Minutes

Audit, Risk and Improvement Committee Meeting

25 March 2026

Shire of Victoria Plains
Council Chambers, Calingiri
AND
via E-Meeting Protocol

Commencing – 12:01 PM

DISCLAIMER:

The recommendations contained in this document are officers' recommendations only and should not be acted upon until Council has resolved to adopt those recommendations.

The resolutions of Council should be confirmed by perusing the minutes of the Council meeting at which these recommendations were considered. Resolutions are not considered final until the minutes of the meeting are confirmed or advised in writing by the CEO or authorised person.

Members of the public should also note that they act at their own risk if they enact any resolution prior to receiving official written notification of Council's decision.

Recording of Meeting

Members of the public are advised that meetings of Council are audio recorded to assist with ensuring an accurate record of the meeting is provided for the formal minutes of the meeting. In terms of the Privacy Act 1998 this may involve the recording of personal information provided at the meeting. The provision of any information that is recorded is voluntary, however if any person does not wish to be recorded they should not address or request to address the meeting. By remaining in this meeting, you consent to the recording of the meeting.

You are not permitted to record this meeting with any recording device, unless you have the express authorisation of the Council of the Shire of Victoria Plains.

E – Disclaimer

It is the Presiding Member's responsibility to preserve order in the meeting and this can be more difficult in an eMeeting. Therefore, each Council Member must consistently and respectfully follow the Local Government's Meeting Procedures Local Law, any additional eMeeting guidance provided by the Local Government and support the Presiding Member in their conduct of the eMeeting.

The pace of an eMeeting should be slow and orderly. The following practices will help avoid confusion and support effective eMeetings:

Speak clearly and slowly, as connections may be distorted or delayed;

Always state your name to indicate to the Presiding Member that you wish to speak. Restate your name if the Presiding Member has not heard you at first;

In debate, only speak after the Presiding Member has acknowledged you. Then state your name, so that others know who is speaking;

Follow the Presiding Member's directions and rulings;

If you are unclear about what is happening in an eMeeting, immediately state your name to draw the Presiding Member's attention and enable you to then seek clarification from the Presiding Member.

Avoid looking for opportunities to call Points of Order; instead, politely and respectfully gain the Presiding Member's attention and explain any deviation from your Meeting Procedures, the Local Government Act or any other relevant matter.

Commonly used abbreviations	
AAS / AASB	Australian Accounting Standard / Australian Accounting Standards Board
BF Act	Bush Fire Act 1954
BFB	Bush fire brigade
CEO	Chief Executive Officer
CDO	Community Development Officer
DBCA	Dept of Biodiversity, Conservation and Attractions
DFES	Dept of Fire and Emergency Services
DPLH	Dept of Planning, Lands and Heritage
DWER	Dept of Water and Environmental Regulation
EHO	Environmental Health Officer
EFT	Electronic Funds Transfer
FAM	Finance and Administration Manager
JSCDL	Parliamentary Joint Standing Committee on Delegated Legislation
LEMA	Local Emergency Management Arrangements
LEMC	Local Emergency Management Committee
LG Act	Local Government Act 1995
LGGC	WA Local Government Grant Commission
LPP	Local Planning Policy
LPS	Local Planning Scheme
MOU	Memorandum of Understanding
MRWA	Main Roads WA
NNTT	National Native Title Tribunal
OAG	Office of Auditor General
OCM	Ordinary Council Meeting
PTA	Public Transport Authority
RRG	Regional Roads Group
RTR	Roads to Recovery
SAT	State Administrative Tribunal
SEMC	State Emergency Management Committee
SGC	Superannuation Guarantee Contribution
SJAA	St John Ambulance Association
SWALSC	South West Aboriginal Land and Sea Council
WAEC	WA Electoral Commission
WALGA	WA Local Government Association
WSM	Works and Services Manager
WSFN	Wheatbelt Secondary Freight Network
EPA	Environmental Protection Authority
DPIRD	Department of Primary Industries and Regional Development
HCWA	Heritage Council of Western Australia
WAPC	Western Australian Planning Commission
WDC	Wheatbelt Development Commission

CONTENTS

AGENDA

Audit, Risk and Improvement Committee Meeting of the Victoria Plains Shire Council Held in the Shire of Victoria Plains, Council Chambers, Calingiri, AND, via E-Meeting Protocol on 25 March 2026 commencing at 12:01 PM

1 DECLARATION OF OPENING

1.1 Opening

The Meeting was declared open by the Presiding Member at 12 01PM

1.2 Announcements by Chairperson

The Chairperson reminded Elected Members that the meeting was being recorded for the purposes of Minute Taking and uploading of the recording to the Shire Website for public viewing and the meeting will be run in accordance with the Shire's Meeting Procedures Law 2018

2 REMOTE ATTENDANCE BY ELECTED MEMBERS

THAT:

Under regulation 14C (2)(b) of the Admin Regulations, the Shire President can approve Elected Member attendance by electronic means;

In doing so, under r.14C (5) the Shire President must have regard as to whether the location that the Elected Member intends to attend the meeting, and the equipment intended to be used to attend the meeting, are suitable;

Electronic means includes, as per r.14CA(2) by telephone or video conference;

Suitable equipment would include an electronic device that can hold a Teams meeting, and perhaps, the use of headphones;

In accordance with r.14CA (5) the Elected Member must declare that they are able to maintain confidentiality during the meeting. Under r.14CA(7), the declaration by the Elected Member is recorded in the minutes of the meeting;

Summarily, according to Departmental guidance, a suitable location is one that is quiet and private e.g. a private room in your house. If there are other people at the location at the time of the meeting, an Elected Member may be required to close a door and wear headphones.

Approval to Attend and Declaration of Confidentiality

Mr **DAVID LOVELOCK** has **APPROVAL** to attend the Audit, Risk and Improvement Committee Meeting held on 25 March 2006 via teleconference.

3 RECORD OF ATTENDANCE

Members present	Cr D Lovelock – Independent Chair via teleconference. Cr P Bantock Cr S Woods Cr E Williams Cr N Smith (Observer)
Staff attending	CEO- Mr S Fletcher DCEO – Mr C Ashe Council Support Officer – Mrs J Klobas
Apologies	N/A
Approved leave of absence	N/A
Visitors	Nil
Members of the public	Nil

4 DISCLOSURE OF INTEREST

Refer – Local Government Act, Regulations, Code of Conduct, and Declaration Forms in Councillor folders.

Type Item Person / Details

Nil

5 PUBLIC QUESTION TIME

Refer – Local Government Act, Regulations, Local Law and Submission Form & Guidelines circulated.

5.1 Public Questions with Notice

Nil

5.2 Public Question Without Notice

Nil

6 CONFIRMATION OF MINUTES

Officer Recommendation / Committee Resolution ARIC 2603-01

Moved: Cr E Williams **Seconded: Cr P Bantock**

That the of the Audit Committee Meeting held 26 November 2026 as circulated, be **CONFIRMED** as a true and **MINUTES** correct record with amendment to Item 7.10 “Seconded N Williams” to be amended to read “Seconded E Williams”.

Resolution 32– amend “INTO standing orders” to read “MOVE OUT of standing orders”.

CARRIED BY UNANIMOUS DECISION OF COMMITTEE

Voted For: Mr D Lovelock, Cr P Bantock, Cr E Williams and Cr N Smith

Voted Against: Nil

7 REPORTS REQUIRING DECISION

7.3 Internal Audits

7.3.1 Internal Audits – Regulation 17 Internal Controls Review – Credit Card Policy

File Reference	
Report Date	17 March 2026
Applicant/Proponent	Audit, Risk and Improvement Committee
Officer Disclosure of Interest	Nil
Previous Meeting Reference	Nil
Prepared by	Colin Ashe – Deputy Chief Executive Officer
Senior Officer	Sean Fletcher – Chief Executive Officer
Authorised by	Sean Fletcher – Chief Executive Officer
Attachments	1. Financial Management Policy 3.3 Credit Cards

PURPOSE

For the Audit, Risk and Improvement Committee (ARIC) to endorse amendments to Financial Management policy 3.3 Credit Cards – Including store, fuel and debit cards as part of the Internal Controls Review.

BACKGROUND

The AIRC endorsed the Internal Controls Review in Nov 25 and part of this outcome was a review of the shires Credit Card policy. This was also in response to the AOG report and subsequent recommendations in Jun 24.

Broadly the shires extant policy was compliant and in line with the recommendations but needed clearer direction on allowable expenditure and tighter controls on credit card transactions made in error (private use).

COMMENT

Previously policy 3.3 Credit Cards – Including store, fuel and debit cards included:

8. Use of Cards

Corporate Credit Cards or Debit Cards may be used to purchase fuel products upon approval of the CEO and provided it can be demonstrated as being used in a shire asset upon request.

Which has been amended to:

8. Use of Cards

Corporate Credit Cards or Debit Cards may be used to purchase low value items where it is more efficient for on-line purchases of low value or is the only acceptable means to secure the service (e.g. travel booking of flights and accommodation). The following provides broad guidance on acceptable purchases using a Corporate Credit Card less than $500 per transaction:

a) general retail (e.g. industrial and construction supplies, hardware and equipment, and office supplies and printing)

b) food and drink purchases

c) government services (e.g. postal services, licenses, registrations and permits)

d) information technology and digital goods

e) vehicle fuel, parts and services

Exceptions to the indicative $500 threshold

Some transactions by will exceed the threshold due to the nature and requirement to use a corporate credit card because of efficiencies or a vendor account has not / cannot be established. These include:

a) travel and accommodation

b) training and development

c) community events

Where this is required, the established approval forms are to be completed and signed by the CEO or delegate.

Personal / Private Purchases in error

This policy prohibits private or personal purchases by cardholders but recognises there will be occasions where it may be used in error. This may be because the cardholder also has a personal credit card with the same bank or simply transacted in error. Where this occurs the cardholder is to:

a) immediately identify the transactions and advise the CEO or Deputy CEO.

b) Provide a short email of the transactions and why this occurred.

c) Repay the amount either through a shire invoice or over the counter transaction.

The finance team is to monitor these errors and should a pattern emerge, this is to be raised to the CEO.

It should be noted clause 4b in the policy prohibits private use of the corporate credit card. The above provides direction where it is used in error.

CONSULTATION

Applicable Finance Personnel

Mr Sean Fletcher, Chief Executive Officer.

STATUTORY CONTEXT

Regulation 17 of the Local Government (Audit) Regulations 1996:

(1) The CEO is to review the appropriateness and effectiveness of a local government's systems and procedures in relation to:

(a) risk management; and

(b) internal control; and

(c) legislative compliance.

(2) The review may relate to any or all of the matters referred to in sub regulation (1)(a), (b) and (c), but each of those matters is to be the subject of a review not less than once in every 3 financial years.

(3) The CEO is to report to the audit committee the results of that review.

CORPORATE CONTEXT

Strategic Business Plan/Corporate Business Plan

STRATEGIC PRIORITIES	WE KNOW WE ARE SUCCEEDING WHEN
4. CIVIC LEADERSHIP	

4.3 Proactive and well governed Shire	External audits and reviews confirm compliance
	We have sound financial management policies and attract external funding to help achieve our goals
	Councillors attend training and feel supported in their role
	Council is supported by a skilled team

Strategic Priority 4.3 of internal audits and findings is essential to ensure compliance, reduce risk and highlight areas for improvement.

Delegation

Nil

Policy Implications

Section 3 – Financial Management will be updated accordingly upon final approval by council.

Other Corporate Document

Nil

Risk Analysis

Consequence	Consequence Rating:	Likelihood Rating:	Risk Rating	Risk Acceptance/ Controls	Mitigation and Outcome
Compliance	Major (4) Non-compliance results in termination of services or imposed penalties to Shire/Officers	Possible (3) The event should occur at some time	High (12)	Senior Management Team / CEO Risk acceptable with excellent controls, managed by senior management / executive and subject to monthly monitoring	Ensuring any recommendations from the audit are implemented will ensure that the residual risk is low.

FINANCIAL IMPLICATIONS

Nil

VOTING REQUIREMENTS

Simple Majority

Officer Recommendation / Committee Resolution ARIC 2603-02

Moved: Cr P Bantock **Seconded: Cr N Smith**

That the Audit, Risk and Improvement Committee in accordance with Regulation 17(3) of the *Local Government (Audit) Regulations 1996* **RECOMMENDS** to council to endorse the amendment to the Financial Management Policy section 3.3 Credit Cards – Including store, fuel and debit cards as tabled.

CARRIED BY UNANIMOUS DECISION OF COMMITTEE

Voted For: Mr D Lovelock, Cr P Bantock, Cr E Williams and Cr N Smith
Voted Against: Nil

3.3: Credit Cards – Including store, fuel and debit cards

Responsible Areas	Finance and Administration
Responsible Officer	Deputy CEO
Affected Staff	CEO, DCEO, Coordinator Financial Services, MWS, CESM

Objective

To ensure the proper management of corporate credit, store, fuel and debit cards.

Scope

Local Governments are required to ensure that they have effective and accountable systems in place to safeguard the Shire's financial resources. This includes the development of proper systems to authorise, verify and record the proper use of credit cards.

Policy

1. Schedules adopted

The following Policy Schedules are adopted, and form part of this Statement –

- Sch.3.3(a) – Corporate, Store, Fuel and Debit Cards – Cardholder Agreement
- Sch.3.3(b) – Reconciliation of Credit Cards, Store Cards and Debit Cards
- Sch.3.3(c) – Purchasing using Credit Cards

2. Authority

All cardholders must have either the authority or delegated authority to commit Shire to expenditure

3. Personal Use

a) Providing Schedule 3.3(c) – Purchasing using Credit Cards is complied with, personnel may use a Corporate Credit Card for purchases.

b) Cardholders still have full responsibility for the use of the card and must ensure 3.3 (c) is complied with. Breaches of this condition will result in the Shire being liable for any unauthorised transactions and may result in disciplinary action, including but not limited to, repayment of the purchase personally.

4. Cardholder Responsibilities

a) Ensure each card is maintained in a secure manner and guarded against improper use.
b) Cards are to be used only for Shire official activities, there is no approval for any private use.
c) All documentation regarding a card transaction is to be retained by the cardholder and produced as part of the reconciliation procedure.
d) Card limits are not to be exceeded.
e) Purchases on any card are to be made in accordance with Shire of Victoria Plains – Purchasing Policy.
f) Reconciliation is to be completed within 7 days of the date of the card statement being issued.
g) All cards are to be returned to the CEO on or before the employee's termination date with a full acquittal of expenses.
h) All cardholder responsibilities as outlined by the card provider.
i) Cash advances or withdrawals are not permitted.

5. Cardholder Agreement
a) The Cardholder Agreement is contained in Policy Schedule 3.3(a).
b) Failure to comply with any of these requirements could result in the card being withdrawn from the employee.
c) In the event of loss or theft through negligence or failure to comply with the Shire's Policy any liability arising may be passed on to the cardholder.

6. Consequences of Non-Compliance
Failure to comply with the Delegations, Policy or Procedures may result in disciplinary action up to and including termination of employment.

APPLICATION

7. Card Reconciliation Procedures
a) Card statement accounts will be issued to the relevant cardholder who will, within 7 days, acquit the transactions on the account. A template is attached to this policy identifying the reconciliation requirements.
b) Transactions will be supported by a GST invoice stating the type of goods purchased, amount of goods purchased and the price paid for the goods. The receipt shall meet the requirements of the *Goods and Services Tax Act 1999* to enable a GST rebate to be applied.
c) Transactions shall be accompanied by a job number for costing purposes.
d) If no supporting documentation is available the cardholder will provide a declaration detailing the nature of the expense and must state on that declaration all expenditure is of a business nature'. Approval of this expense is referred to the CEO for a decision.
e) Should approval of expenses be denied by the CEO recovery of the expense shall be met by the cardholder.
f) The cardholder shall sign and date the card statement with supporting documentation attached stating all expenditure is of a business nature.
g) A monthly report and reconciliation of all card transactions will be included in the accounts for payment report presented to Council.

8. Use of Cards
Corporate Credit Cards or Debit Cards may be used to purchase low value items where it is more efficient for on-line purchases of low value or is the only acceptable means to secure the service (e.g. travel booking of flights and accommodation). The following provides broad guidance on acceptable purchases using a Corporate Credit Card less than $500 per transaction:

a) general retail (e.g. industrial and construction supplies, hardware and equipment, and office supplies and printing)
b) food and drink purchases
c) government services (e.g. postal services, licenses, registrations and permits)
d) information technology and digital goods
e) vehicle fuel, parts and services
f) Incidentals

Exceptions to the indicative $500 threshold

Some transactions by will exceed the threshold due to the nature and requirement to use a corporate credit card because of efficiencies or a vendor account has not / cannot be established. These include:

a) travel and accommodation
b) training and development

c) community events

Where this is required, the established approval forms are to be completed and signed by the CEO or delegate.

Personal / Private Purchases in error

This policy prohibits private or personal purchases by cardholders but recognises there will be occaisions where it may be used in error. This may be because the cardholder also has a personal credit card with the same bank or simply transacted in error. Where this occurs the cardholder is to:

a) immediately identify the transactions and advise the CEO or Deputy CEO.
b) Provide a short email of the transactions and why this occurred.
c) Repay the amount either through a shire invoice or over the counter transaction.

The finance team is to monitor these errors and should a pattern emerge, this is to be raised to the CEO or Deputy CEO.

On Line Accounts

Personal on-line accounts (Amazon, E-Bay, Temu etc) are not be used for Shire purchases unless approved by the CEO or Deputy CEO to ensure purity of the transactions and minimise risk of fraud or the perception of fraud. A Shire of Victoria Plains account is to be established and is to include contact details (e.g. shire delivery address, contact number and email) where these vendors are used.

9. Disputed Transactions
   a) The Shire is responsible for paying all accounts on the monthly card statement and the bank processes a direct debit from Council's operating bank account for such.
   b) When a Cardholder believes that charges are incorrect they should first contact the supplier to determine the causes of the discrepancy and if necessary the Creditors Officer will notify the bank in writing.
   c) Any amounts in dispute must be highlighted on the copy of the Cardholders statement and a copy of the written notification to the bank attached.

10. Cancelled Cards
    Cancellation of a Card may be necessary where the:

    a) Cardholder changes job function within Council
    b) Cardholder terminates employment with Council
    c) Council terminates employment with the Cardholder
    d) Card is no longer required
    e) Cardholder has not adhered to set procedures
    f) Misuse of the Card.

11. Review of Card Use
    All receipts and documentation will be reviewed and any expenses that do not appear to represent fair and reasonable business expenses shall be referred to the CEO for a decision.

12. Procedures for Lost, Stolen and Damaged Cards
    a) The loss or theft of a credit card must be immediately reported by the cardholder to the card provider regardless of the time or day discovered. The cardholder must also formally advise the Manager Finance & Administration of the loss or theft without delay.

b) Ad·i ce o.f a d!amaged carrel is to be provided!to the M!anager IFina:nce & Ad'mi11istration who willl arrange a ffiipl!acement.

113. Additio11al Cardholders

Th.e CEO is the primary cardholder forUle Shire and may d'el'.egate ad'dition carreloldern within the Shire,'s appKl'lled total credit limit, and in aa::ordance with the Delegation adopted by Council

IRE:FERIEINCIES

Fiuel carolstatements have alllrelevant details provided. Other than certifi:cation by th.e cardhold'.er, no further procedures are req,uired!.

Sch.edu e 3.s(a} - Corporate, store, **Fuel** and Debit Cards - Gardholder Agreement

Coodlitions of use of Corporate Cred'it, store, **Fuel** a:nd Debit Gardis -

1. Einsme all carols are maintained in a secure manner andlguarded agrainst improperuse.
2. Allicards are to !le used 011ly for Shire of Victoria Plains offici activities as presoril!J.ed by the OEO, there iiS110 awrovallgiven for any private use.
3. Einsure no one els.eother tha:n the authorisedicardholder uses a:ny carolissued.
4. Allid'.ocumentatiolliregarding a card transaction is to be retai11.edlby Ul.ecardhold:er and produced oo part of the reconciliation proceclme.
5. Card limits are not to be exceed'.ed.
6. Observe alllcardhol'.der responsibilities as outllned by the card provider.
7. Rurchases on all cards are to be mad'.e in aooord!ance withl Shire of Victmi.;iPlajns R1.m:hasi11g Policy.
8. Reconc◆i.;ition is to be c0ili1pl'.eted within 7 days of th.e date of card statement being issued on the sup,pli.edltemplate.
9. Transactions \I\\ill be supported l)y a GST invoice stating the type of goods purchased(amount of gooos purohlased and thle pricepaid for tlle goodis. Thle reoeipt shall meet the requirements of the *Goods* and *Sewfoes Tax Act 1999* to e11a lie a GST rebate to be a;ppl ed.

110.Transactions shal be acr:ompan·sa by a Jol' nurnbcer, cost oentre a:nd element tYipe for costingl purposes.

11. If lno supporting dooumentation is avail!able t!he cardllol'.der will provide a deolaration detailing the narure of the expense and must state Olkhat d'.ecl!aration alll e)!pendi1ure is o1ia business nature. Ap;pm1-Jal of ttlis exl}ense•is referred to the CIEO tor a decfsion.

112.Should!appro\l'al of expenses be d'.enied!by ttl.e CEO recovery o.fthe e•xpense shal he met by ttl.e• cardhlol'.der.

n.Th.e cardholder shall sign a:nd date eaoh card statement ·lh supporting doournentation attach.ed stating alllexpend'iture iisof 1li Imsinessnature.

14. Lost or stol'en cards sllalllbe ffiiported irnmedi.;iteliyto the card provider and a written aooount of th.e oirclllmstances shall be IPKIVided to the CEOon the nel<it wmting d!ay_

15. Allicards are to !le retlllmed to tll.e•CEO Olli**or** I)etore the empl'.oyee's tem1inatirm d!ate with a rulllacquittal of e)!penses.

ACKNOWLEDGEMENT OF RECEIPT OF CREDIT, STORE, FUEL AND DEBIT CARD/S

a) I have read this policy and understand my responsibilities which include the requirement that the card/s can only be used for official business only and acknowledge receipt of the following cards noted below.
b) I acknowledge that failure to comply with the Delegations or Policies may result in disciplinary action up to and including termination of employment.

Card type Credit, Debit, Store, Fuel	Organisation	Number

Name and Signature _____ Date _____

– End of Schedule

Schedule 3.3(b) – Reconciliation of Credit Cards, Store Cards and Debit Cards

Standard reconciliation format –

Card Reconciliation

CARD -	Type		Number		Cardholder		
Item No.	**Chq/EFT**	**Date**	**Supplier**	**Purchases**	**Amount**	**Type**	**Funding**

Card Total $

– End of Schedule

Schedule 3.3(c) – Purchasing using Credit Cards

HOW I MAKE A PURCHASE

- Use this form to seek prior approval from the card holder before purchasing goods and services using a Corporate Credit Card.
- Obtain prices for purchases, complete this form and submit to the credit card holder for authorisation.
- Once authorised, complete the purchase and attach the receipt/tax invoice and any other supporting documentation to this form and submit to the Finance department.

Request is compliant with Delegation 3.1 and Policy 3.1			
Requested by		Tax invoice or supporting documentation attached	
Signature		Date	

Supplier		
GL Account / Job No	**Description of Goods**	**AMOUNT** (incl GST)
	GST Code	
	TOTAL	

REASON FOR USING CREDIT CARD FOR THE PURCHASE

AUTHORISED

Cardholder positon	Cardholder Name	Cardholder Signature	Date

GST CODES

	Income and purchases subject to GST		Free income and purchase
	No report		Input tax

– End of Schedule

Office Use Only				
Relevant delegations	3.3			
Initial Council adoption	Date	21 June 2018	Resolution #	
Last reviewed	Date	28 February 2023	Resolution #	
Last reviewed	Date	13 January 2026	Resolution #	
Next review due	Date			

7.4 Financial Reporting

7.4.1 Budget Review as at 28 February 2026

File Reference	
Report Date	17 March 2026
Applicant/Proponent	Audit, Risk and Improvement Committee
Officer Disclosure of Interest	Nil
Previous Meeting Reference	Nil
Prepared by	Colin Ashe – Deputy Chief Executive Officer
Senior Officer	Sean Fletcher – Chief Executive Officer
Authorised by	Sean Fletcher – Chief Executive Officer
Attachments	1. 25-26 Budget Review No.2

PURPOSE

To conduct the second budget review for 2025-26 based on Feb 26 financial statements for the Audit, Risk and Improvement Committee (ARIC) endorsement.

BACKGROUND

Council approved the 2025-26 budget that forecast a deficit of ($290,513) at 30 Jun 26 and this was based on an estimated actual closing balance deficit of ($925,728) from 24-25.

In Nov 25 Budget Review No.1 was completed and further adjustment of $73,260 was made as follows:

Budget Amendments

Amendments to original budget since budget adoption - Surplus/ (Deficit)

Description	Council Resolution	Adoption Date	Increase in Available Cash	Decrease in Available Cash	Amended Budget Running Balance
			$	$	$
Forecast Opening Surplus/(Deficit)					(290,513)
Budget Review No.1	OCM 2511-05	26/11/2025		(73,260)	(363,773)
Net Changes			-	(73,260)	(363,773)

Local Government (Financial Management) Regulations 1996; regulation 33A requires a budget review to be undertaken between 01 Jan and the last day in Feb of the financial year and the financial performance review cannot be any earlier than 31 Dec.

Budget Review No. 1 did not meet this required timeframe but is considered to be good governance to regularly review the budget versus actuals. Budget Review No. 2 does fall within the required timeframe so along with good governance, also meets the statutory requirements.

COMMENT

25-26 Budget Review No.2:

Management has made limited progress in addressing the budget deficit. Although savings were realised in the capital program, these were outweighed by higher-than-expected operating

expenditure.

This has equated to $110,343 in further savings from budget review No.1 but the deficit is still forecast to be $253,431. In addition, increased fuel costs and a risk in reduced grants commission payments have not been factored into this forecast and therefore the 30 Jun 26 is likely to be worse.

Attachment 1 provides the full budget review adjustment and can be summarised excluding loan funding and Grader purchases which offset each other:

- $106,689 reduction in revenue primarily unsuccessful Disaster Ready grant (offset by capital expenditure).
- $42,499 reduction in operating expenditure which on the surface appears to be a good result but is skewed by over expenditure in other activities.
- $174,533 in overall capital expenditure reductions, primarily due to budgeted Disaster Ready activities which will not go ahead because of the unsuccessful grants.
- $750,000 of loan funding revenue which will be offset by $750,000 capital expenditure on 2 Graders.

Management will continue to closely monitor the financial outcomes to endeavour to find further savings and offsets but at this stage, it is unlikely the shire will return to a surplus position at EOFY.

CONSULTATION

Mr Sean Fletcher, Chief Executive Officer

Ms Glenn Deocampo, Coordinator Financial Services

Mrs Zoe Clayton, Chief Financial Officer

STATUTORY CONTEXT

Local Government (Financial Management) Regulations 1996; regulation 33A budget review includes:

1. Between 1 January and the last day of February in each financial year a local government is to carry out a review of its annual budget for that year.

2A. The review of an annual budget for a financial year must —

(a) consider the local government's financial performance in the period beginning on 1 July and ending no earlier than 31 December in that financial year;

2. The review of an annual budget for a financial year must be submitted to the council on or before 31 March in that financial year.

3. A council is to consider a review submitted to it and is to determine* whether or not to adopt the review, any parts of the review or any recommendations made in the review.

CORPORATE CONTEXT

Audit, Risk and Improvement Committee Terms of Reference.

Strategic Business Plan/Corporate Business Plan

STRATEGIC PRIORITIES	WE KNOW WE ARE SUCCEEDING WHEN

4. CIVIC LEADERSHIP	
4.3 Proactive and well governed Shire	External audits and reviews confirm compliance
	We have sound financial management policies and attract external funding to help achieve our goals
	Council is supported by a skilled team

Strategic Priority 4.3 - Management considers budget reviews in addition to statutory requirements as good governance allowing early intervention to identify any significant issues.

Delegation

Nil

Policy Implications

Section 3 – Financial Management

Other Corporate Document

Nil

Risk Analysis

Consequence	Consequence Rating:	Likelihood Rating:	Risk Rating	Risk Acceptance/ Controls	Mitigation and Outcome
Compliance	Moderate (3) Short term non-compliance but with significant regulatory requirements imposed	Unlikely (2) The event could occur at some time	Moderate (6)	Operational Manager Risk acceptable with adequate controls, managed by specific procedures and subject to semi-annual monitoring	Ensuring frequent budget reviews in excess of statutory requirements will ensure that the residual risk is low.

FINANCIAL IMPLICATIONS

Amendments to the budget will provide better forecasting and therefore management of councils finances.

VOTING REQUIREMENTS

Simple Majority

Officer Recommendation / Committee Recommendation ARIC 202603-03

Moved: Cr Bantock **Seconded: Cr E Williams**

That the Audit, Risk and Improvement Committee recommends that council **ADOPT** the budget review No.2 and budget amendments and set out in attachment 1.

CARRIED BY UNANIMOUS DECISION OF COMMITTEE

Voted For: Mr D Lovelock, Cr P Bantock, Cr E Williams and Cr N Smith
Voted Against: Nil

Shire of Victoria Plains
Significant Variances to Budget
For the Period Ending 28 February 2026

Schedule	Account Description	Annual Budget	YTD Actual	Revised Forecast	Variance
	Revised Budget Surpus / (Deficit) from Review No.1				**(363,773)**
INCOME					
5	**Disaster Ready Generators** Unsuccessful Grant	55,000	-	-	(55,000)
5	**Disaster Ready Bores** Unsuccessful Grant	55,000	-	-	(55,000)
	WSFN Funding				
	Legacy adjustment 2020-21 contingent liabilities	-	8,694	8,694	8,694
12	**Roads to Recovery Funding** Budgeting error in C/F	906,448	915,690	915,690	9,242
12	**Proceeds from Sale of Plant**				
	Ford Everest (DCEO)	65,000	50,276	50,276	(14,724)
	Caterpillar Excavator	30,000	39,197	39,197	9,197
	Ride on Mover	5,000	16,816	16,816	11,816
	Ford Wildtrak (MWS)	65,000	44,086	44,086	(20,914)
	volitile auction sale prices				
12	**Loan Funding** Plant Replacement Ph 2 - Grader x 2	-		750,000	750,000
	Net Income Variations				**643,311**
EXPENDITURE					
4	**Conference Costs** Leaders Summit CBR, National Roads Bendigo	16,000	18,710	24,710	(8,710)
4	**Consultants**				
	Reduction in requirements				
	- Revaluation	15,000	-	-	15,000
	- Precinct Plan	40,000	-	10,000	30,000
4	**Legal Fees** allocation for Kennedys not required	10,000	-	-	10,000
5	**Ranger Services** Additional Visits	26,400	36,382	58,212	(31,812)
10	**Contractors**				
	Reduced Town Planning Requirements	72,520	22,241	50,000	22,520
4	**Miscellaneous Expenses** EBA Payment missed in budget	1,000	4,844	5,500	(4,500)
14	**Parts and Repairs**	255,000	237,630	290,000	(35,000)

Shire of Victoria Plains
Significant Variances to Budget
For the Period Ending 28 February 2026

Schedule	Account Description	Annual Budget	YTD Actual	Revised Forecast	Variance
13	**Economic Development Officer**	75,000	17,952	30,000	45,000
	Contractor not replaced				
	Net Expenditure Variations				**42,499**
	CAPITAL				
	Yerecoin Sth East Rd	700,000	783,412	783,412	(83,412)
	Bolgart East Rd Seal - renewal	57,250	77,797	77,797	(20,547)
	Poincare St - Seal renewal	60,000	48,437	48,437	11,563
	Cavell St and Haig Intersection	10,000	12,427	12,427	(2,427)
	Calingiri New Norcia Rd - reconstruction	79,198	3,823	3,823	75,375
	Disaster Ready Generators	101,560	-	-	101,560
	Disaster Ready Bores	78,440	-	-	78,440
	DCEO Vehicle (VP00)	75,000	69,550	69,550	5,450
	Service Truck VP49	120,000	112,971	112,971	7,029
	Depot Utility (2WD)	30,000	33,419	33,419	(3,419)
	Bore Development - Goudge / Parker Rd	9,800	4,879	4,879	4,921
	Graders x 2	-	-	750,000	(750,000)
	Net Capital Variations				**(575,467)**
	Revised Surplus / (Deficit)				**(253,431)**

7.7.1 COMPLIANCE AUDIT RETURN 2025

File Reference	
Report Date	17 March 2026
Applicant/Proponent	Department of Local Government, Sport and Cultural Industries
Officer Disclosure of Interest	Nil
Previous Meeting Reference	Nil
Prepared by	Candice Watson – PA to the CEO
Senior Officer	Sean Fletcher – Chief Executive Officer
Authorised by	Sean Fletcher – Chief Executive Officer
Attachments	Nil

Purpose

As per the Local Government (Audit) Regulations, the Audit, Risk and Improvement Committee is required to review the Compliance Audit Return 2025 and present the CAR to Council for adoption.

Background

The CAR is an annual statutory self-assessment completed by all Western Australian local governments to review compliance with specified legislative requirements for the calendar year (1 January – 31 December).

Under section 7.13(1)(i) of the *Local Government Act 1995* and Regulation 14 of the *Local Government (Audit) Regulations 1996*, local governments must carry out a compliance audit each year and prepare a return in the approved form. The ARIC must review the completed CAR and report results to Council.

For the 2025 CAR period, the deadline for submission to the Local Government Inspector is 30 September 2026 (extended from the usual March deadline).

Comment

Regulation 13 – Prescribed Statutory Requirements

What Regulation 13 Entails

Regulation 13 of the *Local Government (Audit) Regulations 1996* prescribes the statutory requirements against which compliance is audited each year. It defines the legislative provisions (both from the *Local Government Act 1995* and other written laws/regulations) that must be assessed in the CAR.

Changes Effective 1 January 2026

With the commencement of the Local Government Inspectorate and amendments to the Audit Regulations from 1 January 2026, Regulation 13 has been updated. This may include changes to the categories and specific legislative references used in the CAR.

In addition, Regulation 15A now allows the Local Government Inspector to determine or limit which statutory requirements are included in the CAR, with further guidance expected to be released by 31 March 2026.

Implications for the 2025 CAR

The updated Regulation 13 may alter some of the compliance categories and questions included in the 2025 CAR format compared to prior years (e.g., disclosure of interests, procurement/tendering, delegations, finance, employees, integrated planning).

Once the Inspector issues the updated CAR form reflecting these changes, the Shire will complete the audit accordingly. The ARIC's role remains to review the completed return before Council acknowledges and adopts it.

Consultation

Mr Sean Fletcher, Chief Executive Officer

Statutory Context

Nil

Corporate Context

Nil

Strategic Community Plan and Corporate Business Plan

4. CIVIC LEADERSHIP	
4.3 Proactive and well governed Shire	External audits and reviews confirm compliance

The CAR is a key audit tool required under the Act and the regulations regarding good governance.

Delegation

Nil

Policy Implications

Where necessary, compliance has occurred with Shire Policies.

Other Corporate Document

Nil

Risk Analysis

Consequence	Consequence Rating:	Likelihood Rating:	Risk Rating	Risk Acceptance/ Controls	Mitigation and Outcome
Non - compliance Not conducting CAR by deadline. Not addressing actions of non-compliance	Extreme (5) Non-compliance results in litigation, criminal charges or significant damages or penalties to Shire/Officers	Likely (4) Probably occur in most circumstances At least once per year	Extreme (20)	CEO & Council (Audit Committee) Risk only acceptable with excellent controls and all treatment plans to be explored and implemented where possible, managed by highest level of authority and subject to continuous monitoring Adequate: Substantial improvement on the years prior to 2022.	With the implementation of Attain and continued monitoring of compliance actions the risk is kept Low.

Financial Implications

Nil

VOTING REQUIREMENTS

Simple Majority

Officer Recommendation / Committee Resolution ARIC 2603-04

Moved: Cr N Smith **Seconded: Cr E Williams**

That the Audit, Risk & Improvement Committee:

1. **Notes** the requirements for the 2025 Compliance Audit Return and the amended submission date of 30 September 2026.
2. **Notes** the updates to Regulation 13 of the Local Government (Audit) Regulations 1996, which prescribe the statutory requirements for the CAR.
3. **Requests** Administration to complete the CAR when the approved form is issued and forward it to the ARIC for review prior to Council consideration.

CARRIED BY UNANIMOUS DECISION OF COMMITTEE

Voted For: Mr D Lovelock, Cr P Bantock, Cr E Williams and Cr N Smith
Voted Against: Nil

7.10 Status Report

7.10.1 Status Report – LGFI, Cybersecurity Report, Audit Survey

File Reference	
Report Date	17 March 2026
Applicant/Proponent	Audit, Risk and Improvement Committee
Officer Disclosure of Interest	Nil
Previous Meeting Reference	Nil
Prepared by	Colin Ashe – Deputy Chief Executive Officer
Senior Officer	Sean Fletcher – Chief Executive Officer
Authorised by	Sean Fletcher – Chief Executive Officer
Attachments	1. LGFI Report 2024 2. Cybersecurity Report 2025 3. Audit Survey 2025

PURPOSE

To inform and update the Audit, Risk and Improvement Committee (ARIC) on the Local Government Financial Indicators Report (LGFI), Cybersecurity Report and Audit Survey.

BACKGROUND

The LGFI is essentially produced by the Department of Local Government, Industry Regulation and Safety.

The Cybersecurity Report is produced by LGIS.

The Audit Survey is conducted by OAG.

Through various briefing sessions, Council has been informed to some extent on these reports and surveys received and these are now officially tabled to the ARIC in detail.

COMMENT

Local Government Financial Indicators (LGFI):

Over the last two financial years, the shire has been required to confirm, comment and if necessary, amend the LGFI. The current task was required to be completed by 30 Jan 26 and was for the 2023-24 financial year.

Unfortunately the LGFI is over a year old, i.e. 2023-24 and since then the 2024-25 annual financial report and audit has been completed and 2025-26 is halfway completed at Jan 26. Whilst the report is useful for trend lines, the time lag makes it somewhat redundant as per comments below on the 2024-25 current ratio.

Attachment 1 provides the LGFI 2024 and can be summarised as:

- The current ratio at 1.52 exceeds the benchmark of 1.00 indicating the shire can meet short liquidity.
- The debt service ratio at 3.35 exceeds the benchmark of 2.00 indicating the shire can comfortably increase debt levels.
- Net financial liabilities at 0.07 is under the benchmark of 0.30 consistent with the debt service ratio and indicating the level of debt can be increased against its operating revenue. Previously the ratio was negative indicating the shire is not leveraging enough debt to fund activities or projects.
- Operating Surplus Ratio at (0.38) is under the benchmark of 0.00 indicating the shire cannot generate surplus funds for capital projects. This is generally correct but is skewed due to the inclusion of depreciation.

2024-25 Current Ratio

Recently OAG as part of its procedural fairness for 2025 audit results to be tabled in Parliament requested the CEO confirm the shires current ratio for 2024-25 which was 0.81, reduced from 1.52 in 2023-24 and below the benchmark of 1.0. Specifically the draft commentary noted:

Financial analysis

For 2025, we analysed the current ratios of all local government entities with audits finalised by 31 December 2025. The current ratio is an indicator of an entity's ability to meet its short term obligations for payment, with a ratio of less than one suggesting that an entity owes more in the short term than it may be able to afford to pay. Four entities recorded a current ratio of less than one (2024: 2; 2023: 1).

The Shire was one of four shires with this result.

This is not unexpected given the deficit position of 2024-25 and reasons have previously been explained. It is also expressed at a point in time which can change but does highlight the need to ensure strong fiscal management and financial constraint.

Cybersecurity Report

As part of the annual insurance renewal, LGIS undertakes a comprehensive report on cybersecurity controls, the results being provided in attachment 2. The report is based on the questionnaire submitted as part of the renewal and is quite technical to respond to. This is evidenced by the detail provided in the report which arguably in some parts requires an IT specialist to interpret and respond.

After engagement with the shires IT partner, Wallis Computing Solutions (WCS), it is clear that some questions were answered incorrectly which has caused some results to return inadequate controls.

To summarise the results:

- Since 2022-23, the shires results have generally increased positively.
- Against the LGIS average, the shire performs well, often exceeding the average.
- Against the national average is a similar result, often exceeding the average.
- This is a good result given the shire is a tier 4 council and therefore lacks some of the resources that can be afforded in other shires.

In terms of the analysis provided by WCS an management:

2 Endpoint detection and response – with the correct response, this would change to 60%

11 EOL systems replaced or protected – the only one the shire has is Synergy soft that is a read

only system and likely to be protected through a third party.

12 Vendor supply chain – the shire has engaged a third party software vendor (EFTsure) that provides assurance and controls on the validity of bank accounts and payments.

For the 2026-27 insurance renewal, WCS will be engaged to review responses to the questionnaire to ensure correctness and management is confident this result will improve.

Audit Survey

OAG approached the shire to complete a survey on the conduct of the 2024-25 annual financial report audit which is provided at attachment 3. The survey was based on the conduct of the actual auditors, William Buck Accountants and not necessarily OAG themselves. Overall the conduct and feedback from staff was positive, organised and relatively seamless. Management however did make comment at question 22 on the increasing cost with a limited increase the value proposition.

CONSULTATION

Mr Sean Fletcher, Chief Executive Officer

Ms Glenn Deocampo, Coordinator Financial Services

STATUTORY CONTEXT

Nil

CORPORATE CONTEXT

Audit, Risk and Improvement Committee Terms of Reference.

Strategic Business Plan/Corporate Business Plan

STRATEGIC PRIORITIES	WE KNOW WE ARE SUCCEEDING WHEN
4. CIVIC LEADERSHIP	
4.3 Proactive and well governed Shire	External audits and reviews confirm compliance
	We have sound financial management policies and attract external funding to help achieve our goals
	Council is supported by a skilled team

Strategic Priority 4.3 - Management considers the tabling of these reports as good governance, transparency and identification of any significant issues.

Delegation

Nil

Policy Implications

Section 3 – Financial Management

Other Corporate Document

ICT Strategy which incorporates cybersecurity and essential 8.

Risk Analysis

Consequence	Consequence Rating:	Likelihood Rating:	Risk Rating	Risk Acceptance/ Controls	Mitigation and Outcome
Compliance	Moderate (3) Short term non-compliance but with significant regulatory requirements imposed	Unlikely (2) The event could occur at some time	Moderate (6)	Operational Manager Risk acceptable with adequate controls, managed by specific procedures and subject to semi-annual monitoring	Ensuring frequent reviews reduces the residual risk to low.

FINANCIAL IMPLICATIONS

VOTING REQUIREMENTS

Simple Majority

Officer Recommendation / Committee Recommendation ARIC 2603-05

Moved Cr N Smith **Cr P Bantock**

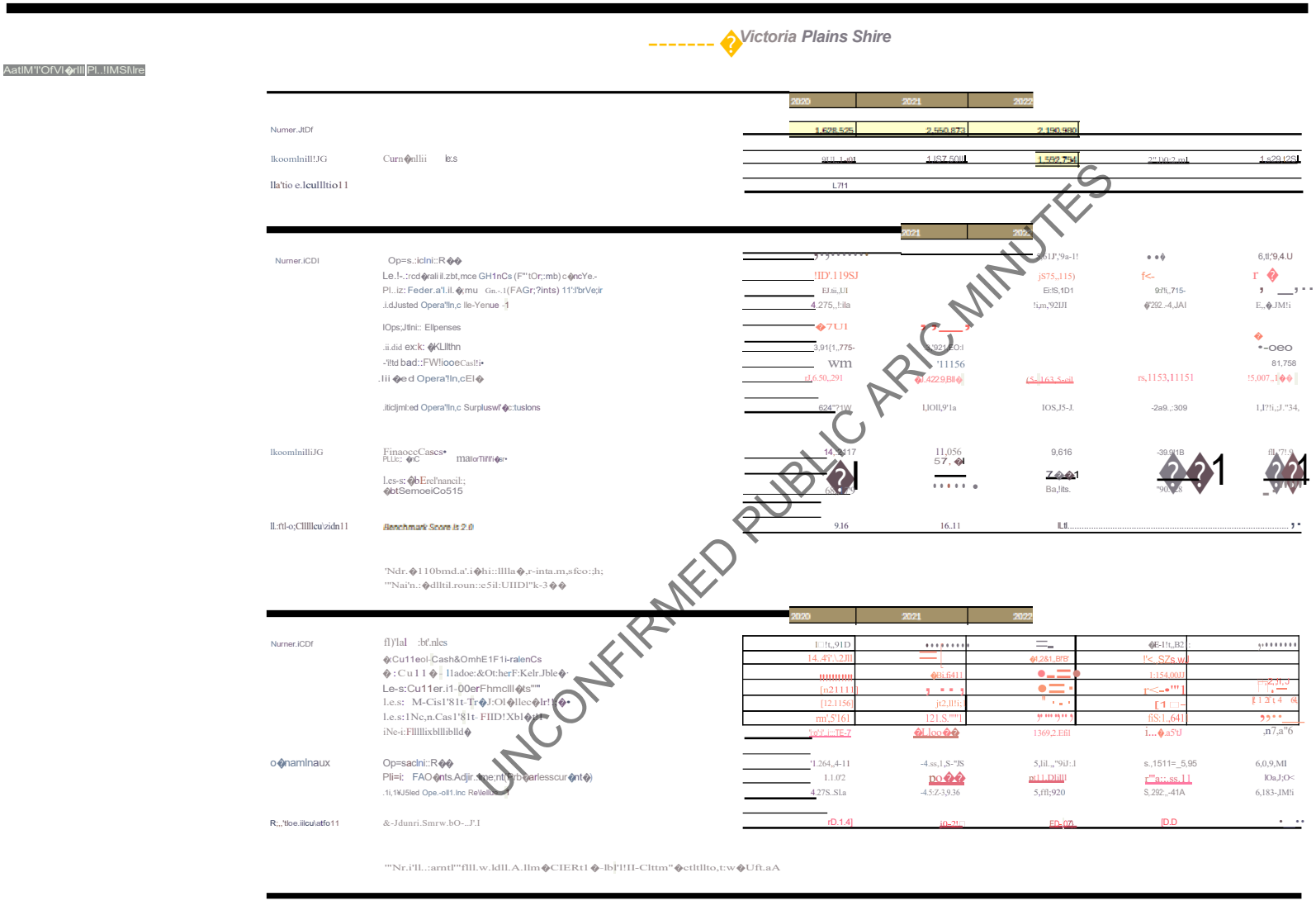
That the Audit, Risk and Improvement Committee **RECEIVES** the:

1. Local Government Financial Indictors 23-24 report
2. Cybersecurity Report.
3. Audit Survey.

As tabled.

CARRIED BY UNANIMOUS DECISION OF COMMITTEE

Voted For: Mr D Lovelock, Cr P Bantock, Cr E Williams and Cr N Smith
Voted Against: Nil



LGFI Model								
Numerator	Operating Revenue	$	4,264,441	4,554,538	5,617,934	5,758,995	6,079,441
	Plus: FA Grants Adjustment (Prior year less current year)	$	11,072	(30,602)	(340,014)	(466,581)	103,604
	Plus: Grants, contributions for asset renewal*	$	1,186,184	1,879,646	1,445,581	1,565,086	0
	Adjusted Operating Revenue - 2	$	5,461,697	6,403,582	6,723,501	6,857,500	6,183,045
	Less: Operating Expenses	$	(7,575,711)	(7,356,645)	(9,234,789)	(9,366,670)	(8,533,550)
	Adjusted Operating Surplus	$	(2,114,014)	(953,063)	(2,511,288)	(2,509,170)	(2,350,505)
Denominator	Operating Revenue	$	4,264,441	4,554,538	5,617,934	5,758,995	6,079,441
	Plus: FA Grants Adjustment (Prior year less current year)	$	11,072	(30,602)	(340,014)	(466,581)	103,604
	Plus: Grants, contributions for asset renewal*	$	1,186,184	1,879,646	1,445,581	1,565,086	0
	Adjusted Operating Revenue - 2	$	5,461,697	6,403,582	6,723,501	6,857,500	6,183,045
Ratio Calculation	*Benchmark Ratio is 0.0*		**(0.39)**	**(0.15)**	**(0.37)**	**(0.37)**	**(0.38)**

**Note: Due to lack of inputs for "Grants, contributions for asset renewals" the model considers the entire grants (towards new, upgrade, renew) line item for the purpose of calculating this ratio*


Victoria Plains Shire
Actual
FY 2020
FY 2021
FY 2022
FY 2023
FY 2024
84
61
72
72
CLlifefH Ratio
Debt Ser;iceCOVerag,, Ratio
OperalingSurpbrt RaUO
Net Rmmciol LiahiLily Ratio
LGFI Score
Improving
2023
2024
UNCONFIRMED PUBLIC ARIC MINUTES

LGFI Model	
Example text...	Please write as much commentary as necessary in yellow cells, boxes will expand to capture input
LGA commentary Operating Surplus Ratio	
Example text...	Please write as much commentary as necessary in yellow cells, boxes will expand to capture input
LGA commentary Net Financial Liability Ratio	
Example text...	Please write as much commentary as necessary in yellow cells, boxes will expand to capture input
Overall LGA commentary re. LGFI	
Example text...	Please write as much commentary as necessary in yellow cells, boxes will expand to capture input

JLT

JLT Public Sector

Top Cyber-Security Controls Review 2025

Shire of Victoria Plains

Report printed September 2025

JLT Public Sector

- Through our deep knowledge of the Local Government, JLT Public Sector has developed a unique method to provide protection solutions for Local Government clients.

- As part of our “client first” philosophy, we place the needs of the Public Sector first. We do this by providing products and services that provide confidence, reduce volatility and that support the unique challenges of the Public Sector over the long term.

- JLT Public Sectors work with mutual funds in the local government market in particular, demonstrates this ability to work innovatively with our clients to produce effective insurance solutions designed to protect the long term interests of their staff and community.

Executive Summary

Cyber risk is a highly dynamic environment and has been regularly identified by Local Government CEO's in the annual JLT Public Sector Risk Survey report as a top two risk.

JLT Public Sector has created this laser-focused analysis of your organisations 12 Key Control areas to assist in setting priorities to enhance your overall cyber-posture.

Ultimately this will assist to enhance the Local Government sector's cybersecurity posture and help avoid costly cyber breaches and keep your community's data secure.

JLT Public Sector have utilised the data collected through the annual Cyber questionnaire to generate this report and help guide Councils in improving your cybersecurity controls.

This document provides Council with a valuable feedback loop to assist in setting priorities to enhance their cyber position over the coming 12 months and beyond.

This annual report now includes report bench-marking information for your reference against the National and State average.

JLT Public Sector is able to differentiate the Local Government Mutuals and individual Council's risk exposure through the extensive data provided during the annual questionnaire.

This data proved crucial in demonstrating the implementation of specific controls to lower the impact of cyber-attacks across the sector and mapping the progression of the sector as a whole. .

Whilst the local Government Sector in Australia has experienced an increase in the frequency of claims, severity levels of the high-profile cyber incidents have not been experienced to date.

This however does not mean the sector is immune from attack. The necessary controls require implementation and monitoring to adequately address the threat environment

---

The proliferation of cyber-related crime has steadily increased across the globe for the past two decades. .

Developments in technology, complimented by changing working patterns have seen incidents exponentially increase over that time. More recently there have been 'mega-breaches' of contact information onto the dark web of up to 16 billion records in a a single event. Some of these breaches contain duplicate information from previous leaks.

Conversations among cyber-professionals have now shifted from the number of attacks and operational defences to strategically focusing on building cyber-resilience. The foundations of cyber-resilience are the key controls highlighted in this report, based on your data and your organisations defences.

Twelve Key Controls and The Essential Eight

Essential Eight Maturity Model

First launched in June 2018 “The Australian Cyber Security Centre (ACSC) has developed prioritised mitigation strategies tohelp cyber security professionals in all organisations mitigate cyber security incidents caused by various cyber threats.” (www.cyber.gov.au/acsc)

12 Key Controls

The JLT Public Sector 12 Key Controls were created by our specialist cyber risk team and developed in consultation with our global clients and risk carriers as a way to benchmark and model the risk-maturity of Councils across key control areas.

The demand for basic control data is now significant to ensure the longevity of placement for your cyber risk transfer program.

The 12 Key Control framework recognises all of the Essential Eight Maturity Model components and in addition, draws attention to the training of people, how end-of-life systems are managed and the management vendors.

Twelve Key Controls and The Essential Eight cont.

The following table maps the 12 Key Controls methodology against the Essential Eight Government approach. This provides an overview of how the two models can be viewed together in assisting the prioritisation of your Council's cyber risk treatments and avoiding duplication of effort.

12 KEY CONTROLS	ESSENTIAL EIGHT
1. MULTI-FACTOR AUTHENTICATION	7. MULTI-FACTOR AUTHENTICATION
2. ENDPOINT DETECTION & RESPONSE	5. RESTRICTED ADMINISTRATIVE PRIVILEGES 6. PATCH APPLICATIONS
3. SECURED, ENCRYPTED & TESTED BACKUPS	8. REGULAR BACKUPS
4. PRIVILEGED ACCESS MANAGEMENT	5. RESTRICTED ADMINISTRATIVE PRIVILEGES
5. EMAIL FILTERING & WEB SECURITY	1. APPLICATION CONTROL 3. CONFIGURE MICROSOFT OFFICE MACRO SETTINGS
6. PATCH & VULNERABILITY MANAGEMENT	2. PATCH OPERATING SYSTEMS 6. PATCH APPLICATIONS
7. CYBER INCIDENT RESPONSE PLANNING & TESTING	8. REGULAR BACKUPS
8. CYBER SECURITY AWARENESS TRAINING & PHISHING TESTING	
9. HARDENING TECHNIQUES	4. USER APPLICATION HARDENING
10. LOGGING & MONITORING/NETWORK PROTECTIONS	3. CONFIGURE MICROSOFT OFFICE MACRO SETTINGS
11. END-OF-LIFE SYSTEMS REPLACED OR PROTECTED	6. PATCH APPLICATIONS
12. VENDOR/DIGITAL SUPPLY CHAIN RISK MANAGEMENT	5. RESTRICTED ADMINISTRATIVE PRIVILEGES

Tightening up your IT Enterprise: 12 Key Controls to implement/enhance (1/2)

Multi-Factor Authentication (MFA) for remote access & admin / priviliged access

MFA/2FA is a second set of credentials required for access to a system or data of interest. MFA/2FA prevents attackers from effectively using them without this additional factor. Remote working has put MFA/2FA at the forefront to secure access, especially remote access and privileged access to critical systems & sensitive data.

Secured, encrypted, and tested backups

Attackers are looking to delete backups prior to launching a ransomware attack launch so they can successfully cripple and extort their victims. It is essential to secure backups through encryption and isolation from the network (offline or MFA-controlled access with dedicated identities), as well as regular testing of backups and recovery plans.

Patch management / Vulnerability management

Regular vulnerability scans and patch management reduce the risk of cyber attacks on the network. Such actions allow organisation to apply patches or uncover existing vulnerabilities and remediate before threat actors have a chance to exploit.

Email filtering & Web Secuirty

Malicious links and files are still the primary way to insert ransomware, steal passwords, and potentially access critical systems. Today's first line of defense includes advanced technologies to filter incoming emails, block malicious sites or downloads, and test suspicious content in a secure "sandbox' environment that enhance network integrity and security.

End of Life System should be replaced or protected

End-of-life systems or technology is a risk as they receive no more security updates such as bug fixes, patches, or security monitoring. Therefore the technology is practically not supported and will be affected by unfixable vulnerabilities. It needs to be either protected by compensating controls or upgraded to 'supported' systems.

Privileged Access Managment (PAM)

Privileged accounts are the keys of a network. When attackers compromise these accounts, the likelihood of causing significant harm is extremely high because there's no more limit to actions that can be performed. Limiting the number of privileged accounts, using strong password security practices or vaults, MFA, and enhanced monitoring of these accounts is critical to network security.

**New Dark Web Audit Reveals 15 Billion Stolen Logins From 100,000 Breaches (forbes.com)

Tightening up your IT Enterprise: 12 Key Controls to implement/enhance (2/2)

Cyber Incident Response planning & testing

An up-to-date Cyber Incident Response (CIR) plan with a trained team and experienced senior leadership provides efficiency and effectiveness in response to cyber incidents. Practice through tabletop exercises provide "Muscle Memory." When combined with backups and business continuity plans and monitoring of endpoints and the network, they significantly help mitigate impacts on business operations and your organisation's reputation. An issue highlighted in the recent Optus and Medibank Private data breaches

Hardening techniques including Remote Desktop Protocol (RDP) mitigation

Attackers exploit default device settings or misconfigurations. Defining security baselines to harden devices, continuously managing secure configurations, and controlling changes are all critical to preventing attackers from reaching and exploiting their targets. Particularly, the use of RDP should be avoided.

Endpoint Detection and Response (EDR)

Advanced anti-malware solutions on workstations, servers, and mobile devices detect malicious programs and contain/minimise their spread. Technology allows organisations to remotely respond to attacks and even prevent data leakage.

Cybersecurity awareness training / phishing testing

Attackers have taken advantage of COVID-19 – when people were stressed the most – as a guise to spread ransomware. There will always be environmental factors that attackers can exploit to deceive people. Employee Cybersecurity Training and phishing campaigns help ensure people remain aware of changes in the cyber environment and remain cautious.

Logging & monitoring / Network protections

Logging and monitoring network activities allows organisations to identify unauthorised activity and questionable behaviors; furthermore it allows attacker's actions to be detected and contained at an early stage. Automated technology combined with human operator monitoring is needed to watch and review network activities or anomalous behaviors of users. Also, firewalls, network segmentation, intrusion detection and prevention systems, data leak prevention systems, etc. help mitigate against network attacks.

Vendor / Digital Supply Chain Risk Management

A significant proportion of attacks or incidents are initiated through the supply chain, whether it's a third party access that is leveraged, a trusted software update that is compromised, a malicious code that comes through a library or a critical service that becomes unavailable. Managing cyber supply chain by monitoring risks, dependencies and maintaining continuity plans goes a long way in reducing the overall cyber risk exposure

Ratings Definitions

Rating Definition	Rating
Adequate controls are in place across all or most categories of the specified area. While some controls may require attention or development, implementation has been largely achieved to an acceptable level. **Score: 80% - 100%**	
Adequate controls are in place across some categories of the specified area. Numerous controls require further attention and priority to achieve an acceptable level of implementation. **Score: 50% - 80%**	
Inadequate controls are in place across all or most categories of the specified area. Significant attention and development are required to achieve acceptable levels of implementation **Score: 0% - 50%**	

- Where specific controls or measures were selected by council these critical components to key controls have been specifically noted and colour-coded accordingly.

Shire of Victoria Plains Results

Top Cybersecurity Controls

How did Shire of Victoria Plains score ?

	Key Controls	Questions	22-23	23-24	24-25	25-26
1	Multifactor authentication for remote access and admin/privileged controls	Account monitoring	30%	80%	80%	80%
2	Endpoint Detection and Response (EDR)	Protection capabilities	0%	8%	8%	24%
3	Secured, encrypted, and tested backups	Recovery Protection capabilities	67%	77%	77%	77%
4	Privileged Access Management (PAM)	Account monitoring	22%	72%	72%	72%
5	Email filtering and web security	Protection capabilities	71%	50%	50%	50%
6	Patch management and vulnerability management	Protection capabilities	40%	65%	65%	65%
7	Cyber incident response planning and testing	Business continuity Incident response	18%	76%	76%	76%
8	Cybersecurity awareness training and phishing testing	Training	36%	100%	100%	100%
9	Hardening techniques, including Remote Desktop Protocol (RDP) mitigation	Secure configuration	40%	100%	100%	100%
10	Logging and monitoring/network protections	Governance Log monitoring	70%	70%	70%	70%
11	End-of-life systems replaced or protected	Protection Capabilities	100%	0%	0%	0%
12	Vendor/digital supply chain risk management	Governance	0%	0%	0%	0%

Top Cybersecurity Controls Benchmarking

How does Shire of Victoria Plains compare to other councils in LGIS?

			LGIS Averages				Council
	Key Controls	Questions	3yr Avg	23-24	24-25	25-26	25-26
1	Multifactor authentication for remote access and admin/privileged controls	Account monitoring	52%	49%	53%	54%	80%
2	Endpoint Detection and Response (EDR)	Protection capabilities	38%	38%	41%	35%	24%
3	Secured, encrypted, and tested backups	Recovery Protection capabilities	70%	69%	70%	72%	77%
4	Privileged Access Management (PAM)	Account monitoring	40%	38%	40%	41%	72%
5	Email filtering and web security	Protection capabilities	62%	27%	78%	81%	50%
6	Patch management and vulnerability management	Protection capabilities	56%	54%	56%	58%	65%
7	Cyber incident response planning and testing	Business continuity Incident response	50%	49%	51%	52%	76%
8	Cybersecurity awareness training and phishing testing	Training	42%	36%	41%	50%	100%
9	Hardening techniques, including Remote Desktop Protocol (RDP) mitigation	Secure configuration	83%	83%	82%	83%	100%
10	Logging and monitoring/network protections	Governance Log monitoring	61%	60%	61%	62%	70%
11	End-of-life systems replaced or protected	Protection Capabilities	77%	78%	78%	76%	0%
12	Vendor/digital supply chain risk management	Governance	39%	38%	40%	40%	0%

Top Cybersecurity Controls Benchmarking

How does Shire of Victoria Plains compare to other councils Nationally ?

			National Averages				Council
	Key Controls	Questions	3yr Avg	23-24	24-25	25-26	25-26
1	Multifactor authentication for remote access and admin/privileged controls	Account monitoring	57%	51%	57%	62%	80%
2	Endpoint Detection and Response (EDR)	Protection capabilities	44%	42%	46%	44%	24%
3	Secured, encrypted, and tested backups	Recovery Protection capabilities	72%	70%	72%	75%	77%
4	Privileged Access Management (PAM)	Account monitoring	45%	41%	44%	48%	72%
5	Email filtering and web security	Protection capabilities	69%	53%	69%	85%	50%
6	Patch management and vulnerability management	Protection capabilities	60%	56%	60%	64%	65%
7	Cyber incident response planning and testing	Business continuity Incident response	48%	40%	43%	61%	76%
8	Cybersecurity awareness training and phishing testing	Training	54%	48%	54%	61%	100%
9	Hardening techniques, including Remote Desktop Protocol (RDP) mitigation	Secure configuration	86%	85%	86%	88%	100%
10	Logging and monitoring/network protections	Governance Log monitoring	63%	60%	63%	66%	70%
11	End-of-life systems replaced or protected	Protection Capabilities	66%	68%	66%	64%	0%
12	Vendor/digital supply chain risk management	Governance	46%	44%	46%	50%	0%

Key Controls

1. Multi-Factor Authentication (MFA) for remote access & admin/privileged access

Key Control	The Issue	What are the minimum expected controls	Overall Priority Rating
Multi-Factor Authentication (MFA) for remote access & admin/privileged access	Cyber attacks often start with compromised credentials. MFA is a method to validate or verify a user's request to access an IT resource, by requiring the user to provide two or more pieces of evidence to be authenticated. This can help thwart ransomware attacks.	Enforcement of Multi-Factor Authentication on: • Critical assets • Privileged accounts • Access on remote applications	80%

Account Monitoring			
	8.1	We require multi-factor authentication for all remote login access to the corporate network (e.g., Virtual Private Network (VPN), Remote Desktop Protocol (RDP), or other secure remote access, etc.).	Yes
	8.2	Irrespective of a user's location, we require multi-factor authentication and encrypted channels for all administrative account access.	Yes
	8.3	In addition to the capabilities listed above, irrespective of a user's location, we require multi-factor authentication for access to our most critical or sensitive data or systems.	Yes
	8.4	If there are technological limitations preventing multi-factor authentication, then we enforce complex long passwords (i.e., longer than 14 characters).	No

Key Controls

2. Endpoint Detection and Response (EDR)

Key Control

Endpoint Detection and Response (EDR)

The Issue

Advanced anti-malware solutions on workstations, servers, and mobile devices detect malicious programs and contain their spread. Technology allows organisations to remotely respond to attacks and even prevent data leakage. The time when simple “anti-virus” was good enough is behind us.

What are the minimum expected controls

- Endpoint protection (EPP) and endpoint detection and response (EDR) solutions across your servers and laptops

Overall Priority Rating

24%

Protection Capabilities

11.1

The organisation operates the following Information Technology (IT) and Information/Cybersecurity tools and capabilities (please check all that apply and indicate key vendors):

DDoS mitigation solutions	No	Unified Threat Management (UTM)/ Threat Prevention/ Protection Systems (TPS)	No
Network Data Loss Prevention (DLP) solution	No	Protective Domain Name Service (PDNS)	Yes
Security Information and Event Management (SIEM)	No	Email DLP solution	No
Enforce Sender Policy Framework (SPF)	No	DomainKeys Identified Mail (DKIM)	No
Domain-based Message Authentication, Reporting and Conformance (DMARC)	No	Block malicious and phishing URLs	No

Key Controls

2. Endpoint Detection and Response (EDR)

Multi-Factor Authentication to cloud-based backups	Yes
File Integrity Tools (Whitelisting)	No
Endpoint Detection and Response (EDR) solutions	No
Identity and Access Management solutions	No
Bring Your Own Device (BYOD) security solutions	No
Network Intrusion Detection Systems (NIDS)	No

Host Intrusion Prevention Systems (HIPS)	No
Endpoint DLP solution	No
Advanced Endpoint Security	No
Multi-Factor Authentication to on-premise backups	Yes
Wireless Network Security solutions	No

Key Controls

3. Secured, encrypted, and tested backups

Key Control	The Issue	What are the minimum expected controls	Overall Priority Rating
Secured, encrypted and tested backups	Attackers are looking to delete backups prior to launching a ransomware attack launch so they can successfully cripple and extort their victims. It is essential to secure backups through encryption and isolation from the network (offline or MFA-controlled access), as well as regularly test backups and recovery plans.	• Backup procedure of the critical assets • Off line backups of the critical assets • Regular testing of backups of the critical assets • Checking the integrity of the backups before restoring	77%

Recovery			
	1.1	After an incident is contained, the organisation implements procedures/processes to remediate affected systems and restore systems to our normal or fully operational state.	Yes
	1.2	Our organisation conducts backups for Applications	Continuously / Daily
	1.3	Our organisation conducts backups for Databases	Continuously / Daily
	1.4	Our organisation conducts backups for Servers	Continuously / Daily
	1.5	Our organisation conducts backups for Workstations/laptops and endpoints	Continuously / Daily
	1.6	Our organisation conducts backups for Critical Information (Critical Information means critical information as defined by the organisation's information classification or business continuity / disaster recovery plans/policies)	Continuously / Daily

Key Controls

3. Secured, encrypted, and tested backups Cont.

Recovery	1.7	We test system restoration capabilities by performing a full restoration from a sample set of backup data at least.	Yes
	1.8	To strengthen recovery from malicious encryption (e.g. crypto-ransomware attack), we isolate backup files from the network (i.e. backup files are not continuously accessible from the network).	Yes
Protection Capabilities	1.1	The organisation utilises mandatory encryption to protect critical information and other sensitive information (e.g., PII, PHI, etc.) as defined by information classification and protection policies.	
	1.1.1	Data at Rest	No
	1.1.2	Data in Transit	No
	1.1.3	Corporate laptops and desktops	No
	1.1.4	Data on Removable media	No
	1.1.5	Mobile Devices (e.g., Mobile phones and tablets)	No
	1.1.6	Backups	Yes

Key Controls

4. Privileged Account Management (PAM)

Key Control	The Issue	What are the minimum expected controls	Overall Priority Rating
Privileged Account Management (PAM)	Privileged accounts are the keys of a network. When attackers compromise these accounts, the likelihood of causing significant harm is extremely high. Limiting the number of privileged accounts, using strong password security practices/vaults, MFA, and monitoring these accounts is critical to network security.	• Environment-wide deployment and consistently enforced use of Multi-Factor Authentication • Hardened security measures on privileged accounts and service accounts	72%

Account Monitoring			
	7.1	We limit the use and distribution of administrator or privileged accounts via an account authorisation process requiring senior management approval.	Yes
	7.2	The organisation manages Desktop / Local Administrator privileges via: Please check all that apply and indicate the name of the solution(s).	
	7.2.1	End Privilege Management (EPM)	No
	7.2.2	Local Administrator Password Solution (LAPS).	No
	7.2.3	Privileged Access or Account Management (PAM).	Yes

Key Controls

4. Privileged Account Management (PAM) Cont.

Account Monitoring	7.3	Our organisation implements privileged/administrator account management solutions i.e., session management, automated credential management, or temporary one-time use passwords	Yes
	8.2	Irrespective of a user's location, we require multi-factor authentication and encrypted channels for all administrative account access.	Yes

Key Controls

5. Email filtering and web security

Key Control	The Issue	What are the minimum expected controls	Overall Priority Rating
Email filtering and web security	Malicious links and files are still the primary way to insert malware (i.e. ransomware), steal passwords, and eventually access critical systems. Today's first line of defence includes indispensable technologies to filter incoming emails, block malicious sites or downloads, and test suspicious content in a secure "sandbox" environment.	• Pre-screen e-mails for potentially malicious attachments and links • Tools to monitor web content to block access to vulnerable websites	50%

Protection Capabilities			
3.1	Our organisation installs and regularly updates anti-malware solutions (e.g., anti-virus, anti-spyware, advanced endpoint security) to the following percentage of endpoints, servers, and mobile devices.		75%-100%
3.2	The organisation implements the following malware protections:		
3.2.1	Macro-enabled files cannot be run by default.		No
3.2.2	A quarantine service is provided.		No
3.2.3	Incoming emails are filtered/scanned for malicious attachments and links.		Yes
3.2.4	Email attachments are evaluated in a sandbox to determine if malicious prior to delivery.		No

Key Controls

6. Patch managment and vulnerability management

Key Control	The Issue	What are the minimum expected controls	Overall Priority Rating
Patch management	Unpatched vulnerabilities remain a leading cause of intrusions into systems. Hundreds of vulnerabilities are revealed every month for multiple applications and systems. When technology environments are not patched in a timely fashion, attackers will seek to exploit their vulnerabilities.	• Appropriate patching cadence • Timely urgent installation of all critical patches across your information systems, especially 7 to 10 CVE	65%
Vulnerability management	Regular vulnerability scans and annual penetration testing simulate cyber attacks on the network. Such actions allow organisations to uncover existing vulnerabilities and remediate them before threat actors have a chance to exploit them.	• Comprehensive Patch & Vulnerability Management Policies • Performing vulnerability management tools/services of your critical assets	

Protection Capabilities			
4.1	Vulnerability scans are performed at least (select from dropdown list), and the organisation prioritises vulnerability remediation.		Daily
4.2	In addition to the capabilities above, our organisation deploys automated patch management processes/tools to update operating systems, software/applications, and other application software or firmware.		No
4.4	In addition to the capabilities above, our remote access solution performs a pre-login security assessment and security scan of the device attempting a connection before permitting access to our corporate network.		Yes
4.5	Our organisation's target timeframe to patch Common Vulnerability Scoring System (CVSS) v3 Critical Severity 7.0+ vulnerabilities across your enterprise is:		72 hours

Key Controls

6. Patch managment and vulnerability management Cont.

Protection Capabilities	5.1	In our organisation, annual or more frequent penetration testing (i.e., testing that emulates adversary actions and hostile cyber attacks) is conducted on the network and critical systems.	No
	5.2	Our processes require penetration testing activities that include, but are not limited to, the following: a) annual assessment(s) b) independent penetration agents simulate adversary actions c) testing scope includes the network and business critical systems/ applications d) penetration test results and recommendations are risk-rated and/or prioritised to mitigate or remediate vulnerabilities and weaknesses identified.	Yes

* Criteria for question 4.6 changed in 2024 in line with risk transfer requirements under JLT Public Sector Cyber Liability Policy. This may impact the scoring in comparison to last year for some entities.

Key Controls

7. Cyber Incident Response planning and testing

Key Control	The Issue	What are the minimum expected controls	Overall Priority Rating
Cyber Incident Response planning and testing	An up-to-date incident response plan with a trained team provides efficiency, speed, and quality in response to cyber incidents. When combined with backups and business continuity plans, it significantly helps to mitigate the impacts on operations and your organisation's reputation, thereby limiting overall costs.	• Regularly updated and tested incident response plan • Tests should occur at minimum annually	76%

Incident Response	1.1	Our incident response or breach response plan is formally documented and it is aligned with the National Institute of Standards and Technology (NIST) Special Publication 800-61, "Computer Security Incident Handling Guide," the United States Computer Emergency Readiness Team (US-CERT), or ISO/IEC 27035 guidance, and applicable statutes or regulations.	No
	1.3	In addition to the capabilities above, our incident response plans include items such as, but not limited to the following: a) Processes/procedures to classify and prioritise incidents b) Process/procedures for recovery, such as activating the emergency or disaster recovery plans (DRP) c) Names and contact information for relevant authorities, including local law enforcement and regulators d) Communication protocols between the response team and others, such as retained legal counsel, corporate communications/legal departments, and external regulators or law enforcement agencies	Yes

Key Controls

7. Cyber Incident Response planning and testing Cont.

Incident Response	2.4	In addition to the capabilities above, our incident response strategy is integrated with our organisation/corporate business continuity/ recovery plans and IT disaster recovery capabilities.	Yes
	4.1	Our organisation conducts incident response tabletop reviews at least annually.	Yes
Business Continuity	1.1	Our organisation maintains a business continuity/disaster recovery plan, and the plan is tested.	Yes

Key Controls

8. Cybersecurity awareness training and phishing training

Key Control	The Issue	What are the minimum expected controls	Overall Priority Rating
Cybersecurity awareness training and phishing training	Recently, attackers took advantage of COVID-19 – when people were stressed the most - as a guise to spread ransomware. There will always be environmental factors that attackers can exploit to deceive people. Training and phishing campaigns help ensure people remain aware and vigilant.	• Carry out annual security awareness campaigns for employees • Carry out annual phishing campaign	100%

Training			
	1.1	We have established a cybersecurity training program.	Yes
	1.2	In our organisation, cybersecurity training is mandatory for all employees (select period from list).	Monthly
	2.1	Our cybersecurity awareness program materials train users to avoid common cyber-risks and threats, such as social engineering and phishing.	Yes
	2.6	The organisation conducts internal phishing campaigns at least annually.	Yes

Key Controls

9. Hardening techniques including Remote Desktop Protocol (RDP)

Key Control	The Issue	What are the minimum expected controls	Overall Priority Rating
Hardening techniques including Remote Desktop Protocol (RDP)	Attackers exploit default device settings or misconfigurations. Defining security baselines to harden devices, continuously managing secure configurations and change control processes are essential to preventing attackers from reaching their target.	• Hardened baseline configuration materially rolled out across systems and applications • Change management process in case of change to configuration	100%

Secure Configuration	1.1	We implement standard secure configuration images for operating systems and software applications.	Yes
	2.1	Our system configuration management tools (e.g., Active Directory Group Policy, etc.) enforce and redeploy configuration settings to systems.	Yes

Key Controls

10. Logging & monitoring / Network Protections

Key Control	The Issue	What are the minimum expected controls	Overall Priority Rating
Hardening techniques including Remote Desktop Protocol (RDP)	Logging and monitoring network activities enable the organisation to identify something possibly harmful that might be happening. And attackers actions can be detected and contained at an early stage. Automated technology combined with operators monitoring is needed to watch network events or anomalous behaviour of users.	• Capability to detect potential incidents as they occur (e.g. SOC, SIEM, audit logs)	70%

Governance	**10.1**	Our organisation operates its own Security Operations Center (SOC) and/or has an outsourced Managed Security Service Provider (MSSP) with the following capabilities at a minimum: a) Established incident alert thresholds b) Security Incident and Event Management (SIEM) monitoring and alerting for unauthorised access connections, devices, and software.	Own / MSSP
	10.2	In addition to the capabilities above, the SOC/MSSP capabilities include, but are not limited to, the following: a) 24x7 operations b) mix of signature and heuristic-based detection c) incident response, containment, and remediation capabilities d) active threat intelligence and analytics delivering rapid alerts/notification and/or countermeasures e) processes are continuously improved.	Yes
Log Monitoring	**5.1**	We implement a SIEM (Security Information and Event Management) or log analytic tool for unified aggregation, consolidation, correlation, analysis, and alerting.	No

Key Controls

11. End-of-life systems replaced or protected

Key Control	The Issue	What are the minimum expected controls	Overall Priority Rating
End-of-life systems replaced or protected	End-of-life (EOL) systems or technology become a risk because patches and other forms of security support are no longer offered. Once the software/technology is practically not supported it will be impacted by unfixable vulnerabilities. It needs to be either protected by compensating controls or upgraded to “supported” platforms.	• EOL systems (hardware and software) should be prioritised for replacement; specific solutions vary from system to system and application to application. Identification of a replacement system(s) or application(s) vary based on requirements and purpose for use. Until EOL systems are replaced, they should be hardened and limited to restricted access only to prevent unauthorised use and access. Hardening may include establishing a “gatekeeper” system that is the only authorised system to communicate with the EOL system until an acceptable EOL system is put in place.	0%

Protection Capabilities	6.1	Our organisation relies on operating systems, software, or hardware that is no longer supported or is considered “end-of-life” (EOL) by the manufacturers. (If yes, summarise EOL cases)	Yes

Key Controls

12. Vendor / Digital Supply Chain Risk Managment

Key Control	The Issue	What are the minimum expected controls
Vendor / Digital Supply Chain Risk Management	A significant proportion of attacks or incidents are initiated through the supply chain, whether it's a third party authorised access that is leveraged, a trusted software update that is compromised, malicious code that comes through a library, or a critical service that becomes unavailable. Managing cyber supply chain by monitoring risks and dependencies, and maintaining continuity plans goes a long way in reducing the overall cyber risk exposure.	• Third Party Vendor Risk Management requires a combination of technical and non-technical processes in determining the risk associated with allowing vendors authorised access to the organisation's IT resources and/or data. Prior to granting access, a tailored process used to review and assess the risk imposed to the organisation by providing access should be implemented. Finance / Contracts, IT, IT Security, Risk Management, and the Business Owner who requires the vendor's service(s) should review, document, and approve the risk. Understanding the vendor's cybersecurity program and leveraging external assessment providers such as Security Scorecard or Bitsight can provide insight to the vendor's external cybersecurity risk profile.

Overall Priority Rating
0%

Key Controls

12. Vendor / Digital Supply Chain Risk Management

Governance	11.1	The organisation conducts security assessments and periodic re-assessments on third party partners and other service providers with access to information assets.	No
	11.2	The organisation reviews independent audit reports (e.g., SSAE 18 SOC 2, HITRUST certification, or Standardised Information Gathering (SIG), Agreed Upon Procedures (AUP)*) from third party partners and other service providers with access to information assets at least annually.	No
	11.3	Our organisation requires vendors to maintain insurance or another means of indemnification for losses caused by the provider, including from a privacy breach.	No
	12.1	The organisation requires interconnection agreements for connections between the organisation's network and external networks (e.g., third-parties, vendors, etc.).	No

* In 2024, the previous question 12.2 was removed from this section. This may adversely affect total scores.

Next Steps ?

This report is designed to assist Council to set priorities to improve your cyber-security position. JLT Public Sector recommend the following next steps to achieve this objective.

NEXT STEPS….

Discuss 12 Key Controls:
Review Key Controls in conjunction with key stakeholders at your Council. Utilise the 12 Key Control framework to set priorities to enhance cyber-security at your Council within realistic time frames and budget.

Should you require further advice:
Contact your Account Manager.

A. Audit Process

Please indicate the extent of your agreement or disagreement with the following statements. Please respond on the basis of your experience with the OAG in its conduct of your organisation's **2024-25 annual financial report audit**.

	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Unsure
1 The auditors communicated with us effectively.	○	○	○	◉	○	○
2 The auditors adequately understood our organisation.	○	○	○	○	◉	○
3 The auditors had the professional knowledge required to conduct the audit.	○	○	○	○	◉	○
4 The auditors conducted themselves professionally during the audit.	○	○	○	○	◉	○
5 The OAG's audit program was undertaken in a timely manner.	○	○	○	○	◉	○
6 The auditors were responsive to our needs.	○	○	○	◉	○	○
7 Senior audit staff were appropriately involved in the audit.	○	○	○	○	◉	○

8 Overall, how would you rate the **quality of the audit process**?

Very Poor 1	2	3	4	5	6	7	8	9	Excellent 10
○	○	○	○	○	○	○	◉	○	○

9 Do you have any comments or suggestions for improvement regarding the **process** for your organisation's 2024-25 annual financial report audit? In particular, if you disagreed or strongly disagreed with any of Questions 1-7, please explain why.

Audit ran well, was on time and issues or findings were discussed first prior to any recommendations on the management report.

B. Audit Reporting

Please indicate the extent of your agreement or disagreement with the following statements. Please respond on the basis of your experience with the OAG's reporting of your organisation's **2024-25 annual financial report audit**.

	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Not Applicable/ Unsure
10 We had adequate opportunity to comment on the audit findings and issues before the management letters were formally issued.	○	○	○	○	◉	○
11 The OAG's management letters communicated the audit findings and issues clearly.	○	○	○	○	◉	○
12 The OAG's management letters were balanced and fair.	○	○	○	◉	○	○
13 The OAG's management letters were issued in a timely manner.	○	○	○	○	◉	○
14 The Auditor General's audit opinion was issued in a timely manner.	○	○	○	○	◉	○

15 Overall, how would you rate the **quality of the OAG's reporting** related to your organisation's 2024-25 annual financial report audit?

Very Poor 1	2	3	4	5	6	7	8	9	Excellent 10
○	○	○	○	○	○	○	◉	○	○

16 Do you have any comments or suggestions for improvement regarding the OAG's **reporting** of your organisation's 2024-25 annual financial report audit? In particular, if you disagreed or strongly disagreed with any of Questions 10-14, please explain why.

C. Value of the OAG's annual financial report audit

Please indicate the extent of your agreement or disagreement with the following statements about the **value of the OAG's annual financial report audit**.

	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Unsure
17 We value the assurance we obtain from the annual audit of our financial statements.	○	○	○	○	◉	○
18 We value the OAG's recommendations to improve the financial management of our organisation.	○	○	○	◉	○	○

19 Overall, how would you rate the **value** of the OAG's annual financial report audit?

Very Low 1	2	3	4	5	6	7	8	9	Very High 10
○	○	○	○	○	○	○	◉	○	○

20 Please indicate the extent of your agreement or disagreement with the following statements about **additional products and services the OAG provide**.

Additional products and services the OAG provide are valuable to our entity:	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Unsure
a Better practice guides	○	○	○	◉	○	○
b Annual Audit Results Report to Parliament	○	○	◉	○	○	○
c General Computer Controls report to Parliament	○	○	◉	○	○	○
d Entry and exit briefing documents	○	○	○	◉	○	○
e Audit Committee attendance and briefings	○	○	○	◉	○	○

21 Do you have any comments or suggestions for improvement regarding the **value to your organisation** of the OAG's annual financial report audit? In particular, if you disagreed or strongly disagreed with any of Questions 17-18 and 20, please explain why.

The contractors William Buck who undertake the Audit do an excellent job in providing the assurance and improvements which are always welcomed.

D. General comments and organisational information

22 Are there any **general comments** you wish to make about the Office of the Auditor General's performance or any of the issues covered in the questionnaire?

The cost of audit is significant to a small rural council and continue to increase year by year. In my experience the contractor does an excellent job in conducting the hands-on audit. There is some value in OAG providing some macro advice, but one would think, as appointed auditors from a panel, this should come from the contractor to reduce costs.

To assist us to analyse the survey responses, please provide the following information.

Name of person providing this questionnaire response:

Colin Ashe

Organisation to which this survey relates:

Shire of Victoria Plains

Consent

23 Do you consent to ORIMA Research providing your completed questionnaire to the Office of the Auditor General to provide direct feedback to OAG staff as part of the OAG's continuous improvement program?

- (●) Yes
- ( ) No

8 CLOSURE OF MEETING

There being no further business, the Presiding Member declared the meeting closed at 12.40 pm

These minutes were confirmed at the Audit Committee Meeting held on

Signed _____ Date _____

(Presiding member at the meeting which confirmed the minutes)

Committee Minutes are unconfirmed until they have been adopted at the following meeting of Council.