***Appendix 2:*** *Risks and Risk Description*

The list of risks listed below is developed based on the review of several sources and materials. Therefore, the senior management must review the list and other risk groups like Enterprise Risk Management, Internal Controls, Internal Audit and Information Security.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Risk Category | | Ref # | Risk Description | Receptor | Potential Impact and Consequence |
| ERP Implementation and Organisation Related Risk | | R1 | Inadequate enterprise resources for governance and oversight (e.g., Board, Audit Committee, Legal Counsel, Enterprise Risk Management) | Operational, Financial, Reputational | Legal and governance issues, specifically vendor management and contacts |
| R2 | Customisation and modification result in ongoing maintenance challenges | Operational, Financial | Unable to onboard standard applications or modules due to customisation |
| R3 | Inability to integrate with existing systems can lead to data exchange and data duplication issues | Operational, Financial | Inefficient operation |
| R4 | Resistance to change or accept the system and process change leads to cost overruns | Operational, Financial, Employee Morale | Low employee morale and productivity |
| Project Management Related Risks | | R5 | Significant costs related to project management resources: IT personnel, specialists related project management | Financial | Cost overrun due to project management costs |
| R6 | Costly initial investments: Servers, databases, cloud services, and other supporting systems | Financial | Cost overrun due to high initial investments |
| R7 | Expensive ongoing management: Training, support, maintenance and change management | Financial | Cost overrun due to ongoing management |
| R8 | Significant time required for project implementation: Requirements gathering to user training | Operational, Financial | Delayed implementation |
| R9 | Poor quality: Functionalities, user-friendly interfaces, and ability to use with minimal configurations | Operational, Financial, Reputational | Unable to meet the business or user requirements |
| SDLC  Related  Risks | **System Analysis and Requirements** | R10 | Inadequate system analysis and requirements: Threat/vulnerability analysis, assets identification & rating and existing controls | Operational, Financial | Incomplete requirements;  Inadequate risk identification |
| R11 | Insufficient documentation with necessary details | Operational, Financial | Poor or incomplete system design |
| **System Design** | R12 | Poor and incorrect selection of architecture approach, design approach, programming languages and methodologies | Operational, Financial | Inefficient development |
| R13 | Incomplete design documents with insufficient detail | Operational, Financial | Poor or incomplete development |
| **Development** | R14 | Incomplete designs | Operational, Financial | Incomplete solution |
| R15 | Insufficient expertise in development/programming | Operational, Financial | Poor solution with missing requirements |
| R16 | Inadequate documentation to support the code | Operational, Financial | Incomplete testing |
| R17 | Incomplete unit tests which do not reflect the requirements | Operational, Financial | Solution with missing requirements |
| R18 | Technical errors or omissions | Operational, Financial | Poor solution with missing requirements |
| R19 | The rapid pace of technological change can create challenges | Operational, Financial | Outdated and obsolete solution |
| **Testing** | R20 | Incompatible components | Operational, Financial | incomplete test results |
| R21 | Missing functionality | Operational, Financial | Solution with missing requirements |
| R22 | Inadequate documentation with new requirements based on the testing | Operational, Financial | Poor installation and UAT testing |
| **Installation and UAT** | R23 | User issues may not be identified promptly | Operational, Financial | Solution with missing requirements |
| R24 | Environmental incompatibilities | Operational, Financial | Incomplete UAT and implementation |
| R25 | UAT failure or fail to meet user requirements | Operational, Financial | Solution with missing requirements |
| **Ops and Maintenance** | R26 | Inadequate training | Operational, Financial, Employee Morale | Poor performance; Low employee morale |
| R27 | Insufficient resources to support the solution | Operational, Financial, Employee Morale | Poor performance |
| R28 | Lack of maintenance and updates: Patching, Upgrading and Vulnerability Management | Operational, Financial, Employee Morale | Outdated and obsolete solution |
| Security and Availability | | R29 | Coordinate cyber-attacks using various attack vectors such as external, internal, and supply chain | Operational, Financial, Reputational, Employee Morale | Employee and business data leakage;  Legal and regulatory issues |
| R30 | The solution may not be available due to human error or natural disaster | Operational, Financial, Reputational, Employee Morale | Solution not available; Poor performance |