Appendix 1 – Risk Register

The risk register focuses on technical, business, cyber, and economic risks associated with the project, with each risk scored for probability and impact.

Risk	Description	Mitigations	Probability	Impact
Compliance and Regulatory Risks	Failure to meet legislative compliance or regulatory requirements.	Thoroughly review relevant regulations and compliance requirements specific to industry and geography. Ensure that any suppliers are assessed on their ability meet and to adapt to emergent statutory and regulatory requirements. Ensure across project board that new software and the acquisition of software adheres to necessary standards and regulations.	3	5
Time Overrun	Risk of the project not being procured and delivered in time for meeting the expiration of the current contract	To work with the project board consisting of teams across the Council and consultants to make sure that each stage of work is delivered to schedule and budget and that risks are mitigated for. To draft mitigations for each phase in case of project slippage.	3	4
Risk of legal challenge to the contract award	Risk of an unsuccessful bidder issuing a legal challenge, leading to substantial delays in contract award and project	Make sure the procurement is run in accordance with legal requirements by working in collaboration with the Council’s procurement and legal teams.	2	4
Budget Overruns	Risk of the project exceeding the budget due to unforeseen challenges or extended timelines.	Clearly define the scope and requirements of the migration project to prevent scope creep. To identify all capital and revenue costs during procurement, including support. Regularly review and adjust the budget as needed based on actual expenditures and project progress.	3	4

Risk	Description	Mitigations	Probability	Impact
Inadequate In-house resource limitations	Lack of sufficient knowledge within in- house IT team and planning department to manage and troubleshoot technical migration issues effectively.	Work with consultants at TerraQuest, internal teams and suppliers to bridge the knowledge gap during procurement and the initial phases of the migration. Work with project board to build resilience within teams to support the use of the new system.	4	4
Dependency on Single Vendor	Over-reliance on a single supplier, potentially leading to challenges in vendor management or negotiation leverage.	Evaluate the risks associated with vendor lock-in and consider strategies for maintaining flexibility. To draft thorough ITT and contract to ensure that all business needs can be met with supplier and adequate supplier support is built into contract. To assess the market as part of open tender process to ensure that the vendor continues to meet our needs in terms of cost (value for money), capabilities, and service levels.	3	3
Cyber Security and Data Protection Vulnerabilities	Potential security vulnerabilities during and after migration, including data breaches or loss.	Conduct a thorough DPIA and security assessment during procurement stage and prior to migration. Regularly update and patch systems to protect against vulnerabilities.	3	5
Business Continuity During and Following Migration	Risk of significant downtime or disruption to business operations during the migration process.	ICT to help identify scope and technical requirements of migration to help develop a data migration strategy. Develop a comprehensive business continuity plan that includes fallback and rollback procedures. Ensure that backups are in place and evaluated before beginning migration activities to minimize downtime and maintain operations.	3	5

Risk	Description	Mitigations	Probability	Impact
Technical Complexity of Migration	Challenges in migrating complex business systems with multiple interfaces, particularly one large application never migrated to cloud before.	Consider implementing a phased migration approach. Begin with less critical workloads to gain familiarity with the process. Work with ICT to understand dependencies and complexities beforehand.	4	5
Post-adoption technical support	Difficulties in managing and maintaining updates to the system following procurement and implementation of the information management system.	Set out in tender documents and contract provisions for system support and module customisation from the supplier. Identify and resource in-house champions and training from the supplier where available to build in-house resilience in maintaining the database system.	3	4
Data Loss or Corruption	Risk of losing critical data or experiencing data corruption during the migration process.	Implement robust data backup and recovery strategies. Ensure data integrity by conducting pre-migration data assessments and post-migration data validation. Utilize data replication and backup services for additional protection where possible.	2	5

Risk	Description	Mitigations	Probability	Impact
Best 'go-live' window for implementation and testing	Will need to consider the best go-live window for a new system, for example launching the software all at once with a single transition, or if it would be more convenient to phase-in implementation of the system to minimise operational disruption.	Once a supplier has been decided, and the work streams required to set up the new system is identified, the project board will evaluate the benefits and risks of both a phased and big bang approach to go-live to minimise operational disruption. Adequate resource and time is required to be planned for user testing across different service areas.	3	3
User Adoption and Training	Potential resistance or slow adoption of the new cloud environment by end-users due to lack of training or awareness.	Develop a comprehensive training and change management program to support users. Offer various training formats (e.g., workshops, online courses, documentation) tailored to different roles within the organization. Engage users early in the migration process to gather feedback and adjust training materials accordingly.	3	3

Probability Scale (Likelihood)

1. Rare: The risk is unlikely to occur.
2. Unlikely: The risk may occur only in exceptional circumstances.
3. Possible: The risk might occur at some time.
4. Likely: The risk is likely to occur at some time.
5. Almost Certain: The risk is expected to occur in most circumstances.

Impact Scale (Severity)

1. Negligible: The impact is minimal and can be easily managed or absorbed.
2. Minor: The impact causes some disruption but can be managed with minimal efforts.
3. Moderate: The impact causes noticeable disruption and requires management attention.
4. Major: The impact causes considerable disruption and may require significant resources to manage.
5. Catastrophic: The impact causes extreme disruption and can be beyond the current means to manage.

This page is intentionally left blank