## what to do in case of a change in requirements of the project

including the impacts, risks and steps needed to mitigate the risks

Impacts:

1. System Downtime: Modifications to an ICT system often require scheduled downtime, limiting user access during the transition period.

2. Performance Issues: Changes can result in unexpected performance degradation if not thoroughly tested and optimized beforehand.

3. Data Integrity: The transition may compromise data integrity, risking loss or corruption of critical information.

4. User Adaptation: Significant changes may necessitate users to adapt to new interfaces or processes, potentially leading to productivity disruptions.

Risks:

1. Security Vulnerabilities: New system changes might introduce security vulnerabilities, exposing the system to potential breaches and data breaches.

2. Operational Disruption: Poorly integrated changes can disrupt critical business operations, causing productivity losses and revenue impacts.

3. Cost Overruns: Unforeseen issues stemming from changes can lead to increased troubleshooting and resolution costs, exceeding the allocated budget.

4. Compliance Issues: Updates may inadvertently result in non-compliance with regulatory standards, inviting legal consequences and reputational damage.

Steps to Mitigate the Risks:

1. Thorough Planning: Develop a comprehensive plan encompassing all aspects of the transition, from implementation to post-deployment monitoring.

2. Impact Analysis: Conduct a thorough impact analysis to gauge the potential effects of the changes on stakeholders and operational processes.

3. \*\*Testing:\*\* Execute rigorous testing in a controlled environment to identify and address issues before full deployment, ensuring system stability.

4. \*\*Stakeholder Communication:\*\* Maintain transparent communication with all stakeholders throughout the transition process to manage expectations and address concerns promptly.

5. \*\*Backup Procedures:\*\* Establish robust backup procedures to safeguard against data loss and facilitate restoration to previous states if necessary.

6. \*\*Security Audits:\*\* Perform post-implementation security audits to identify and rectify any vulnerabilities or weaknesses in the system.

7. \*\*Training Programs:\*\* Implement training programs to facilitate smooth user transitions, minimizing operational disruptions and ensuring effective utilization of the new system.

8. \*\*Continuous Monitoring:\*\* Continuously monitor the system post-implementation for performance and security issues, enabling timely intervention and optimization efforts.