**Collaborative Learning Discussion 2: The Effect of Risk on the SDLC**

Read Roy et al (2015) and Hijazi et al (2014) ( See unit 4 reading) and then answer the questions below.

* As an **individual**, list on the discussion forum what you believe to be the top 5 overall causes of risks, as highlighted by the articles cited.
* **Outside of the Discussion Forum**, discuss these with your team – can you compile an overall agreed list of the five most important causes?
* Then go on to **individually** produce a list of 5 possible mitigations for these causes – you may find that Ross et al (2016) (the NIST SP 800-160v1 guide) a useful aid in creating this.
* **Outside of the Discussion Forum**, discuss the mitigations with your team – can you agree on the best mitigation for each major cause?

1. Incorrect resources estimation Roy et al (2015)

Inadequate estimation of project time, cost, scope and other resources. Hijazi et al (2014)

Estimate the likelihood of occurrence and consequences of each identified security risk

3. Ambiguous requirements Roy et al (2015)

Unclear Project Scope and Requirements, Miscommunication Hijazi et al (2014)

Having Proof of concept and UAT environment for user to look and feel

4. Improper design risk Roy et al (2015)

Incomplete Design Document Hijazi et al (2014)

Document the service request by user and commit by user

• Supplier/vendor problems Roy et al (2015)

Apply supplier relationship management, priority alignment and commit on the SLA

Impossible complete testing (Coverage Problem) Hijazi et al (2014)

Limiting on the components and feature, having automation testing for every release

https://www.redhat.com/en/topics/devops/what-cicd-pipeline

Roy et al (2015)

P.121

Risks for software project management have been classified as Known risk, Unknown risk, Predictable risk, Unpredictable risk [ 3 ]. Another approach used in [ 6 ] identifies risks as Technical risk, Management risk, Financial risk, Contractual and legal risk, and Personal risk. On the other hand in [ 7 ], it was observed that risks are identified as Business risk, Commercial risk, Economical risk, Project risk, Product risk.

P.129

As for example, if a risk of conflicting requirements is left unidentified at the requirement specification level as no conflict identification technique (mechanism) has been applied at that level, the risk will naturally be carried forward and in worst case it might been slipped as undetected and carried up to implementation. The risk, when occurred might not only cause some serious business loss, identification, and mitigation of the problem would also be very cumbersome and extremely difficult.

On the other hand, if appropriate mechanism be applied at every stages of SDLC, it not only will identify and arrest a lot of risks to propagate further and cause serious damages, maintenance overhead will also be minimized and more robust software can be offered to the users.

1. Incorrect resources estimation

2. User/customer uncertainty

3. Ambiguous requirements

4. Improper design risk

5. Development system and risk with development system

6. Inadequate management process

7. Improper work environment

• Lack of strategic framework or conflict over strategy

• Lack of adaptation to technological change

• Supplier/vendor problems

• Poor management of change

• Too much faith in ability of the technology to fix the problems (User expectation)

Hijazi et al (2014)

Inadequate estimation of project time, cost, scope and other resources.

Unclear Project Scope and Requirements, Miscommunication

Incomplete Design Document

Large size components, complex system

Impossible complete testing (Coverage Problem)