

# AUDIT COMMITTEE MINUTES

6 JUNE 2019

**REPORT ITEM 11.1 – ATTACHMENTS 1 – 4**

**REPORT ITEM 11.2 – ATTACHMENT**

Eastern Metropolitan Regional  
Council

Internal Audit Report

Investment Policies

**PAXON** GROUP

Private Client Services  
Audit and Assurance  
Taxation

Perth • Melbourne • Sydney | April 2019 – Version 1.0

Liability limited by a scheme approved under Professional Standards Legislation.

# Table of Contents

---

- Executive Summary ..... 3
- 1 Introduction ..... 5
  - 1.1 Background ..... 5
  - 1.2 Internal Audit Objective..... 5
- 2 Scope ..... 6
- 3 Methodology..... 7
- 4 Inherent Limitations..... 8
- 5 Detailed Audit Findings..... 9
- 6 Efficiencies and Other Observations ..... 11
- Appendix A..... 12

## Executive Summary

Process	Excellent	Very Good	Satisfactory	Needs Improvement	Not Satisfactory
	★★★★★	★★★★	★★★	★★	★
	Strengths		Weaknesses		Rating
<b>Investment Policies</b>	<ul style="list-style-type: none"> <li>• A revised “<i>Management of Investments Policy</i>” was adopted by Council in February 2019 and is available on the EMRC’s intranet. Paxon found current investment practices comply with this policy;</li> <li>• A “<i>Management Guideline for Investments</i>” exists;</li> <li>• Appropriate controls exist to address identified investment risks;</li> <li>• Investments are duly authorised by the CEO in terms of the approved policy;</li> <li>• Comprehensive details are provided to the CEO to support proposed investments; and</li> <li>• Processes are in place to provide reasonable assurance the Council is receiving the best possible return on investments.</li> </ul>		<ul style="list-style-type: none"> <li>• No weaknesses were noted.</li> </ul>		★★★★★

# Overall Report Rating

Rating	Excellent	Very Good	Satisfactory	Needs Improvement	Not Satisfactory
	☆☆☆☆☆				

See Appendix A for a guide to the overall report rating scale.

# 1 Introduction

---

## 1.1 Background

The EMRC's Annual Financial Report for the year ended 30 June 2018 (Report) records interest earnings of \$2,416,358 for the financial year (\$2,471,983 for 2016/2017). The Report discloses cash and cash equivalents of \$97,180,201 as at 30 June 2018 (\$90,799,929 as at 30 June 2017). As per note 10 to the Report, \$87,253,192 of the cash and cash equivalents are categorised as "restricted" due to restrictions imposed by regulations or other externally imposed requirements.

## 1.2 Internal Audit Objective

The EMRC's "*Strategic Internal Audit Plan – 2016 – 2019*" records the following audit objectives for Investment Policies:

- Determine whether there are adequate reporting processes in place to provide reasonable assurance that investment information is useful and received in a timely manner;
- Identify whether an investment policy exists, is authorised and available to the relevant staff;
- Identify whether investments are authorised in accordance with approved policy; and
- Identify whether processes are in place to provide reasonable assurance that the Council is receiving the best possible return on investment.

## 2 Scope

The following process was covered in the internal audit:

Process	Key Risks
Investment Policies	<ul style="list-style-type: none"> <li>• Non-compliance with policy;</li> <li>• Inappropriate policy; and</li> <li>• Absence of, or non-compliance with funds management procedures.</li> </ul>

### Scope exclusions:

The internal audit covered the period from 1 July 2018 to 31 March 2019.

## 3 Methodology

---

Our methodology for the internal audit comprised:

- Conducting an initial meeting with management to obtain an understanding of processes and potential issues;
- Developing overview documentation of the processes including key controls by discussion with staff and review of the processes;
- Evaluating the adequacy of the controls to cover the identified risks and testing the compliance with the key controls;
- Researching the issues, weaknesses and potential improvements noted from our discussions and review of the existing processes including compliance with key controls;
- Developing appropriate recommendations for improvement for discussion with management;
- Drafting a report of findings and recommendations and obtaining formal responses from management; and
- Finalising the report and issuing it to the Director Corporate Services for distribution to the Audit Committee and relevant management.



## 4 Inherent Limitations

---

Due to the inherent limitations in any internal control structure, it is possible errors or irregularities may occur and not be detected. Further, the internal control structure, within which the control procedures that have been reviewed operate, has not been reviewed in its entirety and therefore no opinion is expressed as to the effectiveness of the greater internal control structure.

It should also be noted our internal audit was not designed to detect all weaknesses in control procedures as it was not performed continuously throughout the period subject to review.

The internal audit conclusion and any opinion expressed in this report have been formed on the above basis.

## 5 Detailed Audit Findings

Each issue detailed in this Section is rated based on the following scale:

Rating	Definition
High	<ul style="list-style-type: none"> <li>Major contravention of policies, procedures or laws, unacceptable internal controls, high risk for fraud, waste or abuse, major opportunity to improve effectiveness and efficiency, major risk identified. Immediate corrective action is required. A short-term fix may be needed prior to it being resolved properly.</li> </ul>
Medium	<ul style="list-style-type: none"> <li>Significant contravention of policies, procedures or laws, poor internal controls, significant opportunity to improve effectiveness and efficiency, significant risk identified. Corrective action is required. Need to be resolved as soon as resources can be made available, but within six months.</li> </ul>
Low	<ul style="list-style-type: none"> <li>Minor contravention of policies and procedures, weak internal controls, opportunity to improve effectiveness and efficiency, moderate risk identified. Corrective action is required. Need to be resolved within twelve months.</li> </ul>

---

Business Issue	Risk Rating	Implication	Recommendation	Agreed Management Action	Ownership/ Timing
No Business Issues were identified.					

---

## 6 Efficiencies and Other Observations

Below is a summary of our other observations arising from the internal audit, which may assist you in improving the efficiency and effectiveness of your control environment. These observations are provided for your information and a formal response is not required.

Audit Area	Description
<p><b>Investment Policies</b></p>	<p>Due to local government processes and protocols, council policies are generally reviewed on an annual basis. With reference to EMRC <i>“Management of Investments Policy”</i> the items contained within this policy dictates the nature and type of investments that the Council can make any given time. Due to the changing ratings issued by ‘Standard &amp; Poor’s’ for each level of investment the policy does not get updated with these new ratings. A decision to make an investment could be based on a different ‘market’ information as per the council policy.</p> <p>Paxon suggests that EMRC continually updates the Appendix within the Policy to align with the recent credit agency ratings as per the monthly Prudential Investment Services report. It should reflect the following:</p> <ul style="list-style-type: none"> <li>• The names of complying authorised deposit-taking institutions (ADIs);</li> <li>• Current credit ratings for ADIs; and</li> <li>• Correct contributions percentages for ADIs.</li> </ul> <hr/> <p>Paxon examined the EMRC’s <i>“Management Guideline for Investments”</i> and noted the document was <i>“Adopted/Reviewed”</i> in June 2013. Paxon found the Guideline does not disclose appropriate detail as to the different approaches followed for depositing investment funds in:</p> <ul style="list-style-type: none"> <li>• ANZ;</li> <li>• Westpac; and</li> <li>• Via Austraclear clearing house.</li> </ul> <p>The EMRC should update its <i>“Management Guideline for Investments”</i> to ensure it includes appropriate references to the different approaches followed for depositing investment funds with different financial institutions.</p>

## Appendix A

Level	Rank	Stars	Financial Loss	Non-Financial Considerations
1	Not Satisfactory	☆	>\$1m	<ul style="list-style-type: none"> <li>Several medium rated observations or one or more high rated observations, significant risk for non-compliance with policies and regulations, serious violations of law, significant opportunities for improvement, substantiated, public embarrassment, very high multiple impacts, high widespread multiple news profile and third-party actions.</li> </ul>
2	Needs Improvement	☆☆	>\$100k<\$1m	<ul style="list-style-type: none"> <li>Several medium rated observations and no high rated observations, control weak in one or more areas, non-compliance with policies and regulations, violation of law (not serious), substantial opportunities for improvement, substantiated, public embarrassment, high impact, high news profile and third-party actions.</li> </ul>
3	Satisfactory	☆☆☆	>\$50k<\$100k	<ul style="list-style-type: none"> <li>Many low rated observations and/or few medium rated observations, several low rated violations of policy, minor violations of regulations, no violations of law, moderate opportunities for improvement, substantiated, public embarrassment, moderate impact and moderate news profile.</li> </ul>
4	Very Good	☆☆☆☆	>\$10k<\$50k	<ul style="list-style-type: none"> <li>Several low rated observations and/or one or two medium rated observations, minor contraventions of policies and procedures, no violations of law, minor opportunities for improvement, substantiated, low impact and low news profile.</li> </ul>
5	Excellent	☆☆☆☆☆	<10k	<ul style="list-style-type: none"> <li>Few low rated observations, no internal control weaknesses noted, good adherence to laws, regulations and policies, excellent control environment, unsubstantiated, low impact, low profile or no news item.</li> </ul>

### **Perth**

Level 5, 160 St Georges Terrace  
Perth Western Australia 6000  
Telephone: +61 8 9476 3144  
Facsimile: +61 8 9476 3188  
GPO Box 2753, Perth WA 6001

### **Melbourne**

Level 27, 101 Collins Street  
Melbourne VIC 3000  
Telephone: +61 3 9111 0046  
Facsimile: +61 3 9111 0045

### **Sydney**

Level 57, MLC Centre, Martin Place  
Sydney NSW 2000  
Telephone: +61 2 8355 3690  
Facsimile: +61 2 8355 3689

[www.paxongroup.com.au](http://www.paxongroup.com.au)

providingvalue

Eastern Metropolitan Regional  
Council  
Internal Audit Report  
Procurement 2019

**PAXON** GROUP

Private Client Services  
Audit and Assurance  
Taxation

Perth • Melbourne • Sydney | May 2019 – Version 3.0  
Liability limited by a scheme approved under Professional Standards Legislation.

# Table of Contents

---

Executive Summary .....	3
1 Introduction .....	4
1.1 Background .....	4
1.2 Internal Audit Objective.....	4
2 Scope .....	5
3 Methodology.....	6
4 Inherent Limitations.....	7
5 Detailed Audit Findings.....	8
6 Efficiencies and Other Observations .....	10
Appendix A.....	11



## Executive Summary

Process	Excellent	Very Good	Satisfactory	Needs Improvement	Not Satisfactory
	★★★★★	★★★★	★★★	★★	★
	Strengths		Weaknesses		Rating
Procurement	<ul style="list-style-type: none"> <li>• A “Purchasing Policy” is in place;</li> <li>• The Tender Procedure document 1.3 was reviewed and adopted by Council on 6 December 2018;</li> <li>• Corporate credit card guidelines are in place;</li> <li>• A pre-numbered electronic purchase order system is used;</li> <li>• Management reports are produced to help ensure the probity of the procurement process; and</li> <li>• All issues raised in the previous Procurement internal audit report have been addressed. There are no outstanding issues.</li> </ul>				★★★★★

## Overall Report Rating

Rating	Excellent	Very Good	Satisfactory	Needs Improvement	Not Satisfactory
	★★★★★				

See Appendix A for a guide to the overall report rating scale.

# 1 Introduction

---

## 1.1 Background

The 2017/2018 Annual Report of the Eastern Metropolitan Regional Council (“EMRC”) records total expenses of \$27,903,608 and total revenue of \$39,351,664.

Paxon has been engaged by the EMRC to review the Procurement process of the Council.

## 1.2 Internal Audit Objective

The overall objective for this internal audit of Procurement was to provide assurance effective and efficient controls are in place for the Procurement process of the EMRC.

## 2 Scope

---

The following process was covered in the internal audit:

Process	Key Risks
Procurement	<ul style="list-style-type: none"> <li>• Efficiency;</li> <li>• Probity on tenders; and</li> <li>• Compliance with Local Government Act and Regulations.</li> </ul>

### Scope exclusions:

The scope of the internal audit of Procurement excluded the following:

- Contract Management.

The internal audit covered the period from 1 July 2018 to 31 March 2019.

## 3 Methodology

---

Our methodology for the internal audit comprised:

- Conducting an initial meeting with management to obtain an understanding of processes and potential issues;
- Developing overview documentation of the processes including key controls by discussion with staff and review of the processes;
- Evaluating the adequacy of the controls to cover the identified risks and testing the compliance with the key controls;
- Researching the issues, weaknesses and potential improvements noted from our discussions and review of the existing processes including compliance with key controls;
- Developing appropriate recommendations for improvement for discussion with management;
- Drafting a report of findings and recommendations and obtaining formal responses from management; and
- Finalising the report and issuing it to the Director Corporate Services for distribution to the Audit Committee and relevant management.

## 4 Inherent Limitations

---

Due to the inherent limitations in any internal control structure, it is possible errors or irregularities may occur and not be detected. Further, the internal control structure, within which the control procedures that have been reviewed operate, has not been reviewed in its entirety and therefore no opinion is expressed as to the effectiveness of the greater internal control structure.

It should also be noted our internal audit was not designed to detect all weaknesses in control procedures as it was not performed continuously throughout the period subject to review.

The internal audit conclusion and any opinion expressed in this report have been formed on the above basis.

## 5 Detailed Audit Findings

Each issue detailed in this Section is rated based on the following scale:

Rating	Definition
High	<ul style="list-style-type: none"> <li>Major contravention of policies, procedures or laws, unacceptable internal controls, high risk for fraud, waste or abuse, major opportunity to improve effectiveness and efficiency, major risk identified. Immediate corrective action is required. A short-term fix may be needed prior to it being resolved properly.</li> </ul>
Medium	<ul style="list-style-type: none"> <li>Significant contravention of policies, procedures or laws, poor internal controls, significant opportunity to improve effectiveness and efficiency, significant risk identified. Corrective action is required. Need to be resolved as soon as resources can be made available, but within six months.</li> </ul>
Low	<ul style="list-style-type: none"> <li>Minor contravention of policies and procedures, weak internal controls, opportunity to improve effectiveness and efficiency, moderate risk identified. Corrective action is required. Need to be resolved within twelve months.</li> </ul>

---

Business Issue	Risk Rating	Implication	Recommendation	Agreed Management Action	Ownership/ Timing
o There were no Business Issues arising					

---

## 6 Efficiencies and Other Observations

Below is a summary of our other observations arising from the internal audit, which may assist you in improving the efficiency and effectiveness of your control environment. These observations are provided for your information and a formal response is not required.

Audit Area	Description
Procurement	<ul style="list-style-type: none"> <li>• None</li> </ul>



## Appendix A

Level	Rank	Stars	Financial Loss	Non-Financial Considerations
1	Not Satisfactory	☆	>\$1m	<ul style="list-style-type: none"> <li>• Several medium rated observations or one or more high rated observations, significant risk for non-compliance with policies and regulations, serious violations of law, significant opportunities for improvement, substantiated, public embarrassment, very high multiple impacts, high widespread multiple news profile and third-party actions.</li> </ul>
2	Needs Improvement	☆☆	>\$100k<\$1m	<ul style="list-style-type: none"> <li>• Several medium rated observations and no high rated observations, control weak in one or more areas, non-compliance with policies and regulations, violation of law (not serious), substantial opportunities for improvement, substantiated, public embarrassment, high impact, high news profile and third-party actions.</li> </ul>
3	Satisfactory	☆☆☆	>\$50k<\$100k	<ul style="list-style-type: none"> <li>• Many low rated observations and/or few medium rated observations, several low rated violations of policy, minor violations of regulations, no violations of law, moderate opportunities for improvement, substantiated, public embarrassment, moderate impact and moderate news profile.</li> </ul>
4	Very Good	☆☆☆☆	>\$10k<\$50k	<ul style="list-style-type: none"> <li>• Several low rated observations and/or one or two medium rated observations, minor contraventions of policies and procedures, no violations of law, minor opportunities for improvement, substantiated, low impact and low news profile.</li> </ul>
5	Excellent	☆☆☆☆☆	<10k	<ul style="list-style-type: none"> <li>• Few low rated observations, no internal control weaknesses noted, good adherence to laws, regulations and policies, excellent control environment, unsubstantiated, low impact, low profile or no news item.</li> </ul>

### **Perth**

Level 5, 160 St Georges Terrace  
Perth Western Australia 6000  
Telephone: +61 8 9476 3144  
Facsimile: +61 8 9476 3188  
GPO Box 2753, Perth WA 6001

### **Melbourne**

Level 27, 101 Collins Street  
Melbourne VIC 3000  
Telephone: +61 3 9111 0046  
Facsimile: +61 3 9111 0045

### **Sydney**

Level 57, MLC Centre, Martin Place  
Sydney NSW 2000  
Telephone: +61 2 8355 3690  
Facsimile: +61 2 8355 3689

[www.paxongroup.com.au](http://www.paxongroup.com.au)

providingvalue

Eastern Metropolitan Regional  
Council  
Internal Audit Report  
Taxation

**PAXON** GROUP

Private Client Services  
Audit and Assurance  
Taxation

Perth • Melbourne • Sydney | May 2019 – Version 1.0

Liability limited by a scheme approved under Professional Standards Legislation.

# Table of Contents

---

Executive Summary .....	3
<b>1 Introduction .....</b>	<b>4</b>
1.1 Background .....	4
1.2 Internal Audit Objective.....	4
<b>2 Scope .....</b>	<b>5</b>
<b>3 Methodology.....</b>	<b>6</b>
<b>4 Inherent Limitations.....</b>	<b>7</b>
<b>5 Detailed Audit Findings.....</b>	<b>8</b>
<b>6 Efficiencies and Other Observations .....</b>	<b>10</b>
<b>Appendix A.....</b>	<b>11</b>

## Executive Summary

Process	Excellent	Very Good	Satisfactory	Needs Improvement	Not Satisfactory
	★★★★★	★★★★	★★★	★★	★
	Strengths		Weaknesses		Rating
Taxation	<ul style="list-style-type: none"> <li>Business Activity Statements are submitted timeously;</li> <li>Fringe Benefit Return are submitted accurately and on time;</li> <li>Tax payments are made in time;</li> <li>Tax invoices issued to customers comply with legal obligations; and</li> <li>Proper accounting records are kept enabling compliance with tax reporting obligations.</li> </ul>		<ul style="list-style-type: none"> <li>No weaknesses were noted.</li> </ul>		★★★★★

## Overall Report Rating

Rating	Excellent	Very Good	Satisfactory	Needs Improvement	Not Satisfactory
	★★★★★				

See Appendix A for a guide to the overall report rating scale.

# 1 Introduction

---

## 1.1 Background

The EMRC's Annual Financial Report for the year ended 30 June 2018 records goods and services taxes paid of \$2,116,625 for the financial year (\$2,079,857 for 2016/2017). In addition, the EMRC is subject to other tax legislation which include employment taxes.

## 1.2 Internal Audit Objective

The EMRC's *"Strategic Internal Audit Plan – 2016 – 2019"* records the following audit objective for Taxation:

*"Assess the level of compliance with applicable State and Commonwealth legislation."*

## 2 Scope

---

The following process was covered in the internal audit:

Process	Key Risks
Taxation	<ul style="list-style-type: none"><li>• Non-compliance with legislation; and</li><li>• Late submission of returns and payments.</li></ul>

---

### Scope exclusions:

The internal audit covered the period from 1 July 2018 to 31 March 2019.

## 3 Methodology

---

Our methodology for the internal audit comprised:

- Conducting an initial meeting with management to obtain an understanding of processes and potential issues;
- Developing overview documentation of the processes including key controls by discussion with staff and review of the processes;
- Evaluating the adequacy of the controls to cover the identified risks and testing the compliance with the key controls;
- Researching the issues, weaknesses and potential improvements noted from our discussions and review of the existing processes including compliance with key controls;
- Developing appropriate recommendations for improvement for discussion with management;
- Drafting a report of findings and recommendations and obtaining formal responses from management; and
- Finalising the report and issuing it to the Director Corporate Services for distribution to the Audit Committee and relevant management.



## 4 Inherent Limitations

---

Due to the inherent limitations in any internal control structure, it is possible errors or irregularities may occur and not be detected. Further, the internal control structure, within which the control procedures that have been reviewed operate, has not been reviewed in its entirety and therefore no opinion is expressed as to the effectiveness of the greater internal control structure.

It should also be noted our internal audit was not designed to detect all weaknesses in control procedures as it was not performed continuously throughout the period subject to review.

The internal audit conclusion and any opinion expressed in this report have been formed on the above basis.

## 5 Detailed Audit Findings

Each issue detailed in this Section is rated based on the following scale:

Rating	Definition
High	<ul style="list-style-type: none"> <li>Major contravention of policies, procedures or laws, unacceptable internal controls, high risk for fraud, waste or abuse, major opportunity to improve effectiveness and efficiency, major risk identified. Immediate corrective action is required. A short-term fix may be needed prior to it being resolved properly.</li> </ul>
Medium	<ul style="list-style-type: none"> <li>Significant contravention of policies, procedures or laws, poor internal controls, significant opportunity to improve effectiveness and efficiency, significant risk identified. Corrective action is required. Need to be resolved as soon as resources can be made available, but within six months.</li> </ul>
Low	<ul style="list-style-type: none"> <li>Minor contravention of policies and procedures, weak internal controls, opportunity to improve effectiveness and efficiency, moderate risk identified. Corrective action is required. Need to be resolved within twelve months.</li> </ul>

---

Business Issue	Risk Rating	Implication	Recommendation	Agreed Management Action	Ownership/ Timing
No Business Issues were identified.					

---

## 6 Efficiencies and Other Observations

Below is a summary of our other observations arising from the internal audit, which may assist you in improving the efficiency and effectiveness of your control environment. These observations are provided for your information and a formal response is not required.

Audit Area	Description
<p><b>Taxation</b></p>	<p>The incorrect FBT tax rate was used in calculating the 2018 FBT tax refund which resulted in an additional \$3,040.69 refund which was received in the 2018/2019 financial year. The additional \$3,040.69 refund was recorded as “Income Financial Services EMRC” by means of a journal on 1/10/2018. This amount is technically a prior year adjustment which should be included in the Retained Surplus as at 01/07/2018. However, due to the \$3,040.69 being immaterial, Paxon accepts its allocation to a revenue account during the 2018/2019 financial year. Paxon recommends the EMRC brings this matter to the attention of its external auditors.</p>

## Appendix A

Level	Rank	Stars	Financial Loss	Non-Financial Considerations
1	Not Satisfactory	☆	>\$1m	<ul style="list-style-type: none"> <li>Several medium rated observations or one or more high rated observations, significant risk for non-compliance with policies and regulations, serious violations of law, significant opportunities for improvement, substantiated, public embarrassment, very high multiple impacts, high widespread multiple news profile and third-party actions.</li> </ul>
2	Needs Improvement	☆☆	>\$100k<\$1m	<ul style="list-style-type: none"> <li>Several medium rated observations and no high rated observations, control weak in one or more areas, non-compliance with policies and regulations, violation of law (not serious), substantial opportunities for improvement, substantiated, public embarrassment, high impact, high news profile and third-party actions.</li> </ul>
3	Satisfactory	☆☆☆	>\$50k<\$100k	<ul style="list-style-type: none"> <li>Many low rated observations and/or few medium rated observations, several low rated violations of policy, minor violations of regulations, no violations of law, moderate opportunities for improvement, substantiated, public embarrassment, moderate impact and moderate news profile.</li> </ul>
4	Very Good	☆☆☆☆	>\$10k<\$50k	<ul style="list-style-type: none"> <li>Several low rated observations and/or one or two medium rated observations, minor contraventions of policies and procedures, no violations of law, minor opportunities for improvement, substantiated, low impact and low news profile.</li> </ul>
5	Excellent	☆☆☆☆☆	<10k	<ul style="list-style-type: none"> <li>Few low rated observations, no internal control weaknesses noted, good adherence to laws, regulations and policies, excellent control environment, unsubstantiated, low impact, low profile or no news item.</li> </ul>

### **Perth**

Level 5, 160 St Georges Terrace  
Perth Western Australia 6000  
Telephone: +61 8 9476 3144  
Facsimile: +61 8 9476 3188  
GPO Box 2753, Perth WA 6001

### **Melbourne**

Level 27, 101 Collins Street  
Melbourne VIC 3000  
Telephone: +61 3 9111 0046  
Facsimile: +61 3 9111 0045

### **Sydney**

Level 57, MLC Centre, Martin Place  
Sydney NSW 2000  
Telephone: +61 2 8355 3690  
Facsimile: +61 2 8355 3689

[www.paxongroup.com.au](http://www.paxongroup.com.au)

providingvalue

Eastern Metropolitan Regional  
Council  
IT Vulnerability Assessment

**PAXON** GROUP

Private Client Services  
Audit and Assurance  
Taxation

Perth • Sydney • Melbourne | May 2019 – Version. 1  
Liability limited by a scheme approved under Professional Standards Legislation.

# Table of Contents

---

- Executive Summary ..... 3**
- 1 Introduction ..... 5**
  - 1.1 Audit Objectives ..... 5
  - 1.2 Scope ..... 5
- 2 Methodology ..... 6**
- 3 Inherent Limitations ..... 7**
- 4 Risk Assessment Classifications ..... 8**
- 5 Metadata Assessment ..... 10**
  - 5.1 Scope ..... 10
  - 5.2 External Perimeter Port Scan Results ..... 10
  - 5.3 Publicly Discoverable Email Addresses ..... 10
- 6 Detailed Findings – External Network Penetration Test ..... 14**
  - 6.1 Remote Management Service Accepting Unencrypted Credentials ..... 14
  - 6.2 Outlook Web Access Supports TLSV1.0 ..... 16
  - 6.3 DNS Server could be used in a distributed denial of service attack ..... 17
- 7 Detailed Findings - Web Services Penetration Test ..... 19**
  - 7.1 Outdated & Unsupported Software ..... 19
  - 7.2 External Facing Administrator Interface ..... 20
  - 7.3 Webservers Lacking Protective HTTP Headers ..... 21
- Appendix A – Detailed Testing Methodology ..... 24**



## Executive Summary

---

Paxon Group was engaged by The Eastern Metropolitan Regional Council (“EMRC”) to perform Vulnerability Assessment of the IT environment.

The assessment was conducted in a way to simulate an external hacker engaged in a targeted attack against the target network and the web sites with the goals of:

- Defying if a remote attacker can gain control over web applications and the servers;
- Determining the impact of a security breach on:
  - Denial of Service attack; and
  - The confidentiality of the customers’ personal data.

The assessment was conducted per Open Web Application Security Project (OWASP) and National Institute of Standards & Technology (NIST) with recommendations made in accordance with these standards. All tests and actions were conducted under controlled conditions.

Paxon Group conducted the external testing between 15<sup>th</sup> April and 3rd May 2019.

### Findings

Paxon Group was ultimately unable to gain unauthorized access to target systems or data during the limited time-frame of this test. However, medium risk security issue been observed. One of the network devices had the remote management interface exposed to the internet. The interface accepted the credentials of the insecure protocol. An attacker suitably positioned to view a legitimate user's network traffic could intercept the credentials to the network device and penetrate into corporate network. To exploit this vulnerability, an attacker must be suitably positioned to eavesdrop on the victim's network traffic. This scenario typically occurs when a client communicates with the server over an insecure connection such as public Wi-Fi, or a corporate or home network that is shared with a compromised computer.

It should be noted that Paxon Group’s Penetration Test reports do not include findings of vulnerabilities that have little likelihood of playing a role in the compromise of target systems or data. Paxon Group Penetration Tests focus on vulnerabilities exploited, or those that could be exploited under a realistic attack scenario that falls outside the scope of testing.

New attack techniques are developed on a regular basis, potentially affecting the security of all systems and networks. Similarly, new flaws may be discovered in infrastructure components leading to vulnerabilities in the network through no fault of the Eastern Metropolitan Regional Council (“EMRC”).

### Recommendations

Paxon Group has documented tactical recommendations for the remediation of specific vulnerabilities in later sections of this report. Observations documented during testing, we suggest the following strategic actions that EMRC can take to further improve the overall security posture:

- Applications should use transport-level encryption (SSL/TLS) to protect all communications passing between the client and the server. The Strict-Transport-

Security HTTP header should be used to ensure that clients refuse to access the server over an insecure connection;

- Review system baselines for adherence to best practices regarding the use of default passwords and community strings, exposed services, default content, and other configuration options. Ensure those baselines are uniformly enforced across all systems with a security configuration management program or tool; and
- Verify that a patch management process is in place. Ensure that systems are configured according to base security standards and hardening documentation prior to being deployed to the production environment. Regularly patch systems and ensure security fixes are applied in a timely manner. Refer to security best practices for server hardening.

**List of Vulnerabilities**

	Title	Likelihood	Consequence	Overall Risk
1	Remote management service accepting unencrypted credentials	Possible	Moderate	<b>MEDIUM RISK</b>
2	Outlook Web Access supports TLSv1.0	Rare	Moderate	<b>LOW RISK</b>
3	DNS server could be used in a distributed denial of service attack.	Unlikely	Minor	<b>LOW RISK</b>
4	Outdated and unsupported software	Unlikely	Minor	<b>LOW RISK</b>
5	External facing administrator interface	Rare	Moderate	<b>LOW RISK</b>
6	Webservers lacking protective HTTP headers.	Unlikely	Minor	<b>LOW RISK</b>

# 1 Introduction

The Eastern Metropolitan Regional Council (“EMRC”) engaged Paxon Group to undertake a review of the Information Technology (IT) Vulnerability Assessment as per EMRC’s “Strategic Internal Audit Plan 2016 – 2019.”

## 1.1 Audit Objectives

The EMRC’s “Strategic Internal Audit Plan – 2016 – 2019” records the following audit objectives for the IT Vulnerability Assessment:

- Identify and review information system security controls to ensure the availability, integrity and confidentiality of information;
- Determine whether current systems provide effective controls to mitigate vulnerabilities and are operating efficiently;
- Conduct an external vulnerability assessment using no knowledge of the organisation using a set of defined tools;
- Conduct an external vulnerability assessment using detailed knowledge of key devices and services using a set of defined tools; and
- Provide pro-active advice to enhance the prevention of malicious attacks to information systems.

## 1.2 Scope

The following process and risks will be covered in the internal audit:

Process	Key Risks
IT Vulnerability	<ul style="list-style-type: none"> <li>• Unavailability of information systems;</li> <li>• Unreliable information;</li> <li>• Leakage of information; and</li> <li>• Potential theft of data.</li> </ul>

## 2 Methodology

---

Our methodology for this internal audit comprises of the following. For the detailed testing methodology, which breaks down each of the below items, please refer to Appendix A:

- Conducting an initial meeting with management to obtain an understanding of processes and potential issues;
- Developing overview documentation of the processes including key controls by discussion with staff and review of the processes;
- Evaluating the adequacy of the controls to cover the identified risks and testing the compliance with the key controls;
- Following up and confirming action taken on any previous business issues identified and recommendations made;
- Researching the issues, weaknesses and potential improvements noted from our discussions and review of the existing processes including compliance with key controls;
- Developing appropriate recommendations for improvement for discussion with management;
- Drafting a report of findings and recommendations and obtaining formal responses from management; and
- Finalising the report and issuing it to the Director Corporate Services for distribution to the Audit Committee and relevant management.

### 3 Inherent Limitations

---

Due to the inherent limitations in any internal control structure, it is possible errors or irregularities may occur and not be detected. Further, the internal control structure, within which the control procedures that have been reviewed operate, has not been reviewed in its entirety and therefore no opinion is expressed as to the effectiveness of the greater internal control structure.

It should also be noted our internal audit was not designed to detect all weaknesses in control procedures as it was not performed continuously throughout the period subject to review.

The internal audit conclusion and any opinion expressed in this report have been formed on the above basis.

## 4 Risk Assessment Classifications

### Risk Matrix

The following risk matrix is utilised in assessing each of the issues as indicated within this report.

	Insignificant	Minor	Moderate	Significant	Catastrophic
Almost Certain	Medium Risk	Medium Risk	HIGH RISK	EXTREME RISK	EXTREME RISK
Likely	Low Risk	Medium Risk	HIGH RISK	HIGH RISK	EXTREME RISK
Possible	Low Risk	Low Risk	Medium Risk	HIGH RISK	EXTREME RISK
Unlikely	Low Risk	Low Risk	Medium Risk	Medium Risk	HIGH RISK
Rare	Low Risk	Low Risk	Low Risk	Medium Risk	HIGH RISK

### Likelihood

The likelihood was categorised into the following:

- **Almost Certain:** It should be expected that this vulnerability will be exploited and may already have been exploited. The vulnerability is easy to identify and can be exploited automatically or using system tools such as a web browser. The vulnerability does not require any additional special access such as account credentials.
- **Likely:** The vulnerability is likely to be exploited by an attacker in the lifetime of the system. This vulnerability can either be exploited using automated tools or system tools such as a web browser, or is immediately apparent and easy to exploit. Exploitation does not require a high level of access.
- **Possible:** The vulnerability has a moderate likelihood of being exploited. The vulnerability may require special access or special, publicly available tools.
- **Unlikely:** The vulnerability is unlikely to be exploited. Exploitation requires additional vulnerabilities in the system, specifically written tools or an abnormally high level of access.
- **Rare:** The vulnerability requires special circumstances, high levels of access or an impractical level of resources to exploit.

### Consequence

A rating was issued to the consequence of the vulnerability should it be exploited to its full extent. The consequence was categorised into the following:

- **Catastrophic:** The exploitation of this vulnerability could result in levels of financial, reputational, compliance, or operational damage that would threaten

the existence of the organisation. The vulnerability could potentially result in physical harm such as injury or death.

- **Significant:** The exploitation of this vulnerability could cause high levels of financial, reputational or operational damage. The vulnerability could cause non-compliance with regulations or standards.
- **Moderate:** The exploitation of this vulnerability could cause financial, reputational or operational damage. The vulnerability could affect compliance status with regulations or standards.
- **Minor:** The exploitation of this vulnerability could potentially cause minor reputational damage or operational inconvenience. User experience could be affected.
- **Insignificant:** This vulnerability cannot be actively exploited, however it could be used to assist in the exploitation of other vulnerabilities.

### Overall Risk

As a result of the likelihood and consequence categorisations, each vulnerability is assigned an overall risk rating. These ratings are as follows:

- **Extreme:** This vulnerability should be remediated as soon as possible. Access to the system should potentially be restricted or denied while remediation efforts are in progress.
- **High:** The vulnerability should be remediated as soon as possible.
- **Medium:** The vulnerability should be resolved in the next release.
- **Low:** The vulnerability should be resolved when practical.

## 5 Metadata Assessment

### 5.1 Scope

The following IP addresses were in scope of the testing:

- 61.29.87.152/29

The following externally hosted web sites were in scope:

- emrc.org.au
- rgang.org.au
- perthseasternregion.com.au

### 5.2 External Perimeter Port Scan Results

It is possible to determine which TCP ports are open. Paxon recommends reviewing open ports on regular basis and ensure only necessary ports are exposed to the internet.

The following ports were open during the test:

Host	Protocol	Ports
61.29.87.153	TCP	23 (Telnet)
61.29.87.154	TCP	541 (rlogin), 1723 (PPTP), 8010 (HTTP), 8013 (HTTP)
61.29.87.155	TCP	25 (SMTP), 53 (DNS), 443 (HTTPS), 1723 (PPTP), 8010 (HTTP), 8013 (HTTP), 8082 (HTTP)
61.29.87.155	UDP	53 (DNS)
61.29.87.157	TCP	1723 (PPTP), 8010 (HTTP), 8013 (HTTP)

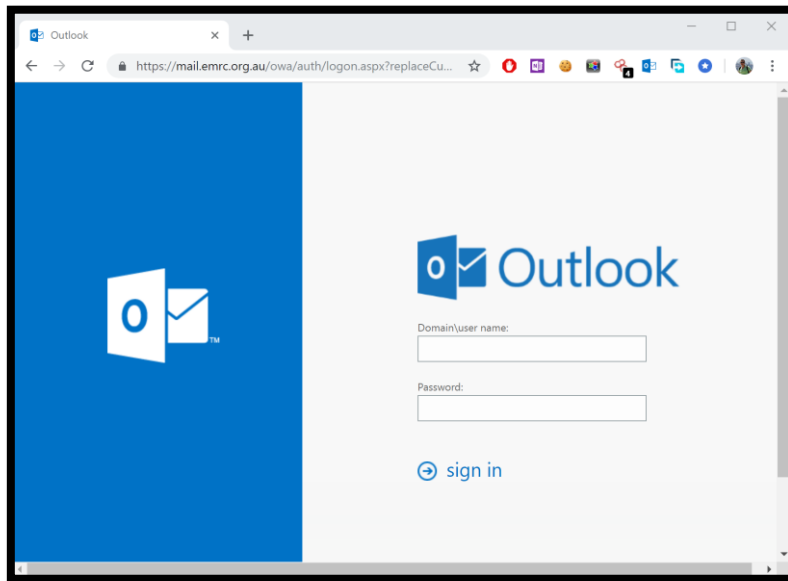
### 5.3 Publicly Discoverable Email Addresses

Using automated web crawling software, it was possible to identify a list of email addresses associated with the EMRC.

The majority of emails listed below were located on various government websites, as opposed to personal services. Email addresses may need to be published online to facilitate ongoing business activities; however, this increases the risk that such users may be subject to generic spam campaigns or even targeted phishing attacks.

Furthermore, given that the EMRC's exchange service is publicly accessible; an attacker may be able utilise this information to determine an appropriate list of usernames to launch further attacks in an attempt to access the email system.





**Screenshot 1: Outlook web access exposed to the internet**

The following is a list of email addresses discovered from public resources:

- mail@emrc.org.au
- environment@emrc.org.au
- BS4Y@emrc.org.au
- stephen.fitzpatrick@emrc.org.au
- WasteEducation@emrc.org.au
- regionaldevelopment@emrc.org.au
- Evans@emrc.org.au
- jaya.vaughan@emrc.org.au
- Catherine.Levett@emrc.org.au
- Peter.Schneider@emrc.org.au
- warren.hill@emrc.org.au
- sales@emrc.org.au
- bronwyn.lee@emrc.org.au
- emicol@emrc.org.au
- joanne.woodbridge@emrc.org.au
- Marilyn.Horgan@emrc.org.au
- Joanne.Woodbridge@emrc.org.au

Further, an additional email had been compromised previously and had credentials posted publicly:

- stephen.fitzpatrick@emrc.org.au (LinkedIn breach)

```
[+] Checking Breach status for stephen.fitzpatrick@emrc.org.au [ pwned ]
[+] Breach      : LinkedIn
[+] Domain     : linkedin.com
[+] Date       : 2012-05-05
[+] Fabricated  : False
[+] Verified   : True
[+] Retired    : False
[+] Spam       : False
```

**Screenshot 1. Breached corporate account**

- Peter.Schneider@emrc.org.au (LinkedIn breach)

```
[+] Checking Breach status for Peter.Schneider@emrc.org.au [ pwned ]
[+] Breach      : LinkedIn
[+] Domain     : linkedin.com
[+] Date       : 2012-05-05
[+] Fabricated  : False
[+] Verified   : True
[+] Retired    : False
[+] Spam       : False
```

**Screenshot 2. Breached corporate account**

### Recommendation

Ensure appropriate user awareness training is undertaken regularly to inform employees of the dangers associated with phishing emails, and how to readily identify them. Additionally, employees should be discouraged from using their EMRC's email address to sign up to any non-work-related services.

Ensure that employees are required to regularly change their passwords for all EMRC accounts, to use different passwords for council and third-party systems, and that any complexity requirements defined are adhered to.

### Managements Comments

*The EMRC does need to publish some email addresses online to facilitate business activities. Of the listed 16 unique email addresses discovered from online sources, 44% related to former staff whose accounts have been either disabled or deleted, and one was an incomplete address. Staff have been encouraged to use group email addresses such as [sales@emrc.org.au](mailto:sales@emrc.org.au) as there are no login passwords associated with a group email. Mail addressed to a group is forwarded to the group members.*

*The EMRC's password policy requires staff to change passwords at least every 42 days. Furthermore there is an account lockout after 3 incorrect attempts with no reset period. IT staff need to unlock the accounts of locked-out users.*

*We are aware of a number of staff corporate email addresses that have been used as a login to external services that have been compromised. These have been identified from the website*

---

<https://haveibeenpwned.com/> that verifies if an email address has been compromised in breaches of sites such as LinkedIn, Adobe, Dropbox, Yahoo mail and others. We agree with the recommendations and will include in future IT Security training recommendations to:

- Avoid using an EMRC email address when signing up to non-work related services;
- Never use the same password for multiple services;
- Periodically change passwords to external Internet services.

# 6 Detailed Findings – External Network Penetration Test

## 6.1 Remote Management Service Accepting Unencrypted Credentials

**Risk Assessment**

Likelihood	Consequence	Overall Risk
Possible	Moderate	<b>MEDIUM RISK</b>

**Description**

The target is determined to be a Cisco device, which uses protocols such as HTTP, TELNET, rlogin, FTP, and SNMP for configuration management. These services can be accessed and are an invitation for malicious users to break in.

**Risk**

Malicious users can exploit this vulnerability to deploy a range of known attacks against accessible services. Brute force attacks such as password guessing and ‘Denial of Service’ are also possible.

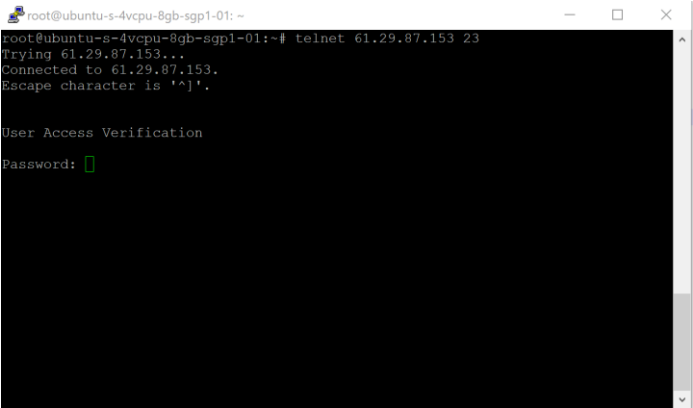
**Recommendations**

Consider taking the following precautionary measures:

- Disable services that are not needed;
- Consider putting access controls on these services. Access controls can be put together using the features in the device (if available) or using an external firewall;
- Do not use default passwords and replace them with hard to guess passwords; and
- Change passwords frequently.

**Additional notes**

Vulnerable hosts: 61.29.87.153  
 Service name: TELNET(Cisco) on TCP port 23.



Screenshot 3. Telnet Transmits Cleartext Credentials

### Management Comments

*This device is the Cisco router used with the iPing SHDSL Internet service. It was recently replaced by the ISP when the old unit failed.*

*The router was pre-configured when received and the EMRC was not provided with any login credentials. We have attempted to login with known CISCO default passwords and have verified that the default password has been changed.*

*The EMRC has contacted the ISP and requested:*

- *Telnet be disabled on the router;*
- *Remote access (if required) to be replaced with SSH and an access control list;*
- *The router be hardened;*
- *A check be made that DDOS protection is enabled.*

*Note that the EMRC would disable remote access to external facing routers as a routine step.*

## 6.2 Outlook Web Access Supports TLSV1.0

### Risk Assessment

Likelihood	Consequence	Overall Risk
Rare	Moderate	LOW RISK

### Description

TLS is capable of using a multitude of ciphers (algorithms) to create the public and private key pairs.

For example if TLSv1.0 uses either the RC4 stream cipher, or a block cipher in CBC mode.

RC4 is known to have biases and the block cipher in CBC mode is vulnerable to the POODLE attack.

TLSv1.0, if configured to use the same cipher suites as SSLv3, includes a means by which a TLS implementation can downgrade the connection to SSL v3.0, thus weakening security.

A POODLE-type attack could also be launched directly at TLS without negotiating a downgrade.

### Risk

An attacker can exploit cryptographic flaws to conduct man-in-the-middle type attacks or to decryption communications.

### Recommendations

Disable the use of TLSv1.0 protocol in favour of a cryptographically stronger protocol such as TLSv1.2. The following openssl commands can be used to do a manual test: `openssl s_client -connect ip:port -tls1` If the test is successful, then the target support TLSv1

### Additional notes

The vulnerability affects the Outlook Web Access interface on mail.emrc.org.au Suitably positioned attacked can potentially decrypt the traffic and get unauthorized access to the user mailboxes

Protocols	Support
TLS 1.3	No
TLS 1.2	Yes
TLS 1.1	Yes
TLS 1.0	Yes
SSL 3	No
SSL 2	No

Screenshot 4. Mail Server supports TLSv1.0

**Management Comments**

*The EMRC agrees that it is desirable to disable the TLSv1.0 protocol. We understand that there is a requirement for a specific patch or hotfix to be installed on our mail server (Exchange 2016) before the protocol can be disabled. We consider it unlikely that the EMRC is running any applications that rely on the TLSv1.0 protocol and are currently checking to verify this before commencing the process to disable the protocol.*

**6.3 DNS Server could be used in a distributed denial of service attack**

**Risk Assessment**

Likelihood	Consequence	Overall Risk
Unlikely	Minor	LOW RISK

**Description**

The remote DNS server answers to any request. It is possible to query the name servers (NS) of the root zone ('.') and get an answer that is bigger than the original request. By spoofing the source IP address, a remote attacker can leverage this 'amplification' to launch a denial of service attack against a third-party host using the remote DNS server.

**Risk**

If the server is used in denial of service attacks, it will negatively affect the organization brand.

**Recommendations**

Restrict access to your DNS server from public network or reconfigure it to reject such queries.

**Additional notes**

Affected services: 61.29.87.155 (udp/53)

The DNS query was 17 bytes long, the answer is 505 bytes long.

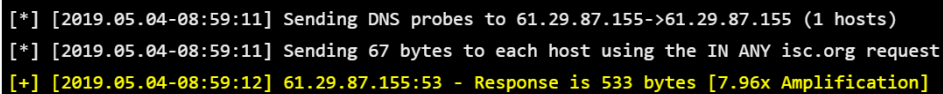
```
;; -->HEADER<<- opcode: QUERY, rcode: NOERROR, id: 6081
;; flags: qr rd ra ; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 12
;; QUESTION SECTION:
;; . IN NS

;; ANSWER SECTION:
. 86400 IN NS m.root-servers.net.
. 86400 IN NS b.root-servers.net.
. 86400 IN NS c.root-servers.net.
. 86400 IN NS d.root-servers.net.
. 86400 IN NS e.root-servers.net.
. 86400 IN NS f.root-servers.net.
. 86400 IN NS g.root-servers.net.
. 86400 IN NS h.root-servers.net.
. 86400 IN NS a.root-servers.net.
. 86400 IN NS i.root-servers.net.
. 86400 IN NS j.root-servers.net.
. 86400 IN NS k.root-servers.net.
. 86400 IN NS l.root-servers.net.
```

```
;; AUTHORITY SECTION:

;; ADDITIONAL SECTION:
m.root-servers.net. 86400 IN A 202.12.27.33
m.root-servers.net. 86400 IN AAAA 2001:dc3::35
b.root-servers.net. 86400 IN A 199.9.14.201
b.root-servers.net. 86400 IN AAAA 2001:500:200::b
c.root-servers.net. 86400 IN A 192.33.4.12
c.root-servers.net. 86400 IN AAAA 2001:500:2::c
d.root-servers.net. 86400 IN A 199.7.91.13
d.root-servers.net. 86400 IN AAAA 2001:500:2d::d
e.root-servers.net. 86400 IN A 192.203.230.10
e.root-servers.net. 86400 IN AAAA 2001:500:a8::e
f.root-servers.net. 86400 IN A 192.5.5.241
f.root-servers.net. 86400 IN AAAA 2001:500:2f::f

;; Query time: 308 msec
;; SERVER: 61.29.87.155
;; WHEN: Tue Apr 30 03:14:59 2019
;; MSG SIZE rcvd: 505
```



```
[*] [2019.05.04-08:59:11] Sending DNS probes to 61.29.87.155->61.29.87.155 (1 hosts)
[*] [2019.05.04-08:59:11] Sending 67 bytes to each host using the IN ANY isc.org request
[+] [2019.05.04-08:59:12] 61.29.87.155:53 - Response is 533 bytes [7.96x Amplification]
```

**Screenshot 5. The query is 67 bytes, the response is 533 bytes**

### Management Comments

*This DNS server is the primary name server for all of the EMRC's active domains. As such, its purpose is to accept queries from the Internet and direct them to the EMRC's websites, mail server and VPN endpoint.*

*A solution to this issue would be to utilise the DNS facilities of our Internet Registrar, Melbourne IT, which would allow the EMRC to remove the DNS server from the public network.*

*The EMRC will commence a project to transition the name server function from the EMRC hosted DNS server to Melbourne IT's DNS facility. This will transfer the risk of a loss of reputation from the EMRC to Melbourne IT which is better equipped to handle the risk of their name servers being used in a DOS attack.*



## 7 Detailed Findings - Web Services Penetration Test

### 7.1 Outdated & Unsupported Software

#### Risk Assessment

Likelihood	Consequence	Overall Risk
Unlikely	Minor	LOW RISK

#### Issue description

Outdated and unsupported software places the information systems at risk of exploitation, as identified vulnerabilities may exist in the software.

Given the level of information disclosed in relation to the target applications, attackers can enumerate the software versions in use, and identify related vulnerabilities, which may lead to a compromise.

#### Risk

No exploits have been available in the public for these software versions.

#### Issue remediation

Paxon recommends an aggressive patch management program as a crucial part of an overall risk management plan.

Organizations that do not have the local expertise to evaluate security patches should assume every patch presents risk and simply deploy security patches as they are published.

#### Additional notes

Vulnerabilities affecting <https://www.perthseasternregion.com.au/> ,  
<https://www.emrc.org.au> and <https://www.rgang.org.au/>

- The library jquery version 1.9.1.min has known security issues.  
CVE-2015-9251: jQuery versions on or above 1.4.0 and below 1.12.0 (version 1.12.3 and above but below 3.0.0-beta1 as well) are vulnerable to XSS via 3rd party text/JavaScript responses (3rd party CORS request may execute) (<https://github.com/jquery/jquery/issues/2432>).
- The library Bootstrap version 3.3.0 has known security issues.  
The data-target attribute in bootstrap versions below 3.4.0 is vulnerable to Cross-Site Scripting (XSS) attacks. Please refer to vendor documentation (<https://github.com/twbs/bootstrap/pull/23687>, <https://github.com/twbs/bootstrap/issues/20184>) for the latest security updates.
- The library moment version 2.9.0 has known security issues.  
Moment versions below 2.11.2 are vulnerable to regular expression denial of service when user input is passed unchecked into moment.duration() blocking the event loop for a period of time. (<https://github.com/moment/moment/issues/2936>).

**Management Comments**

These risks were communicated to the EMRC’s Web Hosting provider with the following response:

*I believe the likelihood of these vulnerabilities being utilised for an attack is minimal, however they are still vulnerabilities that should be addressed. We have recently upgraded the version of jQuery being used in the front-end to the latest version across our base CMS install. This update will be rolled out to all CouncilConnect members in the coming subscription period (along with the latest CMS). We have included updates to both Bootstrap and Moment libraries as a result of this email and have setup a process to be more pro-active in identifying and resolving security issues with associated scripts / plugins.*

**7.2 External Facing Administrator Interface**

**Risk Assessment**

Likelihood	Consequence	Overall Risk
Rare	Moderate	<b>LOW RISK</b>

**Issue description**

It was identified that the Spark CMS administrative console was accessible over the internet. Such interfaces are frequently targeted by attackers, as they can be leveraged to gain remote access to the underlying host and web applications.

**Risk**

The issue can potentially lead to web services compromise and web site defacement. Paxon attempted to login to the console using the common passwords, but he was unable to guess the valid combination. The risk was assessed as Low.

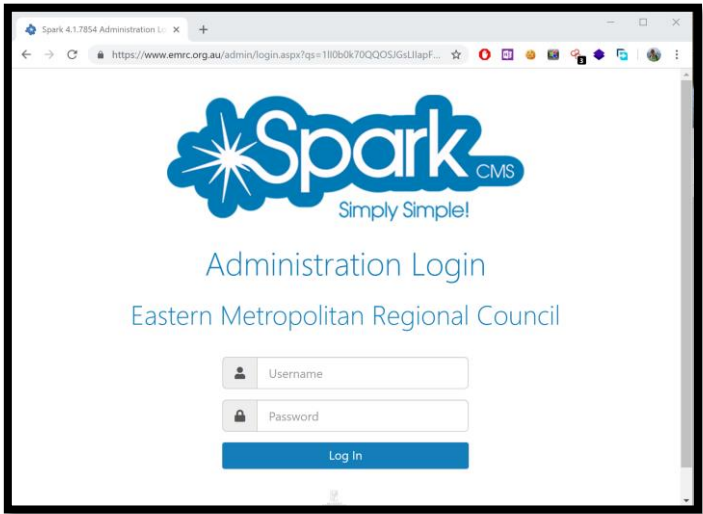
**Issue remediation**

Restrict the access to the administrative interfaces by IP address.

**Additional notes**

Affected services:

- <https://www.rgang.org.au/admin/>
- <https://www.perthseasternregion.com.au/admin/>
- <https://www.emrc.org.au/admin/>



Screenshot 6. External facing administrator interface

**Management Comments**

The EMRC had requested that access to the Spark CMS be restricted to the EMRC’s IP addresses in October 2017 when our current websites were being developed. At the time our service provider was able to restrict access to our Intranet, but was not able to filter access to the CMS as it was common to all of their clients. We have re-submitted the request and have obtained the following response:

*Changes to the IP Address lockdown capability allow for folders within a website to be restricted. While this hasn’t been tested with the Administration section of the website yet, we will test and adjust CMS to allow this to happen. It has been added to our roadmap with priority.*

**7.3 Webservers Lacking Protective HTTP Headers**

**Risk Assessment**

Likelihood	Consequence	Overall Risk
Unlikely	Minor	<b>LOW RISK</b>

**Issue description**

The webservers were found to be missing protective HTTP headers which assist in hardening the overall security posture of the associated web applications. The headers found to be missing include:

*Strict-Transport-Security (HSTS)*

This header should be configured for all sites where an HTTPS alternative is available. By configuring this header, the browser will redirect all communications to the alternate HTTPS URL for the duration configured. This has the added benefit of

preventing downgrade attacks where the client may be forced to access the site over HTTP, thus divulging sensitive information to a listening attacker.

*Content-Security-Policy (CSP)*

This header restricts the sources from which the browser will load resources including scripts, styles and media. By permitting only trusted sources and secure HTTPS channels, this header can help prevent XSS and sniffing attacks.

*Feature-Policy*

Feature Policy is a new header that allows a site to control which features and APIs can be used in the browser.

**Issue remediation**

Configure the following HTTP headers on all affected servers:

*Strict-Transport-Security: max-age=31536000 ; includeSubDomains*

This option ensures that the browser remembers that the webpage is only accessible over HTTPS and includes all associated sub domains. Note that this will also affect internal applications under the affected domain, and is difficult to roll back prior to the expiry of the header. Implementation of HSTS should be carefully planned and staged using progressively larger max-age values.

*Content-Security-Policy: default-src 'self'*

For sites that only load resources from a single web application server, configure the CSP header to only allow resources to be loaded from that server for all resource types. If resources are loaded from other trusted sources, create a more specific CSP header.

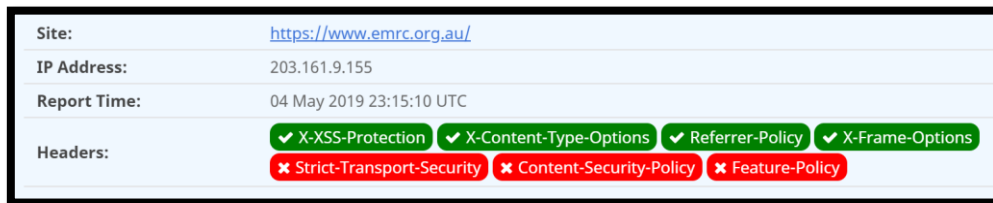
*Feature-Policy: vibrate 'self'; usermedia \*; sync-xhr 'self' https://example.com*

In the above example by specifying vibrate and allowing it for self the feature is disabled for all origins except our own.

**Additional notes**

Headers missing on [www.emrc.org.au](http://www.emrc.org.au)

- Strict-Transport-Security
- Content-Security-Policy
- Feature-Policy



Screenshot 7. Headers missing on [www.emrc.org.au](http://www.emrc.org.au)

Headers missing on [www.perthseasternregion.com.au](http://www.perthseasternregion.com.au)

- Strict-Transport-Security
- Content-Security-Policy
- Feature-Policy

Site:	<a href="https://www.perthseasternregion.com.au/">https://www.perthseasternregion.com.au/</a>
IP Address:	203.161.9.155
Report Time:	04 May 2019 23:23:40 UTC
Headers:	<div style="display: flex; justify-content: space-between; align-items: flex-start;"> <div style="display: flex; gap: 5px;"> <span style="background-color: #28a745; color: white; padding: 2px 5px;">✔ X-XSS-Protection</span> <span style="background-color: #28a745; color: white; padding: 2px 5px;">✔ X-Content-Type-Options</span> <span style="background-color: #28a745; color: white; padding: 2px 5px;">✔ Referrer-Policy</span> <span style="background-color: #28a745; color: white; padding: 2px 5px;">✔ X-Frame-Options</span> </div> <div style="display: flex; gap: 5px;"> <span style="background-color: #dc3545; color: white; padding: 2px 5px;">✘ Strict-Transport-Security</span> <span style="background-color: #dc3545; color: white; padding: 2px 5px;">✘ Content-Security-Policy</span> <span style="background-color: #dc3545; color: white; padding: 2px 5px;">✘ Feature-Policy</span> </div> </div>

Screenshot 8. Headers missing on [www.perthseasternregion.com.au](https://www.perthseasternregion.com.au)

Headers missing on <https://www.rgang.org.au>

- Strict-Transport-Security
- Content-Security-Policy
- Feature-Policy

Site:	<a href="https://www.rgang.org.au/">https://www.rgang.org.au/</a>
IP Address:	203.161.9.155
Report Time:	04 May 2019 23:25:21 UTC
Headers:	<div style="display: flex; justify-content: space-between; align-items: flex-start;"> <div style="display: flex; gap: 5px;"> <span style="background-color: #28a745; color: white; padding: 2px 5px;">✔ X-XSS-Protection</span> <span style="background-color: #28a745; color: white; padding: 2px 5px;">✔ X-Content-Type-Options</span> <span style="background-color: #28a745; color: white; padding: 2px 5px;">✔ Referrer-Policy</span> <span style="background-color: #28a745; color: white; padding: 2px 5px;">✔ X-Frame-Options</span> </div> <div style="display: flex; gap: 5px;"> <span style="background-color: #dc3545; color: white; padding: 2px 5px;">✘ Strict-Transport-Security</span> <span style="background-color: #dc3545; color: white; padding: 2px 5px;">✘ Content-Security-Policy</span> <span style="background-color: #dc3545; color: white; padding: 2px 5px;">✘ Feature-Policy</span> </div> </div>

Screenshot 9. Headers missing on [www.rgang.org.au](https://www.rgang.org.au)

### Management Comments

A request to address these issues was submitted to our Web Host provider with the following response:

*We recently undertook development to update the standard HTTP Headers across the CouncilConnect platform. These headers were automatically added to your website throughout this subscription period. Unfortunately we couldn't implement the Strict-Transport-Security and Content-Security-Policy headers as part of this update as these require specific testing of each website to ensure they work correctly.*

*My understanding of each of these headers is that they help mitigate vulnerabilities by ensuring the browser only loads allowed (trusted) content. By not having them you aren't introducing vulnerabilities. That being said, there is no reason not to have them set provided the website works correctly. We can add these to your websites utilising your support hours if you like?*

*The Feature-Policy header is relatively new which means that current browser support is limited. Similar to above, it provides a mechanism to ensure that certain functionality of a user's device/browser isn't inadvertently used by an untrusted source via your websites. Again we can use support to add this header to your websites, but my recommendation for now would be to leave as is and re-address in 6 to 12 months to see where browser support is.*

*The EMRC has replied to the above response requesting that the Strict-Transport-Security and Content-Security-Policy headers be updated and tested on our websites. We agreed with our provider to leave the Feature-Policy headers and re-assess in 6 to 12 months.*

## Appendix A – Detailed Testing Methodology

### A.1 External Penetration Testing

EMRC IT infrastructure was tested to determine if there are vulnerabilities in the environment that could lead to the compromise of sensitive information or the disruption of services.

#### Discovery and Information Gathering

The hosts were scanned using the Nmap tool to determine what services were exposed to the network. All 65535 ports of the TCP range were scanned as well as common UDP ports.

Each service was then probed by the tool to determine what protocol and application was being exposed. Paxon attempted to identify the type and version of the application running the service.

This provided Paxon with a comprehensive listing of potential areas of attack.

#### Vulnerability Assessment

Paxon used the Tenable Network Security's Nessus Vulnerability Scanner to scan for common security issues and misconfigurations. Nessus was configured with the latest updates from the Professional Feed.

Nessus iterated through each service in the infrastructure and ran through a database of checks for security issues. It detects the following:

- Remote code execution vulnerabilities
- Privilege escalation vulnerabilities
- Information disclosure vulnerabilities
- Unpatched servers
- Insecure services
- Misconfigurations
- Backdoors and Rogue Services
- Insufficient security protections

#### Manual Investigation of Services

The services for each host were manually researched and investigated if necessary. This involved using specific tools for the service in an attempt to find further security vulnerabilities.

- SNMP services were investigated to determine if they could be accessed without authentication or with default community strings;
- Attempts were made to login to FTP servers and SMB services using anonymous and guest accounts;
- Telnet and SSH services were accessed to determine what information was exposed and if default credentials were used;
- Web applications were visited to determine the information and functionality exposed to the network. If the web application contained a login interface, default credentials were entered. Some common web application attacks were attempted; and
- Database servers were reviewed for security misconfigurations that could lead to privilege escalation.

### Exploitation

Any potential vulnerabilities identified during the previous testing phases were manually exploited if possible. The manual exploitation of vulnerabilities ensures that vulnerabilities are genuine and assists in determining the impact and risk presented by the vulnerability.

Exploitation was conducted using the Metasploit Framework.

### Privilege Escalation

If a host was successfully exploited, Paxon used the additional access to attempt to further penetrate the security of the systems. For example, if system access gained access to user credentials or network access to additional servers, this access would then be leveraged in the testing.

The privilege escalation phase gives an understanding of the full scope of compromise should an attack occur, and allows the further identification of potential vulnerabilities.

## A.2 Web Application Penetration Testing

The main EMRC web applications were tested for security vulnerabilities that could allow an internet based attacker to expose information or deface the web site.

### Discovery

The web servers were investigated using a combination of automated tools and manual methods. This included using the Acunetix and Burp spidering functions to gain a list of pages in the application.

### Automated Web Application Scanning

Automated scanning applications were run on the web applications.

The servers were scanned using Acunetix. Acunetix is a highly regarded web application scanner which will iterate through each page in the application and identify common classes of security vulnerabilities. The types of vulnerabilities that are often picked up by Acunetix include:

- Cross Site Scripting
- SQL Injection
- XPATH Injection
- Header Injection
- File Inclusion Vulnerabilities
- Directory Traversal vulnerabilities

Another web application scanner which was also used during testing was Burp Suite. Burp Suite was used in a more targeted way to assist in the manual testing of the application.

All vulnerabilities that were identified with automated testing were verified to ensure their veracity. Vulnerabilities that were marked as false positives have not been included in this report.

### Manual Penetration Testing

Each application was then manually audited by an experienced penetration tester with the assistance of penetration testing tools such as the Burp Suite. The audit

attempted to identify not just common classes of security vulnerabilities, but also vulnerabilities specific to the application itself.

### **A3 Risk Assessment and Classification of Findings**

Each vulnerability that was identified was analysed to determine the impact, likelihood and overall risk that the vulnerability presents. The following risk factors were included in the analysis of the vulnerability:

- The business context of the vulnerability, including whether an attacker could gain access to sensitive information, or could impact the operation of the business;
- The technical context of the vulnerability, including whether an attacker could use this vulnerability to gain further access to the environment, to exploit other vulnerabilities or to access other systems;
- The technical ability required to exploit the vulnerability; and
- Any mitigating factors that could prevent or limit the successful exploitation of the vulnerability.



### **Perth**

Level 5, 160 St Georges Terrace  
Perth WA 6000

Telephone: +61 8 9476 3144

Facsimile: +61 8 9476 3188

GPO Box 2753, Perth WA 6001

### **Sydney**

Level 15, Royal Exchange Building  
56 Pitt Street, Sydney NSW 2000

Telephone: +61 2 8379 6144

### **Melbourne**

Level 27, 101 Collins Street  
Melbourne VIC 3000

Telephone: +61 3 9111 0046

Facsimile: +61 3 9111 0045

[www.paxongroup.com.au](http://www.paxongroup.com.au)

providingvalue

# AUDIT COMMITTEE MINUTES

6 JUNE 2019

REPORT ITEM 11.2 – ATTACHMENT

Eastern Metropolitan Regional  
Council  
Internal Audit Report  
Review of Financial Management  
Systems and Procedures

**PAXON** GROUP

Private Client Services  
Audit and Assurance  
Taxation

Perth • Melbourne • Sydney | May 2019 – Version 1.0  
Liability limited by a scheme approved under Professional Standards Legislation.

# Table of Contents

---

Executive Summary .....	3
1 Introduction .....	6
1.1 Background .....	6
1.2 Internal Audit Objective.....	6
2 Scope .....	7
3 Methodology.....	8
4 Inherent Limitations.....	9
5 Detailed Audit Findings.....	10
6 Efficiencies and Other Observations .....	13
Appendix A.....	14

## Executive Summary

Process	Excellent	Very Good	Satisfactory	Needs Improvement	Not Satisfactory
	★★★★★	★★★★	★★★	★★	★
	Strengths		Weaknesses		Rating
<b>Review of Financial Management Systems and Procedures</b>	<ul style="list-style-type: none"> <li>• Money owed is properly collected;</li> <li>• Receipt reports are compiled, reviewed, signed and dated by two EMRC officers to demonstrate an independent check;</li> <li>• All money collected is retained securely, banked promptly and is fully accounted for;</li> <li>• Monthly reconciliations are performed between the:                             <ul style="list-style-type: none"> <li>○ General ledger and subledgers for debtors and creditors;</li> <li>○ General ledger and asset register;</li> <li>○ General ledger cash book and bank statements; and</li> <li>○ General ledger and "Investment Summary Reports" received from the investment advisor.</li> </ul> </li> <li>• Comprehensive financial information is provided to ordinary meetings of Council;</li> <li>• Proper controls exist for incurring of liabilities and payment of creditors;</li> <li>• Payroll processes are satisfactory and well documented;</li> <li>• Adequate stock control procedures are in place; and</li> <li>• Budgets and budget reviews are undertaken with variances identified and explained.</li> </ul>		<ul style="list-style-type: none"> <li>• Instances of late review of both debtors' reconciliations and creditors' reconciliations.</li> </ul>		★★★★★

The Office of the Auditor General (OAG) performed an interim audit of the EMRC for the financial year ending 30 June 2018. The focus of the interim audit was to evaluate the EMRC's overall control environment. The OAG wrote a letter to the EMRC dated 19 September 2019, including an attached "*listing of deficiencies in internal control and other matters which were identified*" (matters identified). The attachment identified nine matters of which two have not been resolved:

Item	OAG Findings	Paxon's Assessment
1	<ul style="list-style-type: none"> <li>Late presentation of the monthly statement of financial activity.</li> </ul>	<ul style="list-style-type: none"> <li>Paxon found further instances of late presentation of the monthly statement of financial activity. Details are provided in section 5 of this report.</li> </ul>
5	<ul style="list-style-type: none"> <li>Date of review is not recorded on debtors' reconciliations.</li> </ul>	<ul style="list-style-type: none"> <li>Paxon found instances of late review of both debtors' reconciliations and creditors' reconciliations. Details are provided in section 5 of this report.</li> </ul>

Paxon is satisfied with the EMRC's control environment for the other seven matters identified:

Item	OAG Findings	Paxon's Assessment
2	<ul style="list-style-type: none"> <li>Lack of review of recipient created tax invoices (RCTI).</li> </ul>	<ul style="list-style-type: none"> <li>Paxon is satisfied with the additional controls implemented for the review of RCTIs.</li> </ul>
3	<ul style="list-style-type: none"> <li>System accepts duplicate RCTI numbers when raising invoices.</li> </ul>	<ul style="list-style-type: none"> <li>Paxon is satisfied with the additional control implemented to help prevent duplicate RCTI numbers.</li> </ul>
4	<ul style="list-style-type: none"> <li>Listing of receipts not reviewed.</li> </ul>	<ul style="list-style-type: none"> <li>Paxon is satisfied with the internal control implemented to review listings of receipts.</li> </ul>
6	<ul style="list-style-type: none"> <li>Excessive leave balances.</li> </ul>	<ul style="list-style-type: none"> <li>Paxon is satisfied with the EMRC's existing internal controls to manage excessive leave balances.</li> </ul>
7	<ul style="list-style-type: none"> <li>Unrestricted access to payroll module by non-HR/payroll officers.</li> </ul>	<ul style="list-style-type: none"> <li>Paxon found current access to the payroll module is appropriately restricted.</li> </ul>
8	<ul style="list-style-type: none"> <li>"<i>Management of Investment Policy</i>" has not been reviewed by the Council since September 2014.</li> </ul>	<ul style="list-style-type: none"> <li>Paxon found the "<i>Management of Investments Policy</i>" was reviewed by Council on 21/02/2019.</li> </ul>
9	<ul style="list-style-type: none"> <li>Long outstanding purchase orders with zero values.</li> </ul>	<ul style="list-style-type: none"> <li>Paxon is satisfied with the EMRC's existing internal controls for zero value purchase orders.</li> </ul>

Paxon reviewed the current control environment to determine whether it reduces the risks inherent to the OAG's findings to an acceptable level. Where we have noted that the current control environment to be satisfactory for this purpose, our confirmation is only over the period of our review.

## Overall Report Rating

Rating	Excellent	Very Good	Satisfactory	Needs Improvement	Not Satisfactory
		★★★★			

See Appendix A for a guide to the overall report rating scale.

# 1 Introduction

---

## 1.1 Background

Regulation 5(2)(c) of the Local Government (Financial Management) Regulations 1996 (FM Regulations) states:

*“The CEO is to undertake reviews of the appropriateness and effectiveness of the financial management systems and procedures of the local government regularly (and not less than once in every 3 financial years) and report to the local government the results of those reviews.”*

The CEO’s financial management responsibilities are set up in Regulation 5(1) of the FM Regulations which provides for the establishment of efficient systems and procedures for:

- The proper collection of all money owing to the local government;
- The safe custody and security of all money collected or held by the local government;
- The proper maintenance and security of the financial records of the local government (whether maintained in written form or by electronic or other means or process);
- To ensure proper accounting for municipal or trust revenue received or receivable, expenses paid or payable and assets and liabilities;
- To ensure proper authorisation for the incurring of liabilities and the making of payments;
- The maintenance of payroll, stock control and costing records; and
- To assist in the preparation of budgets, budget reviews, accounts and reports required by the Act or these regulations.

## 1.2 Internal Audit Objective

The objective for this internal audit is to provide assurance the CEO established efficient systems and procedures for financial management as stipulated in Regulation 5(1) of the FM Regulations.



## 2 Scope

The following process was covered in the internal audit:

Process	Key Risks
Review of Financial Management Systems and Procedures	<ul style="list-style-type: none"> <li>• Non-compliance with Regulation 5(1) of the FM Regulations.</li> </ul>

**Scope exclusions:**

The internal audit only assessed current financial management systems and procedures.

### 3 Methodology

---

Our methodology for the internal audit comprised:

- Conducting an initial meeting with management to obtain an understanding of processes and potential issues;
- Developing overview documentation of the processes including key controls by discussion with staff and review of the processes;
- Evaluating the adequacy of the controls to cover the identified risks and testing the compliance with the key controls;
- Researching the issues, weaknesses and potential improvements noted from our discussions and review of the existing processes including compliance with key controls;
- Developing appropriate recommendations for improvement for discussion with management;
- Drafting a report of findings and recommendations and obtaining formal responses from management; and
- Finalising the report and issuing it to the Director Corporate Services for distribution to the Audit Committee and relevant management.

## 4 Inherent Limitations

---

Due to the inherent limitations in any internal control structure, it is possible errors or irregularities may occur and not be detected. Further, the internal control structure, within which the control procedures that have been reviewed operate, has not been reviewed in its entirety and therefore no opinion is expressed as to the effectiveness of the greater internal control structure.

It should also be noted our internal audit was not designed to detect all weaknesses in control procedures as it was not performed continuously throughout the period subject to review.

The internal audit conclusion and any opinion expressed in this report have been formed on the above basis.

## 5 Detailed Audit Findings

Each issue detailed in this Section is rated based on the following scale:

Rating	Definition
High	<ul style="list-style-type: none"> <li>Major contravention of policies, procedures or laws, unacceptable internal controls, high risk for fraud, waste or abuse, major opportunity to improve effectiveness and efficiency, major risk identified. Immediate corrective action is required. A short-term fix may be needed prior to it being resolved properly.</li> </ul>
Medium	<ul style="list-style-type: none"> <li>Significant contravention of policies, procedures or laws, poor internal controls, significant opportunity to improve effectiveness and efficiency, significant risk identified. Corrective action is required. Need to be resolved as soon as resources can be made available, but within six months.</li> </ul>
Low	<ul style="list-style-type: none"> <li>Minor contravention of policies and procedures, weak internal controls, opportunity to improve effectiveness and efficiency, moderate risk identified. Corrective action is required. Need to be resolved within twelve months.</li> </ul>

Business Issue	Risk Rating	Implication	Recommendation	Agreed Management Action	Ownership/ Timing
<p><b>1. Statements of financial activity.</b></p> <ul style="list-style-type: none"> <li>Regulation 34(4)(a) of the Local Government (Financial Management) Regulations 1996 stipulates a statement of financial activity is to be presented at an ordinary meeting of council within two months after the end of the month to which the statement relates;</li> <li>The financial statements for September 2018 and November 2018 were only presented to ordinary meetings of Council in the third month after the end of the month to which those statements related; and</li> <li>Paxon reviewed this matter with the EMRC and was informed submission of financial statements to ordinary meetings of Council is dependent on when these meetings occur, as per Section 5.3 (2), "Ordinary meetings are to be held not more than 3 months apart." Paxon can confirm that the Council is compliant with section 5.3 (2) of the Act.</li> <li>Paxon notes that over the period of this audit, when an</li> </ul>	<p>Low</p>	<ul style="list-style-type: none"> <li>The EMRC may not comply with the stipulations of Regulation 34(4)(a) of the Local Government (Financial Management) Regulations 1996 in respect of the presentation of financial statements for September 2018 and November 2018 to an ordinary meeting of council.</li> <li>Paxon notes that this matter has been raised in the past by the previous and current external auditors, the issue relates directly to when the Council is able to call/hold meetings, as per point three and four of Business Issue 1.</li> </ul>	<ul style="list-style-type: none"> <li>The implication and recommendation are only valid if and when the ordinary Council meetings are called, and the Council does not present the financial statements at any of the ordinary monthly meetings. Paxon confirms that this has not occurred.</li> </ul>	<ul style="list-style-type: none"> <li>EMRC stated to Paxon that the presentation of the financial statements to ordinary meetings of Council: <ul style="list-style-type: none"> <li>Depends on when these meetings occur; and</li> <li>Meetings are scheduled to ensure the EMRC complies with section 5.3(2) of the Local Government Act 1995 (Act).</li> </ul> </li> <li>The Act states in section 5.3(2): "Ordinary meetings are to be held not more than 3 months apart." The EMRC has taken the view section 5.3(2) of the Act overrules Regulation 34(4)(a) of the Regulations.</li> </ul>	<p>Completed.</p>

Business Issue	Risk Rating	Implication	Recommendation	Agreed Management Action	Ownership/ Timing
<p>ordinary Council meeting is held the current month and any previous month's financial statements that have not been presented, are all presented at that meeting.</p>					
<p><b>2. Timely review of monthly reconciliations.</b></p> <ul style="list-style-type: none"> <li>• Paxon examined monthly reconciliations between the "General Ledger Detail Trial Balance" and the:               <ul style="list-style-type: none"> <li>○ "Debtors Trial Balance"; and</li> <li>○ "Creditors Trial Balance".</li> </ul> </li> <li>• Paxon found several of these reconciliations were not reviewed in a timely manner (review did not occur in the month after the month reconciled). These late reconciliations were mostly conducted two months after, but in one instance each three months after and five months after the month reconciled. This pattern of late reconciliations was evident across reconciliations performed for both debtors and creditors.</li> </ul>	<p><b>Low</b></p>	<ul style="list-style-type: none"> <li>• The late review of reconciliations delays the discovery of probable instances of errors and/or fraud.</li> </ul>	<ul style="list-style-type: none"> <li>• The EMRC should ensure reconciliations are reviewed within a reasonable period after its completion.</li> </ul>	<p>The EMRC will ensure that the verification between the <i>General Ledger Detail Trial Balance</i> and the <i>Debtors and Creditors Trial Balances</i> will be undertaken in the month immediately following each month end</p>	<p>Manager, Financial Services. Completed</p>

## 6 Efficiencies and Other Observations

Below is a summary of our other observations arising from the internal audit, which may assist you in improving the efficiency and effectiveness of your control environment. These observations are provided for your information and a formal response is not required.

Audit Area	Description
No other observations were noted.	

## Appendix A

Level	Rank	Stars	Financial Loss	Non-Financial Considerations
1	Not Satisfactory	☆	>\$1m	<ul style="list-style-type: none"> <li>Several medium rated observations or one or more high rated observations, significant risk for non-compliance with policies and regulations, serious violations of law, significant opportunities for improvement, substantiated, public embarrassment, very high multiple impacts, high widespread multiple news profile and third-party actions.</li> </ul>
2	Needs Improvement	☆☆	>\$100k<\$1m	<ul style="list-style-type: none"> <li>Several medium rated observations and no high rated observations, control weak in one or more areas, non-compliance with policies and regulations, violation of law (not serious), substantial opportunities for improvement, substantiated, public embarrassment, high impact, high news profile and third-party actions.</li> </ul>
3	Satisfactory	☆☆☆	>\$50k<\$100k	<ul style="list-style-type: none"> <li>Many low rated observations and/or few medium rated observations, several low rated violations of policy, minor violations of regulations, no violations of law, moderate opportunities for improvement, substantiated, public embarrassment, moderate impact and moderate news profile.</li> </ul>
4	Very Good	☆☆☆☆	>\$10k<\$50k	<ul style="list-style-type: none"> <li>Several low rated observations and/or one or two medium rated observations, minor contraventions of policies and procedures, no violations of law, minor opportunities for improvement, substantiated, low impact and low news profile.</li> </ul>
5	Excellent	☆☆☆☆☆	<10k	<ul style="list-style-type: none"> <li>Few low rated observations, no internal control weaknesses noted, good adherence to laws, regulations and policies, excellent control environment, unsubstantiated, low impact, low profile or no news item.</li> </ul>



### **Perth**

Level 5, 160 St Georges Terrace  
Perth Western Australia 6000  
Telephone: +61 8 9476 3144  
Facsimile: +61 8 9476 3188  
GPO Box 2753, Perth WA 6001

### **Melbourne**

Level 27, 101 Collins Street  
Melbourne VIC 3000  
Telephone: +61 3 9111 0046  
Facsimile: +61 3 9111 0045

### **Sydney**

Level 57, MLC Centre, Martin Place  
Sydney NSW 2000  
Telephone: +61 2 8355 3690  
Facsimile: +61 2 8355 3689

[www.paxongroup.com.au](http://www.paxongroup.com.au)

providingvalue