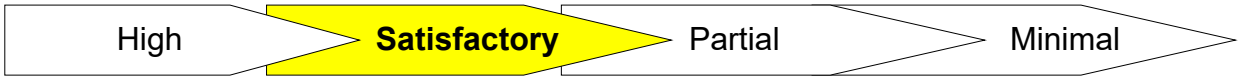
Appendix 2a: Audit Opinion and Themes

Assurance



Cyber Security Incident Management

Objective

To assess the effectiveness of arrangements in place to quickly identify a Cyber Security incident and the suitability of planned strategic and technical responses following an attack.

Themes

In this audit we reviewed the cyber incident management processes and policies in place; design of incident response plans to promptly contain and respond to incidents; follow up procedures from a cyber incident; incident response accountabilities, responsibilities and delegation; governance around incident response management; and alignment with crisis management plans.

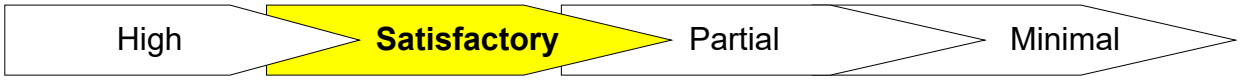
We identified appropriate controls in many areas particularly the understanding of information and cyber security threats to its operations, supported by suitable Government and other partnerships for cyber threat information sharing; tools in place to capture and analyse IT Security events; the documentation of employees roles and responsibilities in response to cyber incidents; communication and escalation plans; consistent reporting criteria and containment strategies.

Despite the fact that the Council has established key incident management controls in place to combat cyber attacks, it is crucial to note that the maturity of cyber security controls is likely to deteriorate over time if no additional activities are performed on a continuous basis, due to the constant changes in the threat landscape.

We identified six recommendations, none of which represent high risk findings:

- The Council should address the key person dependency risk by ensuring that an operational procedure should be documented based on potential cyber threat scenarios (DDoS, phishing attack, ransomware attack etc.) to account for the circumstances where any key personnel involved were to suddenly leave or be out of office at the time of an incident
- The Council should devise and undertaken table-top exercises on a quarterly basis and document observations from the exercises to ensure the processes defined are appropriate and the team involved is comfortable with their parts to play
- The Council should establish formal reporting procedures that occur on a regular basis (at least quarterly) to ensure senior management across the Council are aware of incident volume, security risks and initiatives in place to ensure lessons learned are communicated to staff across departments at the Council
- The Council should ensure they update all playbooks to accurately represent the processes that are followed by the IT security team during an incident response

Assurance



- Management should ensure that lessons learned are documented and shared with the incident response team, team leads and the wider organisation as appropriate
- The Council should implement a mandatory cyber security awareness training module to be completed on an annual basis for all staff members.

Procurement Cards

Objective

To assess the robustness of processes for ensuring staff purchases made using procurement cards is transparent and valid.

Themes

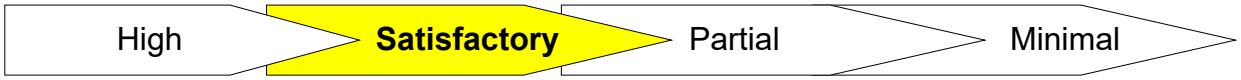
Procurement cards are an important tool to support council staff in the delivery of services, through enabling the purchase of appropriate goods and services. Effective control of the issue and use of procurement cards is important to support that they are used by appropriate staff to purchase items in accordance with council policy.

In this audit, we assessed the controls in place in relation to the set-up, use of and approval of procurement card expenditure. We have identified that the controls in place across all areas covered in the scope of this audit are appropriately designed, particularly in relation to setup and use of procurement cards.

However, the Council should ensure that the use of procurement cards is regularly reviewed and monitored through the spend analysis report to ensure appropriate oversight of use of the cards and expenditure arising. This will allow the Council to identify and resolve issues relating to procurement card spend in a timely manner.

Appendix 2a: Audit Opinion and Themes

Assurance



Accounts Payable

Objective

To assess the robustness of processes for ensuring staff purchases made using procurement cards is transparent and valid.

Themes

This audit focussed on the processes for ensuring accurate, transparent, and valid payments are made to suppliers and individuals. We identified a strong control environment in place over the Accounts Payable process. In particular, we performed detailed testing of the process for onboarding new suppliers, making changes to supplier standing data, and for purchase invoice receipt and processing. We noted that these controls were well designed and did not identify any exceptions in relation to these areas. There are, however, a small number of opportunities to further streamline the process in certain areas:

- Policy and procedure documents should all be reviewed to ensure that they are formalised with a version control matrix setting out the date of last review and date of next scheduled review, and to ensure that policies that have not been reviewed in several years are still reflective of actual working practices. This will mitigate the risk of a lack of clarity in procedures and inconsistencies in processes carried out.
- The process for payment runs and reviewing them for duplicates or other discrepancies is manual, and there is no duplicate payment reporting functionality on Business World, the Council's ERP system. This risk relates to external payment files loaded into the system only, rather than payments generated from invoices processed via the system by the Accounts Payable team. The Council should investigate ways in which Business World can enable automatic reporting on duplicate payments to mitigate the risk of duplicate payments being made due to fraud or error.