Attachment 6.1B

SHIRE OF MERREDIN

PERIOD OF AUDIT: YEAR ENDING 30 JUNE 2023

FINDINGS IDENTIFIED DURING THE FINAL AUDIT

Index of findings	**Potential impact on audit opinion**	**Rating**			**Prior year finding**
		Significant	**Moderate**	**Minor**	
Information system					
1. IT Governance, Policies and Procedures	No		✓		
2. Disaster Recovery Plan Testing	No		✓		
3. Network Access Management	No		✓		
4. Lack of Cybersecurity Training	No		✓		

Key to ratings
The Ratings in this management letter are based on the audit team's assessment of risks and concerns with respect to the probability and/or consequence of adverse outcomes if action is not taken. We give consideration to these potential adverse outcomes in the context of both quantitative impact (for example financial loss) and qualitative impact (for example inefficiency, non-compliance, poor service to the public or loss of public confidence).

Significant - Those findings where there is potentially a significant risk to the entity should the finding not be addressed by the entity promptly. A significant rating could indicate the need for a modified audit opinion in the current year, or in a subsequent reporting period if not addressed. However even if the issue is not likely to impact the audit opinion, it should be addressed promptly.

Moderate - Those findings which are of sufficient concern to warrant action being taken by the entity as soon as practicable.

Minor - Those findings that are not of primary concern but still warrant action being taken.

SHIRE OF MERREDIN

PERIOD OF AUDIT: YEAR ENDING 30 JUNE 2023

FINDINGS IDENTIFIED DURING THE FINAL AUDIT

1. IT Governance, Policies and Procedures

IT policies and procedures
The Shire does not have comprehensive IT and cyber security policies and procedures, which cover various aspects such as access control, physical security, backup protocols, change management, HR security, information classification, and data loss prevention.

IT Strategic Plan
The Shire does not have a structured IT strategic plan to align IT initiatives with the overall business objectives.

Procedure manuals and permission matrices
The Shire does not have procedure manuals and permission matrices for the accounting systems, including payroll. In addition, the Shire does not have logical access control policies, which cover user authentication, authorisation, account management, account requests and approvals, monitoring, and auditing.

Rating: Moderate

Implication
Without comprehensive IT and cyber security policies and procedures to provide guidance to staff, there is a risk that the Shire is exposed to various cyber security risks, which could lead to data breaches or unauthorised access.

Without an appropriately approved IT Strategic Plan, there is a risk that IT resources will not be aligned to the business strategy and priorities.

Without proper procedure manuals, permission matrices, and logical access control policies, there is a risk of security vulnerabilities and compliance issues.

Recommendation
We recommend that management:

- develop and implement comprehensive IT and cyber security policies, which cover access control, physical security, backup protocols, change management, HR security, information classification, and data loss prevention

- establish a structured IT Strategic Plan that aligns technology initiatives with Shire's overall business objectives

- develop procedure manuals, access control policies and permission matrices for the finance and payroll systems, and implement logical access control policies to strengthen security and compliance measures.

Management comment

Action 1: Corporate IT Strategy	*Develop a Corporate IT Strategy for the Shire of Merredin that links to the business objectives outlined in the Shire of Merredin Corporate Business Plan.* **Responsible person:** Executive Manager Corporate Services

SHIRE OF MERREDIN

PERIOD OF AUDIT: YEAR ENDING 30 JUNE 2023

FINDINGS IDENTIFIED DURING THE FINAL AUDIT

	Completion date: 30/09/2024
Action 2: IT Policies/ procedures	*Though a range of processes are currently in place in relation to backups, physical security, HR security and a number of the other areas listed below, the Shire will formalise/ develop documented IT and Cyber Security policies/ procedures that include:* - *Access control (including Account management, Account requests and approvals, Account monitoring, User authentication, Account auditing)* - *Physical security* - *Backup protocols* - *Change management* - *HR security* - *Information classification* - *Data loss prevention* **Responsible person:** Executive Manager Corporate Services **Completion date:** 30/09/2024
Action 3: IT Policies/ procedures	*Review policies created above and determine if further policies are required, or any amendments need to be made.* **Responsible person:** Executive Manager Corporate Services **Completion date:** 31/12/2024
Action 4: Procedures	*Formalise/ develop a series of procedure documents/ work instructions to support the policies referred to in Action 2.* **Responsible person:** Executive Manager Corporate Services **Completion date:** 31/12/2024
Action 5: Permission Matrices	*Completed - Permission matrices are in place for the new payroll system. Staff in the Finance team who complete payroll for the Shire have administrative access and use two-factor identification to access the system. The Executive Manager Corporate Services is the overseer of this system and approves access levels. Employees only have access to enter timesheets and leave requests and check accruals and balances. They are unable to change data within the system. This has been implemented since 1 July 2023.* **Responsible person:** Executive Manager Corporate Services **Completion date:** 01/07/2023
Action 6: Permission Matrices	*A review of user access of the Shire's accounting system has occurred to ensure appropriate access for staff. During the review, all staff access to the Shire's IT system was checked to ensure accuracy.* *Moving forward these reviews will be scheduled quarterly to ensure that security is maintained with the first review to take place prior to 31 January 2024.* **Responsible person:** Executive Manager Corporate Services **Completion date:** 31/01/2024
Action 7: Permission Matrices	*A permission matrix document will be developed that outlines permissions to be assigned to each position in the organisations, as per the organisation structure, to guide future reviews.* **Responsible person:** Executive Manager Corporate Services **Completion date:** 31/01/2024

SHIRE OF MERREDIN

PERIOD OF AUDIT: YEAR ENDING 30 JUNE 2023

FINDINGS IDENTIFIED DURING THE FINAL AUDIT

2. Disaster Recovery Plan Testing

Disaster recovery
Testing of the Disaster Recovery Plan (DRP) is overdue.

Rating: Moderate

Implication
Without adequate testing of the DRP, there is a risk that the DRP in place may not be effective and sufficient enough in ensuring that key IT systems are able to be recovered after a major incident. This could result in prolonged downtime and significant financial losses in a disaster or critical system failure.

Recommendation
We recommend that the IT DRP is adequately tested on regular basis, and these tests should be used to confirm key IT systems and services can be restored or recovered within the required timeframes.

Management comment

Action 1:	*Desktop testing of the Disaster Recovery Plan will be completed by the Executive Management Team.* **Responsible person:** Executive Management Team **Completion date:** 31/03/2024
Action 2:	*A review of the Disaster Recovery Plan will occur once desktop testing has been completed to identify any amendments that may need to be made.* **Responsible person:** Executive Management Team **Completion date:** 30/06/2024

SHIRE OF MERREDIN

PERIOD OF AUDIT: YEAR ENDING 30 JUNE 2023

FINDINGS IDENTIFIED DURING THE FINAL AUDIT

3. Network Access Management

Password policies
The Shire's password policy is inadequate as the minimum password length in the Shire's Active Directory is set at only six characters, which falls short of best practice recommendations. Additionally, the account lockout threshold is set to zero, which created a risk of password guessing, leaving the system vulnerable to brute-force attacks.

Privileged accounts
There was no regular review of privileged accounts in SynergySoft. The Shire has six administrative users.

Rating: Moderate

Implication
Without adequate password policies, there is an increased risk of unauthorised access into the systems, which could lead to data breaches or system compromises.

Without regular reviews of privileged accounts, there is an increased security risks as well as potential misuse of administrative privileges.

Recommendation
We recommend that management:

- implement stronger password policies, and a reasonable account lockout threshold to mitigate the risk of password-related security breaches
- perform regular reviews of privileged accounts to ensure the administrative users continue to align with the business requirements.

Management comment

Action 1: Password Policies	*Completed - All password settings in the IT system have been updated to reflect best practice recommendations. These include minimum 10 characters for passwords. This change was made when the Shire were alerted to the issue in September, however a further review on 10.11.2023 confirmed these are currently in place.* *The password lockout threshold has been set to three attempts. This was completed when the Shire were alerted to the issue in September, however a further review on 10.11.2023 confirmed this is currently in place.* **Responsible person:** Executive Manager Corporate Services **Completion date:** 10/11/2023
Action 2: Privileged Accounts	*Completed - Removal of IT service providers administration status occurred during the Audit visit in September when attention was drawn to the issue.* *A full audit of IT system users was completed at this time and the system presently reflects all current staff accurately.*

SHIRE OF MERREDIN

PERIOD OF AUDIT: YEAR ENDING 30 JUNE 2023

FINDINGS IDENTIFIED DURING THE FINAL AUDIT

	Responsible person: Executive Manager Corporate Services **Completion date:** 22/09/2023
Action 3: Privileged Accounts	*A procedure will be developed to ensure the IT system user review process is completed regularly (at least four times per year), as well as included in onboarding and offboarding processes moving forward.* **Responsible person:** Executive Manager Corporate Services **Completion date:** 31/03/2024
Action 4: Privileged Accounts	*Quarterly review dates will be added to the Shire's compliance system to ensure staff are alerted when reviews are due.* **Responsible person:** Executive Manager Corporate Services **Completion date:** 31/12/2023

SHIRE OF MERREDIN

PERIOD OF AUDIT: YEAR ENDING 30 JUNE 2023

FINDINGS IDENTIFIED DURING THE FINAL AUDIT

4. Lack of Cyber Security Training

We noted that the Shire's employees have not received any cyber security related training.

Rating: Moderate

Implication
There is a risk of staff falling victim to social engineering attacks and other security breaches due to a lack of awareness and preparedness.

Recommendation
We recommend that management ensure all staff are provided with ongoing cyber security awareness training to raise their awareness of cyber threats.

Management comment

Action 1:	*The Shire have completed testing over the previous 12 months to identify areas of risk by utilising phishing campaigns with staff and Councillors. It is recognised that further training is required and available training options for staff will be investigated.* **Responsible person:** Executive Manager Corporate Services **Completion date:** 31/03/2024
Action 2:	*Develop a training schedule to ensure all staff with network access are exposed to cyber security training at least annually.* **Responsible person:** Executive Manager Corporate Services **Completion date:** 31/01/2024
Action 3:	*Implement training, with initial roll-out to be completed by 30 June 2024.* **Responsible person:** Executive Manager Corporate Services **Completion date:** 30/06/2024