# Risk Management Checklist for an Internal IT Project for SMEs

## 1. Project Planning and Scope

- Clearly define the project scope, objectives, and deliverables.
- Identify all stakeholders and their roles.
- Develop a detailed project plan with timelines, milestones, and resource allocation.
- Obtain stakeholder approval and commitment to the project plan.

## 2. Risk Identification

- Conduct a risk assessment workshop with key stakeholders and team members.
- Create a risk register to document potential risks, their causes, and their impacts.
- Categorize risks (e.g., technical, operational, financial, legal, and external).

## 3. Risk Analysis

- Evaluate the likelihood and impact of each identified risk.
- Prioritize risks based on their potential impact on the project.
- Use qualitative and quantitative analysis methods where applicable.

## 4. Risk Mitigation Strategies

- Develop risk mitigation plans for high-priority risks.
- Assign risk owners responsible for managing specific risks.
- Plan for risk avoidance, reduction, transfer, or acceptance strategies.
- Establish contingency plans for critical risks, including rollback.

## 5. Resource Management

- Ensure the project team has the necessary skills and resources.
- Plan for adequate training and support for team members.
- Monitor resource allocation to avoid overloading team members.

## 6. Communication Plan

- Develop a communication plan to keep stakeholders informed about project progress and risks.
- Schedule regular meetings and updates to discuss risk status.
- Ensure transparency in reporting and documentation.

## 7. Technical Considerations

- Assess the technical feasibility of the project.
- Evaluate technology options and their potential risks.
- Plan for system integration and compatibility issues.
- Ensure data security and privacy measures are in place.

## 8. Vendor and Third-Party Management

- Identify and evaluate potential vendors and third-party partners.
- Review and assess vendor contracts and service level agreements (SLAs).
- Monitor vendor performance and manage dependencies.

**9. Change Management**

- Establish a change management process to handle project changes.
- Assess the impact of changes on project scope, schedule, and budget.
- Obtain stakeholder approval for significant changes.

**10. Testing and Quality Assurance**

- Develop a comprehensive testing plan, including unit, integration, and user acceptance testing.
- Identify potential defects and plan for their resolution.
- Ensure quality standards and best practices are followed throughout the project.

**11. Monitoring and Review**

- Implement a risk monitoring system to track and review risks continuously.
- Schedule regular risk review meetings with the project team.
- Update the risk register and mitigation plans as needed.

**12. Documentation and Reporting**

- Maintain thorough documentation of all risk management activities.
- Prepare regular risk management reports for stakeholders.
- Archive project documentation for future reference and lessons learned.

**13. Post-Implementation Review**

- Conduct a post-implementation review to assess project outcomes and risk management effectiveness.
- Document lessons learned and best practices for future projects.
- Ensure ongoing monitoring and support for the implemented IT solution.



www.antonyjnewman.com
tony@antonyjnewman.com