All correspondence to be addressed to:
Chief Executive Officer
PO Box 125 KULIN WA 6365
p: 08 9880 1204 f: 08 9880 1221
e: enquiries@kulin.wa.gov.au
www.kulin.wa.gov.au

Report on Significant Findings from 2023/24 Final Audit

The following items were identified as significant during the 2023/24 Final Audit conducted by AMD Chartered Accountants and the Office of Auditor General.

1. Risk Management Policy

Significant Finding
Our enquiries indicated that the Shire of Kulin has no formal risk management policy in place, documenting assessed risks and risk management procedures. The absence of a risk management policy and associated procedures increases the risk of strategic and operational risks being insufficiently understood or not identified by Shire Management and Council. Additionally, risk levels may unknowingly exceed the Council's appetite.

Recommendation
We recommend that a risk management policy be prepared as a priority, updated and subsequently reviewed on a regular basis.

Management Comment
A risk management policy will be developed when the Executive Manager of Governance & Risk returns from parental leave in October 2024.

2. Cybersecurity Plan

Significant Finding
Our enquiry relating to cybersecurity of the Shire of Kulin identified that the Shire currently does not have any documented cybersecurity policies in place, nor is there a documented cybersecurity response plan in place. Without documented cybersecurity policies and procedures outlining the controls regarding cybersecurity, there is an increased risk of vulnerability to cyber-attacks such as malware or phishing attempts. Furthermore, without an appropriate plan in place, the Shire may not be sufficiently prepared to act in the event of a cybersecurity threat or staff may not be aware of processes that should be followed. This may lead to the Shire's system being compromised, impacts on service delivery, unauthorised access to sensitive information, and potentially financial loss to the Shire.

Recommendation
We recommend a documented cybersecurity policy be developed and communicated to all staff and the Shire also develop a cybersecurity plan, including (but not limited to) addressing the following key areas;

- Risk assessment of the Shire's IT security control environment;
- Identification of safeguards and protections in place; and
- Action plan in the event of a cybersecurity event, including outlining the roles and responsibilities of staff during such an event.

Management Comment
The Shire implemented a Disaster Recovery Plan in April 2024. This covers all IT & cyber disasters that may occur. When the Plan is reviewed in April 2025 we will include more specific information regarding potential cyber-attacks.