Findings identified during OAG Audit - Shire of Nungarin

#	Audit Finding	Response and Action Steps	Actions	Shire of Nungarin Recommendations
1	**Procurement Practices**	- Reinforce procurement policies and practices among staff. - Emphasize timely creation and approval of purchase orders. - Ensure batch payment listings are appropriately signed.	Staff training on procurement policies and practices. Ensure adherence to approval processes for purchase orders and batch payments.	Conduct regular training sessions on procurement policies and practices. Implement an automated system for purchase orders and batch payment approvals.
2	**Excessive Superuser Access**	- Conduct a comprehensive access review based on "need-to-know." - Adjust superuser privileges to minimize unauthorized access.	Perform an immediate access review. Modify superuser privileges based on job requirements.	Establish a periodic access review schedule. Implement a role-based access control system to restrict privileges based on job roles and responsibilities.
3	**Supplier Masterfile Amendments**	- Ensure completion and signing of New/Change of Supplier Details Forms. - Implement regular reviews of forms and audit trail reports.	Implement a process for timely completion and signing of supplier forms. Conduct regular reviews of supplier master files and audit trail reports.	Develop a checklist for supplier amendments and require sign-offs for each step. Implement an automated system for tracking and reviewing supplier master file changes.
4	**Fair Value of Assets - Frequency of Valuations**	- Comply with the updated FM Regulations for fair value assessments. - Ensure a robust fair value assessment is conducted as per regulations.	Develop and execute a plan for fair value assessments in alignment with the updated FM Regulations.	Establish a timeline for regular fair value assessments. Engage external experts for periodic assessments to ensure compliance and accuracy.
5	**Payroll Practices**	- Implement measures for mandatory timesheet approvals. - Enhance record-keeping for terminations. - Introduce senior management review of payroll reports.	Implement a system for mandatory timesheet approvals. Improve record-keeping for terminations. Introduce senior management review of payroll reports.	Introduce an automated timesheet approval system. Implement an electronic record-keeping system for terminations. Conduct regular training for senior management on reviewing payroll reports.
6	**Bank Reconciliations**	- Ensure all bank reconciliations are performed within one month for accuracy.	Establish a process for timely bank reconciliations within one month.	Develop a monthly reconciliation calendar with specific deadlines. Utilize automated reconciliation tools to streamline the process and reduce manual effort.
7	**Risk Management Policy**	- Establish a comprehensive risk management policy. - Maintain an up-to-date risk register.	Develop a detailed risk management policy and ensure the risk register is regularly updated.	Establish a dedicated team responsible for continuous monitoring and updating of the risk register. Conduct regular risk assessment workshops to ensure comprehensive coverage.
8	**Asset Management Plan**	- Develop, review, and update an Asset Management Plan annually.	Formulate and maintain an Asset Management Plan, with regular reviews and updates.	Engage with asset management experts to develop a comprehensive plan. Implement a system for continuous monitoring and updating of asset-related data.
9	**Lack of IT Governance**	- Develop and implement IT policies, a strategic plan, and procedures.	Establish and enforce IT policies, strategic plan, and procedures for consistent governance.	Collaborate with IT experts to create comprehensive policies aligned with industry best practices. Conduct regular training for IT staff on governance procedures and protocols.
10	**No Business Continuity Plan and Disaster Recovery Plan**	- Establish comprehensive Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP) strategies.	Develop and implement a detailed BCP and DRP to address potential disruptions and catastrophic events.	Conduct regular drills and simulations to test the effectiveness of the BCP and DRP. Collaborate with external experts to ensure the plans align with industry standards.
11	**Lack of IT Risk Register and Periodic Meetings for Managing Cybersecurity Risks**	- Develop and maintain an IT risk register. - Conduct regular cybersecurity risk management meetings.	Create and update an IT risk register. Schedule periodic meetings for managing cybersecurity risks.	Collaborate with cybersecurity experts to identify and document potential IT risks. Establish a clear framework for ongoing risk assessments and mitigation strategies.
12	**No Change Management Process in Place**	- Establish a formal change management process to minimize disruptions.	Develop and implement a structured change management process to control IT system changes.	Engage with change management experts to create a customized process aligned with organizational needs. Establish clear communication channels for change notifications and approvals.
13	**No Service Level Agreement with IT Service Provider**	- Develop IT-related policies, SLAs, and performance management practices with the Managed Service Provider.	Create IT policies, SLAs, and performance management practices aligned with the MSP agreement.	Collaborate with the MSP to create customized SLAs. Establish clear performance metrics and reporting mechanisms. Conduct regular reviews and updates to ensure alignment with organizational goals.
14	**Absence of IT and Security Related Training**	- Implement regular IT and security training programs for all staff members.	Initiate regular training programs covering IT and security topics for all staff members.	Collaborate with training providers to create a comprehensive curriculum. Implement regular assessments to measure the effectiveness of training programs. Ensure continuous updates to address emerging threats.