Week 7

Activity 1

1. **Discuss the different tools and techniques for identifying risks.**
   - Information gathering technique:
     - Brainstorming
     - The Delphi Technique
     - Interviewing
     - Root cause analysis
   - SWOT analysis
   - Diagramming techniques

     (Refer to video 2 – slide 23 to 28)

2. **What is risk appetite, risk tolerance and risk utility? Include an example in your explanation.**

   Risk appetite is the degree of uncertainty that an entity is willing to take on, in anticipation of a reward. For example, a risk-averse person will have a lower appetite for risk compared to a risk-seeker.

   Risk tolerance is how much risk an individual or organization can tolerate. It is the maximum acceptable deviation that an entity is willing to accept on the project or business objectives as the potential impact. For example, a project may be accepted if the risks are within tolerances and are in balance with the rewards that may be gained by taking the risks.

   Risk utility is the amount of satisfaction or pleasure received from a potential payoff. For example, utility rises at a decreasing rate for people who are risk-averse which means to say for a risk averse person, the amount of satisfaction diminishes as risk gets higher and the potential payoffs is of no interest to them

3. **Discuss the different responses to negative risks and provide an example for each.**

   Four main response strategies for negative risks (TARA)
   - Risk Transference
   - Risk Avoidance
   - Risk Mitigation (Reduction)
   - Risk Acceptance

   Risk transference is shifting the consequence of a risk and the responsibility for its management to a third party, either internal or external.

   Example 1: During the duration of a project, fluctuation in exchange rate may inflate the project cost. This can be transferred to a financial institution.
   Example 2: Selling a company's debt to another party at a lower price. The company receives less money but it is guaranteed.
   Example3: Purchase special insurance for specific hardware needed for a project. If hardware fails, insurer must replace.

   Risk avoidance is avoiding or eliminating a specific threat, usually by eliminating its causes or not taking that risk. For example, using a new and unfamiliar hardware may cause significant risk and so, the project team may decide to continue using the old equipment because the team knows it works instead of using the new equipment and thereby avoiding the risk.

Risk mitigation or reduction is reducing the impact of a risk event by reducing the probability of its occurrence. An example would be to have an experience project manager to handle the project and thus reducing the risk of the project failing.

Risk acceptance is when the project team decides to accept the risk and its consequences because the severity of the risk is lower than their risk tolerance. An example would be to accept the risk that an off-the-shelf software to be used in the project will be defective. If it’s not going to impact the project too much the project team might feel it’s unnecessary to allocate time and resources to address this risk.

4. Discuss the different responses to positive risks and provide an example for each.

Four main response strategies for positive risks:

- Risk **Exploitation**
- Risk **Sharing**
- Risk **Enhancement**
- Risk **Acceptance**

(Look at Schwalbe text – Page 468 (7e) for explanation and example)

Activity 2

Risks may vary, but could include (see sample risk register solution):

- Security concerns over personal data
- Simplicity of new system for all users
- Integration of the current system to the old system
- Uncertainty over fees and charges of scanner/purchasing ability
- Resistance to change by users
- Low adoption rate from customers and low customer satisfaction (triggers could be poor training and marketing)
- Increased customisation costs
- Uncooperative team members
- Under-utilised team members
- Scanners may not be reliable
- Insufficient stock of hardware (scanner). Root cause could be poor planning (due to the bank's fault) or late delivery by vendor (external cause).
- Transactional security
- Technical security
- Insufficient resources allocated
- Insufficient team member technical skills