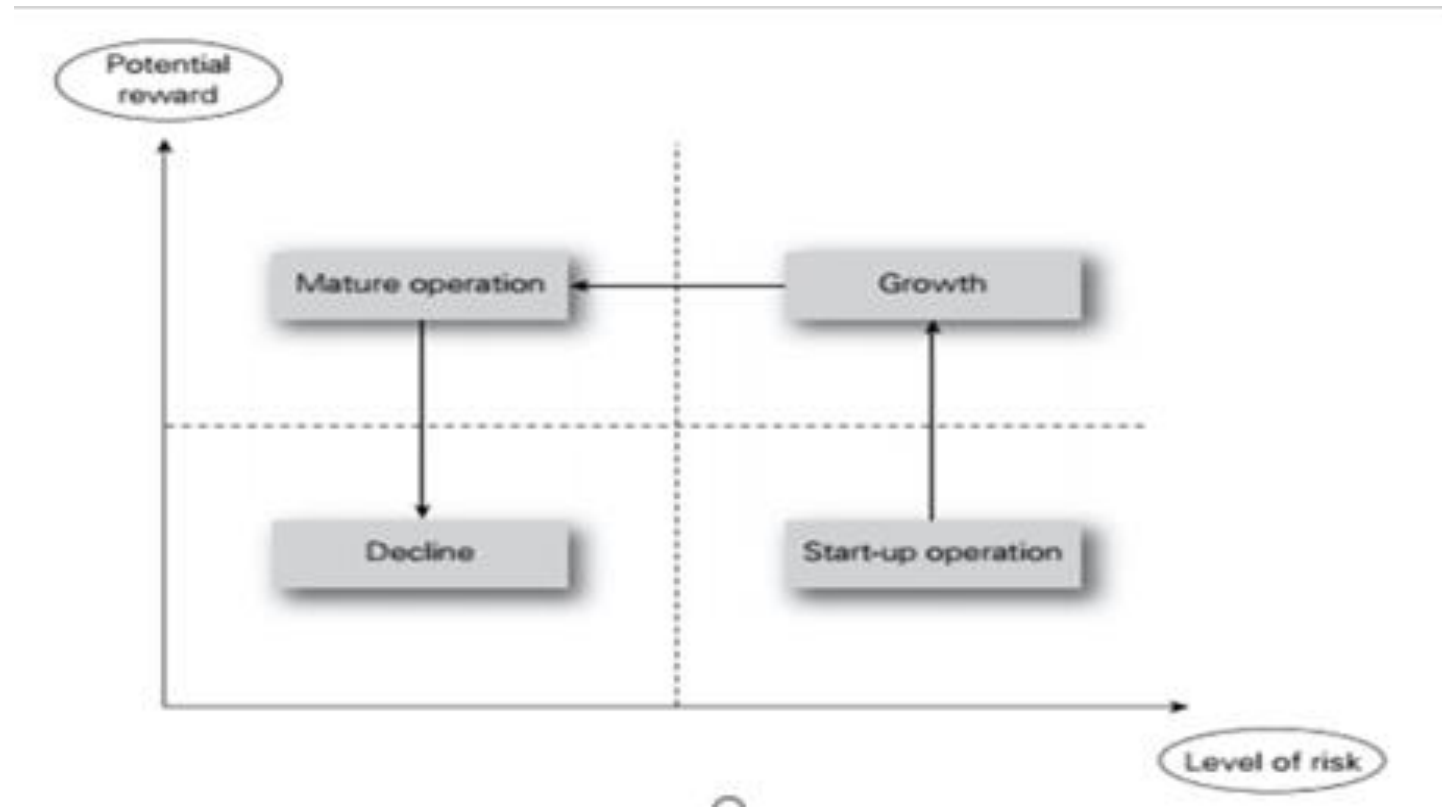
Risk Reward Relationship

- For an organization that is in the start-up phase, a **more aggressive** attitude to risk is required than for an organization that is enjoying growth or one that is a mature organization in a mature marketplace. Where an organization is operating in a mature marketplace and is suffering from decline, the attitude to risk will be much more risk averse.

Lecture

2

Risk Reward Relationship



Risk Reward Relationship

- Different organizations will have different attitudes to risk. Some organizations may be considered to be risk averse, whilst others will be risk aggressive.
- To some extent, the attitude of the organization to risk will depend on the sector and the nature and maturity of the marketplace within which it operates, as well as the attitude of the individual board members.

Risk Reward Relationship

Contribution of Risk Management on Decision Making

- However, the fact that the opportunity entails high risk may not have been fully considered. One of the major contributions from successful risk management is to ensure that strategic decisions that appear to be high risk are actually taken with all of the information available.

Risk Reward Relationship

Contribution of Risk Management on Decision Making

- Improvement in the robustness of decision-making activities is one of the key benefits of risk management. Attitude to risk is a complex subject and is closely related to the risk appetite of the organization, but they are not the same.

Risk Reward Relationship

- Other key factors that will determine the attitude of the organization to risk include the stage in the maturity cycle.
- It is because the attitude to risk has to be different when an organization is a startup operation rather than a mature organization, that it is often said that certain high-profile businessmen are very good at entrepreneurial start-up but are not as successful in running mature businesses.

Risk Reward Relationship

Risk and triggers:

- Risk is sometimes defined as uncertainty of outcomes. This is a somewhat technical, but nevertheless useful, definition and it is particularly applicable to the management of control risks.

Risk Reward Relationship

Risk and triggers:

- Control risks are the most difficult to identify and define, but are often associated with projects. The overall intention of a project is to deliver the desired outcomes on time, within budget and to specification, quality or performance.

Risk Reward Relationship

Risk and triggers:

- Given this uncertainty, these risks should be considered to be control risks and the overall management of the project should take account of the uncertainty associated with these different types of risk.

Bow tie analysis

Bow tie analysis

- Bow tie analysis is a simple process for identifying where new or enhanced controls may be worthwhile. It is a core part of risk treatment planning, particularly where there is a high level of risk or where control effectiveness is assessed as low.

Bow tie analysis

- The start of any bowtie is the 'hazard'. A hazard is something in, around or part of the organization which has the potential to cause damage. Driving a car or storing sensitive data are for instance hazardous aspects of an organization.
- The idea of a hazard is to find the things that are part of your organization and could have a negative impact if control over that aspect is lost. They should be formulated as normal aspects of the organization.

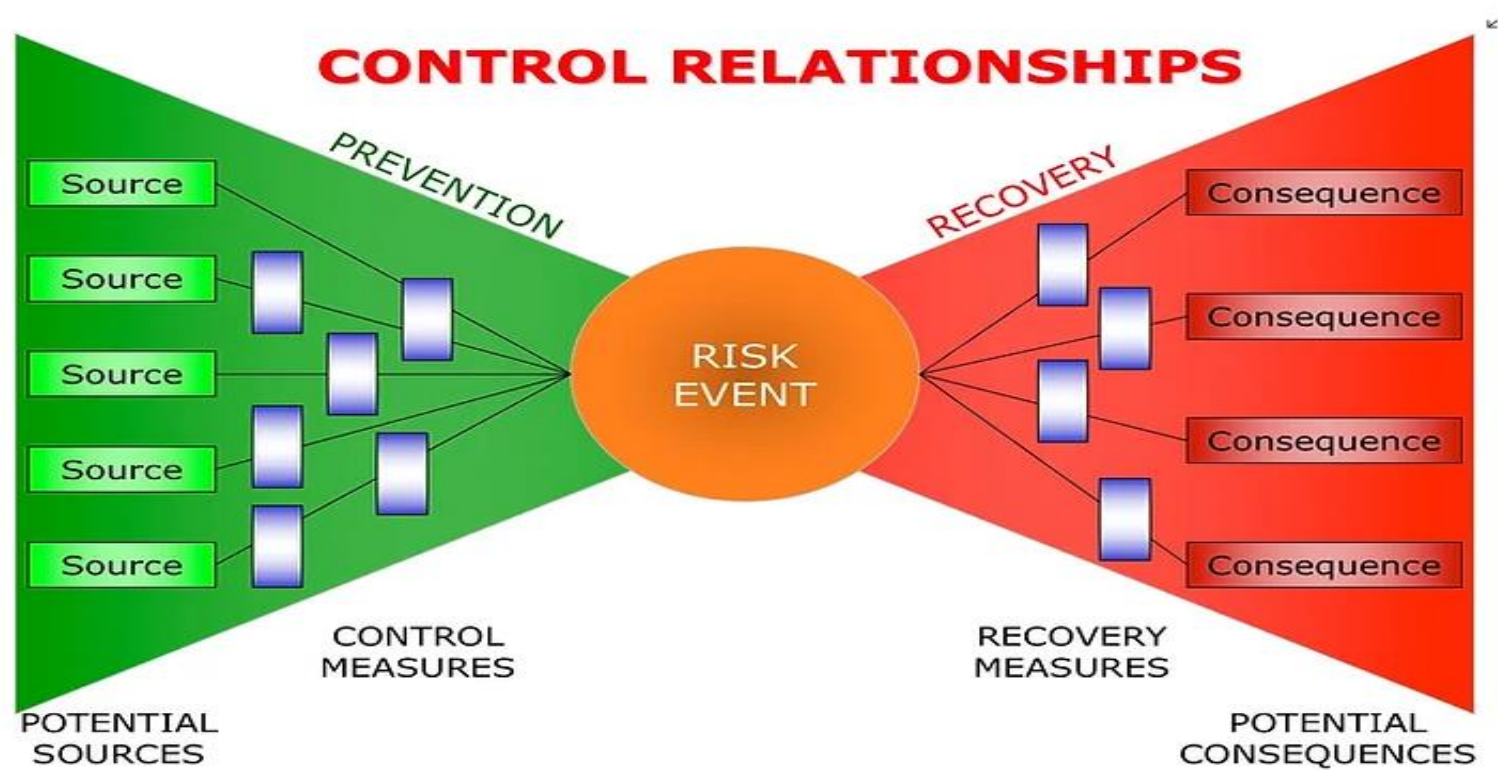
Bow tie analysis

- Once the hazard is chosen, the next step is to define the ‘top event. This is the moment when control is lost over the hazard. There is no damage or negative impact yet, but it is imminent. This means that the top event is chosen just before events start causing actual damage.

Bow tie analysis

- Consequences' are the result from the top event. There can be more than one consequence for every top event. events like 'car roll over', 'oil spill into sea' or 'toxic cloud forms'. Besides containing more specific information, this will help in more specific thinking when coming up with barriers. Think how you want to prevent 'environmental damage' versus 'oil spill into sea'. The second is an actual scenario which makes it much easier to come up with specific barriers

Bow tie analysis



Bow tie analysis

- The left-hand side of the bow-tie represents the source of a particular hazard and will indicate the classification system used by the organization for sources of risk.
- these sources of risk used are the high-level sources of strategic, tactical, operational and compliance (STOC) risks.

Bow tie analysis

- The right-hand side of the bow-tie sets out the impact should the risk events occur, we usually use the high-level components of financial, infrastructure, reputational and marketplace (FIRM) impact of a risk materializing.

Bow tie analysis

- In the center of the bow-tie is the risk event that indicates the categories of disruption that can affect organizations, and the same categories of people, premises, processes and products are used here.

Bow tie analysis

- The purpose of using the bow-tie illustration is to demonstrate the risk classification systems used by the organization and the potential range of impacts should a risk materialize.
- Controls (control techniques) can be put in place to prevent the event occurring and these can be represented by vertical lines on the left-hand side of the bow-tie.

Bow tie analysis

- The causes of the risk then need to be recorded along with the **preventive controls** to stop the risk occurring.
- The impact of the risk is also considered through **loss reduction techniques**. This enables the identification of response controls to lessen the impact of the risk should it occur

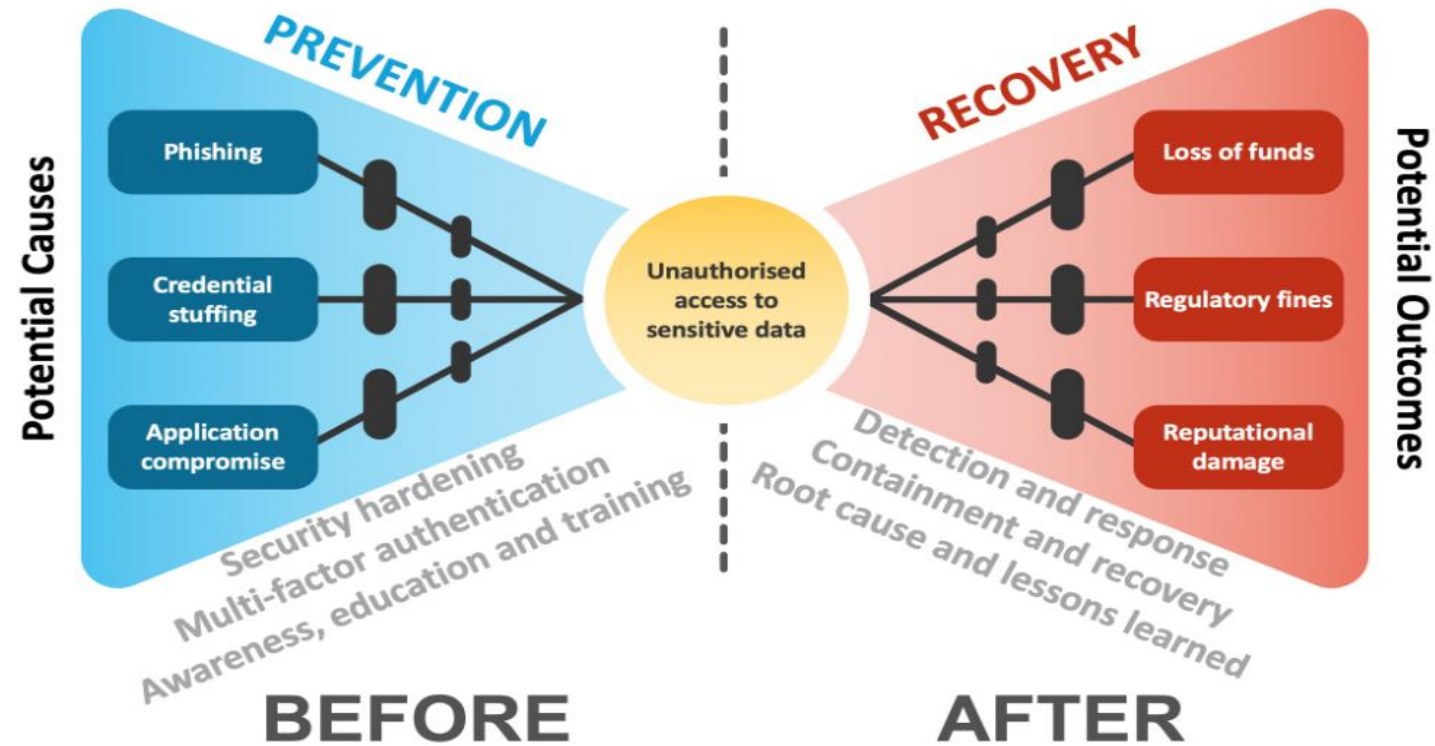
Bow tie analysis

- In a similar manner, recovery controls (Financing techniques or Transferring techniques) can be represented on the right-hand side of the bow-tie.
- The bow-tie representation of the risk management process can be used in many ways, including the representation of opportunity risks

Lecture

2

Bow tie analysis





Thank You