Initial Post

After reading Roy et al (2015), Hijazi et al (2014) and Ross et al (2016) journal, I believe that these are the top 5 overall causes of risks and mitigation methods.

1. Inadequate estimation of resources

Both journals have mentioned the inaccurate project time, budget, scale, and other resources estimation.

In the risk management process of the project planning, the risks could be recognised, the likelihood of occurrence and repercussions estimated, measuring each risk relative to its thresholds. Define risk treatment strategies and measures with each risk that exceeds its limit to mitigate the risk occurrence (Ross et al, 2016).

2. Ambiguous Project Scope and Requirements

Roy and Hijazi journals have similar risk factors regarding the stakeholder requirements and project scope.

Prepare and analyse stakeholder needs and transform the needs into requirements definition. Having consent on the definitions with the stakeholder and developing the aspects of operational and other life cycle concepts (Ross et al, 2016). Record all the requirements and definitions in the document. Moreover, providing a Proof-of-Concept (PoC) environment for users to look at and feel if possible.

3. Improper design risk

Both journals draw out the incorrect design risk which does not match the stakeholder requirements and some of the risk factors might cause by the complex system.

Consider the various kinds of design features and have the stakeholder articulate and commit to the service requirement. Identify, plan for, and get availability to enabling systems or methods that will satisfy the design definition process (Ross et al, 2016). In addition, having refinement meetings with stakeholders in different statuses to verify the needs.

4. Supplier or vendor problems

In nowadays business practice, outsourcing could be common in the project. Regarding Roy et al (2015) journals, choosing supplier or vendor considerations could be a risk for the project.

With the participation of stakeholders, create criteria for choosing a provider. Acceptance is provided to the product or service provider that complies with the terms of the agreement (Ross et al, 2016). Commitment to the priority alignment and Service Level Agreement (SLA), the acquirer requirements outlined in the agreement have been met.

5. Impossible to cover all test cases

With reference to Hijazi et al (2014), due to the many possible interactions, testing might not be able to cover all the combinations and sequences. Some scenarios might even require regression testing for frequent version changes.

The system could divide or limited the number of components and features to separate the test case. Implementing Continuous integration / continuous delivery (CI/CD) software to perform automation testing like smoke testing and sanity testing for version changes (Red Hat, 2019).

References:

Hijazi, H. et al (2014) Risk Factors In Software Development Phases. *European Scientific Journal*. Available from: https://doi.org/10.19044/esj.2014.v10n3p%25p [Accessed 4 April 2022]

Red Hat. (2019) What is a CI/CD pipeline?. *Understanding DevOps*. Available from: https://www.redhat.com/en/topics/devops/what-cicd-pipeline [Accessed 4 April 2022]

Ross, R. et al (2016) Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems. *NIST Special Publication 800-160 VOLUME 1*. Available from: https://doi.org/10.6028/NIST.SP.800-160v1 [Accessed 4 April 2022]

Roy, B. et al (2015) A Study on Software Risk Management Strategies and Mapping with SDLC. *Advanced Computing and Systems for Security.* Available from: http://dx.doi.org/10.1007/978-81-322-2653-6\_9 [Accessed 4 April 2022]