# CONFIDENTIAL

**Note: Confidential Provisions released on 03/02/2021**

| | | | |
|---|---|---|---|
| REPORT FOR: | **Council** | | |
| MEETING DATE: | 11 February 2020 | | |
| REPORT FROM: | Director City Services | | |
| REPORT TITLE: | **Information Report – Auditor General Cyber Security Audit** | | |
| FILE NAME: | F14/494 | RECORD NO: | AR20/1643 |

| COMMUNITY VISION & STRATEGIC PLAN OUTCOMES | |
|---|---|
| **6** | **We Achieve** |
| 6.3 | We aim to provide good governance practices and compliance with all legislative requirements in delivery of services. |
| 6.4 | The use of technology is maximised to ensure that records, data and information systems are maintained to a high standard. |

## PURPOSE

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

## RECOMMENDATION

**Council** receives and notes the report (AR20/1643) dated 13/01/2020, submitted by the Director City Services concerning Information Report – Auditor General Cyber Security Audit".

## 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. Refer letter dated 16 December 2019 – attached.

## DISCUSSION

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 is being conducted on two metropolitan and two regional Councils.

The Audit process commenced at the start of January, and has required the input of Council's Information Services Team, to provide background documentation, and assist with facilitating access to Council Information Technology Systems. The Audit will address Council external facing website, policies and procedures, an include vulnerability and penetration testing.

All activities to date have been conducted externally. The Auditors will be onsite in the last week of January to conduct further audit activities.

The Auditor General has advised that any issues that are identified throughout the audit process will be passed onto Council as they are found, to allow Council the opportunity to mitigate and address any organisational risk in a timely manner.

A draft report will be provided to Council's Information Services Team to provide comment, prior to the report being finalised for submission to Parliament.

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.

**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, attachments, 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.

**Melissa Kretschmer**
**13/01/2020**

**For official use only**
**PRIVATE AND CONFIDENTIAL**

Government of South Australia
Auditor-General's Department

Level 9
State Administration Centre
200 Victoria Square
Adelaide SA 5000
DX 56208
Victoria Square
Tel +618 8226 9640
Fax +618 8226 9688
ABN 53 327 061 410
audgensa@audit.sa.gov.au
www.audit.sa.gov.au

Our ref: I19/805

13 December 2019

Mayor Brett Benbow
Port Augusta City Council
PO Box 1704
PORT AUGUSTA SA 5700

Dear Mayor Benbow

**Examination of the cyber security within Local Government**

## Introduction

The purpose of this letter is to inform the Port Augusta City Council (the Council) that I have determined to conduct an examination of the Council's cyber security management pursuant to section 32(1)(a) of the *Public Finance and Audit Act 1987* (PFAA). An extract of the PFAA is attached for your reference in Attachment 1 to this letter. We will also be examining other selected councils regarding this matter in the local government sector. We will not be examining all 68 councils.

This letter details the examination scope, responsibilities and the reporting process.

On 12 December 2019 my audit representatives Mr Andrew Corrigan, Mr Brenton Borgman, Mr Tyson Hancock and an external specialist Mr David Hobbis discussed the abovementioned matters via a teleconference with Council representatives, including Mr John Banks and Mr Richard Maudslay.

## Examination scope

Council ICT systems and their public facing corporate websites provide a valuable service for council operations. For example, council websites can be used for their rate payers to:

- access council application forms
- payment of rates, fines and infringements and dog registration and renewals
- lodge a development application and notify building inspections
- organise hard waste collections.

Effective management of cyber security arrangements has a direct relationship with the ability of Councils to provide ICT services and activities that maintain appropriate service availability, confidentiality and data integrity.

The public would expect councils to have clear plans and strategies to maintain a reasonable level of security controls applied to their ICT services to protect their confidential rate payer data.

The objective is to examine whether the council is effectively managing their cyber security arrangements and data in the provision of council's ICT services. This includes the effective management of the council's key website services to enable reasonable protection of sensitive data from malicious activity and cyber breaches.

We intend to conduct our examination during the first quarter of 2020 and will examine the Council's ICT governance, system security (including the Council's website), change management and backup and disaster recovery arrangements.

To conduct this examination, we have engaged an external specialist. To reduce the impact on your Council's time, where possible, we intend to use tools to automatically extract information for testing purposes. The specific tools and the timing of their use will be discussed and confirmed with relevant Council representatives.

## Examination responsibility

The examination will involve consultation with the relevant Council staff and review of documentation.

The Auditor-General's powers to obtain information and supporting documentation are specified under sections 30 and 34 of the PFAA. The information and supporting documentation obtained during the examination is used for the sole purpose of performing and reporting the examination and will remain confidential.

For an efficient and effective examination, the Council will need to provide timely access to personnel and information to assist the process. We propose to conduct the examination testing phase over the period January to April 2020. This testing phase however may be extended if timely access to personnel and information is not received

## Reporting process

Section 32 of the PFAA requires the Auditor-General to prepare a report on the results of the examination and provide a copy of the report to both the Council and to Parliament. Any communication on the examination results will be subject to the procedural fairness process outlined below.

At the completion of the examination, we will:

- meet with the Council's key personnel to discuss the examination results
- provide the Council a copy of the draft report on the examination results, including details of any findings and recommendations. At this stage, we will request the Council to formally respond in writing to the findings and recommendations

- provide the Council a copy of the final draft report for review and comment prior to finalising the report to Parliament. The final draft report will include the Council's response.

The President of the Legislative Council and the Speaker of the House of Assembly must, not later than the first sitting day after receiving the final report from the Auditor-General, table it before their respective Houses. To respect the concurrent and mutual reporting obligations to Council and the Parliament, I would appreciate all communication regarding the examination (including email correspondence) being treated as confidential and not made publicly available or published (such as in the Council's meeting minutes).

A copy of the final report will be provided to the Council and made available on our website at www.audit.sa.gov.au from the date it is ordered by Parliament to be published.

## Other matters

Arrangements will be made for a site visit by the audit managers and/or its representatives conducting the examination to obtain an understanding of cyber security management with the officers nominated by the Council.

Attachment 2 to this letter provides a list of required preliminary information as was discussed with the council representatives. I would appreciate the documentation being provided by **15 January 2020**.

Our internal cost of conducting this examination and preparing the report to Parliament will be funded by my Department. Should there be a justifiable reason for seeking some cost recovery I will formally communicate this position and the reason(s) for the changed position.

The senior authorised officers responsible for the conduct of the examination are:

- Mr Andrew Corrigan, Assistant Auditor-General (Specialist Reviews and Analytics)
- Mr Brenton Borgman, Principal Audit Manager (IT Audit)
- Mr Tyson Hancock, Principal Audit Manager (IT Audit)
- Mr David Hobbis, Partner, Deloitte Risk Advisory

The officers can be contacted by email at TeamITA@audit.sa.gov.au or on 8226 9640.

Thank you for your assistance in this matter.

Yours sincerely

Andrew Richardson
**Auditor-General**

cc: Mr John Banks, Chief Executive Officer

**For official use only**

**PRIVATE AND CONFIDENTIAL**

**Attachment 1: Extract of section 32 of the *Public Finance and Audit Act 1987***



## 32—Examination of publicly funded bodies and projects and local government indemnity schemes

(1) The Auditor-General may—

(a) examine the accounts of a publicly funded body and the efficiency, economy and effectiveness of its activities; or

(b) examine accounts relating to a public funded project and the efficiency, economy and effectiveness of the project; or

(c) examine accounts relating to a local government indemnity scheme and the efficiency, economy and effectiveness of the scheme.

(1a) An examination may be made under this section even though the body, project or scheme to which the examination relates has ceased to exist.

(1b) The Auditor-General must conduct an examination under subsection (1) if requested to do so by the Treasurer or the Independent Commissioner Against Corruption.

(2) After making an examination under subsection (1), the Auditor-General must prepare a report setting out the results of the examination.

(3) The Auditor-General must deliver copies of the report to—

(a) any publicly funded body concerned in the examination; and

(b) if the examination was requested by the Treasurer—the Treasurer; and

(c) if the examination was requested by the Independent Commissioner Against Corruption—the Independent Commissioner Against Corruption; and

(d) the President of the Legislative Council and the Speaker of the House of Assembly.

**For official use only**

**PRIVATE AND CONFIDENTIAL**

## Attachment 2: Preliminary documentation request

Please provide the following documentation:

1. Information Security Policies and Procedures
2. Network and infrastructure topology diagram
3. Cyber incident response plan
4. Technology function organisational structure
5. ICT Disaster Recovery plans for the Council's most critical applications
6. List of key third-party technology service providers, including any cloud service providers
7. Copy of the IT audit/security findings arising from recent independent assessments
8. ICT Governance /security committee Terms of Reference (ToR)
9. Change Management policy.