CONFIDENTIAL

Note: Confidential Provisions released on 03/02/2021

Port Augusta
CITY COUNCIL

REPORT FOR:	**Audit Committee**		
MEETING DATE:	19 May 2020		
REPORT FROM:	Director City Services		
REPORT TITLE:	**Information Report – Auditor General Cyber Security Audit Update**		
FILE NAME:	F20/204	RECORD NO:	AR20/20999

STRATEGIC DIRECTIONS	
5	**Governance and Financial Sustainability**
5.5	We meet or exceed legislative and accreditation requirements for all relevant programs.

SUMMARY/ABSTRACT

The purpose of this report is to provide the Audit Committee with an update in relation to an Audit Process that Council has been required to participate in, by the State Government Auditor General.

RECOMMENDATION

Audit Committee recommends Council receives and notes the report (AR20/20999) dated 13/05/2020, submitted by the Director City Services concerning Information Report – Auditor General Cyber Security Audit Update.

BACKGROUND

In December 2019, Council was informed that Port Augusta City Council had been randomly selected to be subject to an Audit for 'Examination of the cyber security within Local Government' by the State Government Auditor General, under the Public Finance and Audit Act 1987. The audit was undertaken both on site and externally between December 2019 and February 2020. The Audit was conducted on two metropolitan and one regional Council.

DISCUSSION

Audit Process

Council welcomes the external review of systems and processes to ensure that our practices meet current industry standards and to mitigate any risk to the organisation.

The Audit process required the input of Council's Information Services Team, to provide background documentation, and assist with facilitating access to Council Information Technology Systems. Communication with the auditors was open throughout the process, and any issues that Council was advised of during the audit process were addressed as a matter of priority.

The Audit reviewed Council's security governance arrangements, system security, change management processes and backup operations and disaster recovery. This included a review of the external facing website, policies and procedures, passwords and system access, security and vulnerability and penetration testing.

Draft Report
A draft report was received in early May and Council has been provided with an opportunity to correct any factual inaccuracies as well as proving some additional comments to provide context to some of the finding. Council will provide feedback to the Auditor General for consideration, and the final report will then be sent to Council for formal comment and response, which will be included in the report. The completed report will be submitted to Parliament later in the year.

The Auditor General has requested that all information in relation to the Audit is to be retained in confidence until such time as the final report is tabled in Parliament.

Audit Findings
It should be noted that Council is providing further context to the audit findings that have been received, and this may change the finding in the final version of the report.

Security Governance
- Lack of cyber security related policies, procedures and standards
- Lack of cyber security awareness
- Insufficient management of risks and contracts over third party service providers
- ICT related risk register and reporting does not exist
- No ongoing ICT security audits, penetration testing or vulnerability assessments

System Security
- Weakness in password controls (already addressed)
- Weakness in privileged user access
- Insufficient user access management
- Security events are not logged or monitored
- Security updates not regularly installed
- Physical access to the server room is not appropriately restricted (not possible)
- Insufficient network segmentation
- Insufficient end-user device security

Change Management
- Insufficient change management protocols

Backup operations and disaster recovery
- No backup and recovery management policy and procedure
- Planning for information security incidents and ICT disaster recovery have not been established

Of the 16 findings made, 10 of these will be addressed with the formalisation and adoption of Policies and Procedures or changes to other documentation that evidence the current arrangements. For many of these findings we already have the systems and processes in place however we were able to demonstrate this as they are not formally documented. For the remaining 6 findings, it is recommended that Council provide further training and review the physical and electronic access to accounts and systems.

With Council now having access to the findings, progress is already being made to address the actions identified. Following the submission of the final report to Parliament, the report will be provided to the Audit Committee, together with a summary of the actions taken by Council as a result of the Audit.

CONFIDENTIALITY PROVISIONS

The Council is satisfied that, pursuant to Section 90(3)(j) of the Act, the information to be received, discussed or considered in relation to this Agenda Item is information the disclosure of which would divulge information provided on a confidential basis by a public authority - Auditor General. It is considered that the open discussion in relation to the Audit, the disclosure of which would breach the Council's obligation to maintain confidentiality, should be considered under confidential provisions.

In addition, the disclosure of this information would, on balance, be contrary to the public interest. The public interest in public access to the meeting has been balanced against the public interest in the continued non-disclosure of the information. The benefit to the public at large resulting from withholding the information outweighs the benefit to it of disclosure of the information. The Council is satisfied that the principle that the meeting be conducted in a place open to the public has been outweighed in the circumstances because the disclosure of the Audit information may severely prejudice Council's Cyber Security and breach confidentiality requirements imposed by a public authority.

Having considered this agenda item in confidence under Section 90(2) and (3)(j) of the Local Government Act 1999, the Council, pursuant to Section 91(7) of that Act orders that report (AR20/20999), discussions and minutes be retained in confidence for a period of 12 months or until such time as advice is received from the Auditor General that the information can be released, and that this order be reviewed every 12 months.

RISK MANAGEMENT

1: Financial/Budget/Asset Management
Council's Information Systems budget includes provisions for the ongoing security, maintenance and upgrade of Council's IT systems and applications.

2: Legal/Policy
The Auditor-General conducted this examination under section 32(1)(a) of Public Finance and Audit Act 1987.

3: Environment/Planning
Not applicable.

4: Community
Council is committed to ensuring the security of all electronic systems and applications, to ensure the ongoing provision of services to the community, and to protect the personal information held within those systems.

Melissa Kretschmer
13/05/2020