SHIRE OF KOJONUP

Audit, Risk and Improvement Committee

Agenda

7 May 2025

TERMS OF REFERENCE

AUDIT, RISK & IMPROVEMENT COMMITTEE (ARIC)

Established under Section 7.1 of the *Local Government Act 1995 (Act)* - every local government must have an Audit Risk & Improvement Committee (ARIC).

Terms of Reference

ARIC is responsible for assisting and independently advising Council in recommending appropriate actions, controls and improvements with regards to audit, risk oversight, governance, finances and systems of internal control.

Its role is to provide oversight related to significant risk exposures and control issues, including fraud risks, governance issues and other matters as necessary or requested by the CEO or Council. This is to ensure the Shire's activities are fully compliant with legislation, regulations, accounting and reporting Standards and that the Shire is executing its responsibility to the community in efficiently utilising their assets.

The ARIC is not responsible for the executive management of these functions. The ARIC will engage with management in a constructive and professional manner in discharging its advisory responsibilities and formulating its advice to Council.

The ARIC is an independent Committee of Council, advising Council on required improvements to ensure compliance.

Duties and Responsibilities:

Members of the ARIC are expected to observe the legal and regulatory obligations of the Local Government.

Committee members must not use or disclose information obtained through the ARIC except in meeting the ARIC's responsibilities, or unless expressly agreed by the President of the Shire.

Committee Members must adhere to the Code of Conduct for Council Members, Committee Members and Candidates and demonstrate behaviour which reflects the Shire's desired culture.

ARIC Members are expected to:

1. act in the best interests of the Shire as a whole;
2. apply good analytical skills, objectivity and good judgement;
3. express opinions constructively and openly, raise issues that relate to the ARIC's responsibilities and pursue lines of enquiry in relation to the "Risk Controls" the Shire has in place;
4. contribute the time required to meet their responsibilities; and
5. exercise due care, diligence and skill when performing their duties.

Member Duties/Responsibilities:

- Oversee the Shire's risk management, through:
  a) Biennial review of the Shire's Risk Management Policy;
  b) Recommending and reviewing the Shire's Risk Appetite Statement in order to recommend the organisation's Risk Tolerance to the Council;
  c) Reviewing reports on the movement of the Shire's current strategic risks, and the emergence of new strategic risks;
  d) Overseeing strategic risks which sit outside of the Shire's Risk Appetite ; and
  e) Monitor and receive reports concerning the development, implementation and on-going management of the Shire's Risk Management Plan and the effectiveness of its Risk Management Framework;

- Overseeing the Shire's processes for managing fraud and corruption, by:
  a) Performing oversight responsibilities and advising Council;
  b) Enquiring with the CEO and the Office of the Auditor General (OAG) about whether they are aware of any actual, suspected, or alleged fraud or corruption affecting the Shire; and
  c) Reviewing summary reports from the CEO on communication from external parties including regulators that indicate problems in the internal control system or inappropriate management actions.
- Overseeing the Shire's financial management and legislative compliance, by:
  a) Reviewing the Shire's annual Compliance Audit Return and reporting the results of that review to Council, in accordance with the Local Government (Audit) Regulations 1996;
  b) Receiving and reviewing reports from the CEO regarding the appropriateness and effectiveness of the Shire's legislative compliance and ensuring any non-compliances are rectified on a timely basis;
  c) Considering and recommending adoption of the annual financial report to Council;
  d) Receive and review the biannual reports from the Chief Executive Officer (CEO) regarding the appropriateness and effectiveness of the Shire's risk management, internal controls and legislative compliance and make recommendations to Council; and
  e) Consider and recommend adoption of the Annual Financial Report to the Council;
- Overseeing the internal audit function, by;
  a) Assessing and making a recommendation to Council on an Internal Audit Plan to ensure that it comprehensively covers material business risks that may threaten the achievement of strategic objectives and which identifies key risks and control mechanisms;
  b) Reviewing the quality and timeliness of internal audit reports;
  c) Monitoring the implementation of internal audit recommendations; and
  d) Considering the implications of internal audit findings on the organisation, its risks, and controls.
- Fulfilling responsibilities pertaining to external audit, by:
  a) Reviewing reports from the OAG, including auditor's reports, closing reports and management letters;
  b) Reviewing management's response to OAG findings and recommendations;
  c) Monitoring the implementation of recommendations from external audits;
  d) Reviewing results of relevant OAG audit reports and better practice publications for guidance on good practices, including any assessment by the CEO; and
  e) Examine the reports of the auditor after receiving a report from the CEO on the matters and:
    a. determine if any matters raised require action to be taken by the Shire; and
    b. ensure that appropriate action is taken in respect of those matters.

Seek information or obtain expert advice through the CEO on matters of concern within the scope of the Committee's terms of reference following authorisation from the Council.

- Fulfilling responsibilities pertaining to reviewing and advising on service area and process changes (Continuous Improvement) to ensure compliance, by:
  f) Reviewing reports and reviews by the CEO on key service processes within the Shire;
  g) Reviewing management's response to OAG findings and recommendations;
  h) Monitoring the implementation of recommendations;
  i) Reviewing results of relevant OAG audit reports and better practice publications on good practice, including any assessments by Management.

Membership

One (1) Independent Chair Role (Presiding Member of Committee);
One (1) Independent Deputy Presiding Member Role;
Four (4) Councillors; and

One (1) Community Member.

The independent roles will be advertised and selected by Council.

Supporting Team Members

Manager Financial and Corporate Services
Governance and Rates Officer
Chief Executive Officer or delegated nominee

Meetings

Quarterly for ordinary meetings and as required related to audit functions.

Voting: Voting is in accordance with Section 5.21 of the *Act*.

Confidentiality: All Committee members will be required to adhere to the Shire's confidentiality requirements as per the Code of Conduct for Council Members, Committee Members and Candidates.

Conduct of Meetings: ARIC Meetings will be held in accordance with the *Act*, subsidiary legislation, and the Shire's Standing Orders.

Committee Sitting Fees and Reimbursements

The Local Government Amendment Act 2023, assented to on 18 May 2023, changes the Local Government Act 1995 to provide for independent committee members to receive meeting fees. An independent committee member is a committee member who is not an elected member or an employee of the local government.

The Salaries and Allowances Tribunal (SAT) has issued a Determination to allow for the payment of meeting fees to independent committee members. Local governments will have the ability to set appropriate fees, within a specified range as determined by the SAT.

The Council will determine the amount of fees payable for independent members when it considers the budget fees and charges on an annual basis.

At this point in time the meetings fees are $0 (Zero). However, reimbursement of approved expenses for independent members may be paid to each independent external members in accordance with Section 5.100 of the *Act*.

AGENDA FOR AN AUDIT, RISK AND IMPROVEMENT COMMITTEE MEETING TO BE HELD ON 7 MAY 2025

TABLE OF CONTENTS

AGENDA

1 DECLARATION OF OPENING

The Chairman will declare the meeting open at _______ am and alert the meeting of the procedures for emergencies including evacuation, designated exits and muster points.

2 ATTENDANCE, APOLOGIES & LEAVE OF ABSENCE

MEMBERS

Cr Roger Bilney	Member
Cr Mick Mathwin	Member
Cr Kerryn Mickle	Member
Cr Paul Webb	Member
Cathrine Ivey	Community Member (Chairperson)
Jill Mathwin	Community Member

STAFF (OBSERVERS)

Grant Thompson	Chief Executive Officer
Tonya Pearce	Governance and Rates Officer

APOLOGIES

3 SUMMARY OF RESPONSE TO PREVIOUS QUESTIONS TAKEN ON NOTICE

Nil

4 CONFIRMATION OF MINUTES

Audit & Risk Committee Meeting held 5 February 2025 (Attachment 4.1)

OFFICER RECOMMENDATION

That the minutes of the Audit & Risk Committee Meeting held on 5 February 2025 be confirmed as a true and accurate record.

5 BUSINESS ARISING

6 DECLARATIONS OF INTEREST

7 SENIOR MANAGEMENT TEAM DISCUSSION

In accordance with the Financial Management Review adopted in February 2019, one senior manager will attend the Audit & Risk Committee on a rotational basis to discuss the following:

- Update on Manager’s areas of responsibility and current projects/issues;
- Questions on Notice from the Audit and Risk Committee;
- Management’s own recommendations for improvement in key areas.

Jill Johnson – Manager Finance & Corporate Services

- Cashflow and Audit Update
- ERP – Payroll Module Implementation
- Update on Financial End of Month processes

8 COMMITTEE TIMETABLE

As a guide and subject to availability, each Audit & Risk Committee agenda will contain the following (list to be expanded at the suggestion of members):

1st Quarter (January – March)

- Committee Status Report
- Compliance Audit Return
- Summary of Risk Management
- Volunteer Management
- Leave Provision Adequacy

2nd Quarter (April – June)

- Committee Status Report
- Summary of Risk Management
- Business Continuity Plan Review

3rd Quarter (July – September)

- Committee Status Report
- Interim Audit Report
- Summary of Risk Management
- Insurance Overview

4th Quarter (October – December)

- Committee Status Report
- Audit Report & Management Letter
- Annual Financial Report
- Annual Report
- Financial Management Review (each 3 years – 2021, 2024…)
- Risk, Legal Compliance & Internal Controls review (each 3 years – 2021, 2024…)
- Summary of Risk Management

The above list will remain at the commencement of each Committee agenda to act as a timetable and enable members to add to the items to be considered.

9 COMMITTEE ISSUES/ACTION STATUS REPORT

Issue / Action #	Issue Description	Actions	Actions Assigned Owner	Due By Date	Category	Priority	Urgency	Action Approved	Risk	Comments/Variance Reporting on progress	Status	Estimated Completion Date	Closed Date	% ACTION COMPLETE
3	CEO and MFCS to look into feasibility of reduction in insurance premiums if the Shire was to increase insurance excesses	Requested with Insurer, assessing impact, not a straight correlation. MFCS to update ARC at next meeting	MFCS	1/04/2025	Insurance	LOW	Urgent - 2 months	NO	LOW	Commenced, requested status verification from LGIS in writing. Ongoing risk assessment	*In Process*	1/05/2025		50%
4	Boscabel Hall	MPS – check if people camping in grounds, arrange Boscabel Hall playground check.	MPS	1/01/2025	Asset	VERY HIGH	Urgent - 2 months	YES	HIGH	Referred to Police.	*In Process*	1/03/2025		85%
5	Volunteers insurance	CEO to research.	CEO	1/04/2025	Insurance	LOW	Urgent - 2 months	NO	LOW	Ongoing assessment of the value proposition versus the risk, discussion with LGIS	*In Process*	1/05/2024		50%
6	DFES & LGIS Coverage	As a result of unfavourable Yalgoo Media the Shire to determine its asset insurance cover for disaster or minor disaster damage particularly on road damage.	MFCS	30/05/2025	Insurance	HIGH	Urgent - 2 months	YES	HIGH		*In Process*	30/05/2025		5%
7	WATC Schedule	Provide the Audit Committee with visibility over the WATC Schedule	MFCS	30/05/2025	Financial Reporting	MEDIUM	Must Have - 6 months	YES	LOW		*In Process*	30/05/2025		5%

10 SUMMARY OF RISK MANAGEMENT

10.1 RISK MANAGEMENT UPDATE

Please refer to the following attachments:

10.1.1 Risk Control Register

10.2 WORK HEALTH AND SAFETY

10.2.2 CEO Safety update - WHS

11 OFFICER REPORTS

11.1 BUSINESS CONTINUITY AND DISASTER RECOVERY PLAN – ANNUAL REVIEW

AUTHOR	Tonya Pearce – Governance and Rates Officer
DATE	Monday, 28 April 2025
FILE NO	CM.PLN.1; RM.POL.1
ATTACHMENT(S)	11.1.1 – Business Continuity and Disaster Recovery Plan (BCDRP) May 2025 (showing changes)

‘PLACEMAKING’ STRATEGIC COMMUNITY PLAN JULY 2023 TO JUNE 2033 To be *“The Cultural Experience Centre of the Great Southern”* STRATEGIC/CORPORATE IMPLICATIONS		
Key Strategic Pillar/s	**Community Goal/s**	**Corporate Objective/s**
Performance	12. A High Performing Council	12.2 SoK monitoring and reporting

DECLARATION OF INTEREST

Nil

SUMMARY

To consider and recommend to Council the reviewed and updated Business Continuity and Disaster Recovery Plan.

BACKGROUND

The Council last reviewed its Business Continuity and Disaster Recovery Plan (Plan) in May 2024.

COMMENT

A Business Continuity and Disaster Recovery Plan, provides guidance at a time when an organisation may be under considerable duress following a disaster that has affected, or in the event of a pandemic continues for some time to affect, the ability to provide essential or required services. Such a Plan identifies priorities and the resources required to return services in as quick and efficient manner as possible or to guide the organisation through a sustained event, aiming to minimise negative impact. Due to the upheaval that may be caused by such events, including dealing with the confusion that may accompany them, a well thought out Plan containing current, up to date information is a vital resource.

Changes to the current Plan are tracked and shown in coloured font in the attachments and relate to changes in personnel roles and contact details.

CONSULTATION

Chief Executive Officer
All Managers

STATUTORY REQUIREMENTS

Local Government Act (1995): s 5.56. Planning for the future

(1) A local government is to plan for the future of the district.

(2) A local government is to ensure that plans made under subsection (1) are in accordance with any regulations made about planning for the future of the district.

POLICY IMPLICATIONS

The Plan is completed in accordance with Council's Risk Management Policy 2.3.4.

FINANCIAL IMPLICATIONS

Nil

RISK MANAGEMENT IMPLICATIONS

The Plan represents part of the Shire's Risk Management documentation. It is vital, from a business continuity and disaster recovery perspective, that details within such a Plan are as current as possible and regular reviews are undertaken.

ASSET MANAGEMENT IMPLICATIONS

Nil

SOUTHERN LINK VROC (VOLUNTARY REGIONAL ORGANISATION OF COUNCILS) IMPLICATIONS

Nil

VOTING REQUIREMENTS

Simple Majority

OFFICER RECOMMENDATION

That it be recommended to the Council that the updated Business Continuity and Disaster Recovery Plan May 2025, as presented, be adopted.

12 CEO UPDATES

12.1 Springhaven Hall & Prior Lease Assignment Update

12.2 Summary of Risk Management Review Presentation

12.3 Enterprise Bargaining Agreement Update with the Australian Services Union

12.4 Cyber Hygiene Report Update

13 OTHER ITEMS FOR DISCUSSION OR FURTHER RESEARCH AS RAISED BY MEMBERS

14 NEXT MEETING

The next meeting of the Audit and Risk Committee is scheduled to be held Wednesday, 6 August 2025 at 9:00am.

15 CLOSURE

There being no further business to discuss, the Chairperson thanked members for their attendance and declared the meeting closed at _____am.

ATTACHMENTS (SEPARATE)

4.1 - Unconfirmed Audit & Risk Committee Minutes 5 February 2025

10.1.1 - Risk Control Register

11.1.1 - Business Continuity and Disaster Recovery Plan May 2025 (showing changes)

12.1.1 - Springhaven Hall & Prior Lease Assignment Update

12.4.1 - Cyber Hygiene Report Update

Kojonup
One community, many choices

2025 SoKO ARIC RISK CONTROL REGISTER:

Key Risk #	Key Risk	Issue / Action #	Risk Control Current Actions	Due By Date	Actions Assigned Owner (SPA)	Department	Category	Risk	Control	Priority	Action Approved	Action Funded	Start Date	Actual Completion Date	Status	% Complete	Comments/Variance Reporting on progress
1	Asset Sustainability Practices	1.1	Restrict access to non-compliant/damaged/dangerous buildings until the future of these facilities is determined.	May-25	MPS	Property Services	Asset Management	HIGH	Effective	HIGH - 6 to12 Months	YES	YES	1/07/2024	1/08/2025	Completed	100%	Structural Changes implemented
		1.2	Implement actions in Risk Assessment Report Showgrounds	Dec-23	CEO	Property Services	Asset Management	MODERATE	Inadequate	MODERATE - 1 year +	YES	YES	1/07/2024		Ongoing	30%	Projects commenced to reduce cost effective risks identified. Ongoing. Budget allocation required each year.
		1.3	MOU for Community Halls	Jul-23	PMRS	Office of the CEO	Contract Management	MODERATE	Adequate	MODERATE - 1 year +	YES	YES	1/07/2024		*In Process*	20%	In process
		1.4	Review and Update Long Term Asset Management Plan, Road Plan, P&E Plan	May-25	MPS	Property Services	Integrated Planning	MODERATE	Adequate	MODERATE - 1 year +	YES	NO	1/07/2024		*In Process*	65%	MWI working on comleting the long term plans
		1.5	Assess Cultural surveys on managed reserves to create a heritage inventory list	Dec-25	MPS	Property Services	Asset Management	EXTREME	Inadequate	URGENT - 1 to 6 months	YES	NO	20/11/2024		*In Process*	5%	Recent mitigation activities highlights gaps in the Shire process. Reviwing the procedures in roads and other activities to identify sensitive areas
2	Business & Community Disruption	2.1	Review and test LEMA Plan	Apr-24	CESM	Regulatory	Emergency Services	HIGH	Adequate	MODERATE - 1 year +	YES	YES	1/07/2024		*In Process*	50%	Desktop exercise being undertaken at LEMC on Monday 5th May 2025.
		2.2	Commence annual building inspections	Mar-24	MPS	Property Services	Asset Management	HIGH	Inadequate	HIGH - 6 to12 Months	YES	YES	14/07/2024	1/09/2024	Ongoing	100%	Building inspections for 2024 completed by Property team, now preparing 2025 inspections program
		2.3	Implementing Bushfire Risk Mitigation Plans for individual assets	Jul-25	MPS	Regulatory	Emergency Services	HIGH	Adequate	HIGH - 6 to12 Months	YES	YES	1/10/2024		Ongoing	10%	BRMP completed March 2024, Extreme risk sites considered and mitigation plans commenced being developed for the extreme risk sites.
		2.4	Create CESM fulltime role to include Mitigation	Apr-25	CEO	Office of the CEO	Emergency Services	HIGH	Inadequate	HIGH - 6 to12 Months	YES	NO	1/04/2024		Completed	100%	Concept role created, funding sign off from Council required, MOU with Shires and DFES requires review March 2025. Council approved reamining in current program for a longer transition timeframe
3	Failure to Fulfil Compliance Requirements (Statutory, Regulatory)	3.1	Governance Officer Role reporting to CEO	Jan-25	CEO	Office of the CEO	Governance	Low	Adequate	URGENT - 1 to 6 months	YES	YES	1/07/2024	1/10/2024	Completed	100%	Workforce Plan adopted by Council, Structural roles in place
		3.2	Internal Audits	Aug-25	CEO	Finance & Corporate Services	Finance	HIGH	Adequate	HIGH - 6 to12 Months	YES	YES	1/03/2025		Ongoing	100%	Being considered post audit. 2025 project
		3.3	Process Review	Mar-25	CEO	Office of the CEO	Governance	HIGH	Inadequate	MODERATE - 1 year +	YES	NO	1/03/2025		Ongoing	25%	Internal process review in key areas required. One functional area per year to be considered. Finance and HR first of the rank
		3.4	Data Collection Review	Apr-25	CEO	Office of the CEO	Governance	HIGH	Inadequate	MODERATE - 1 year +	YES	NO	1/03/2025		*In Process*	90%	Compliance Audit data, KPI data and other critical reporting data required. New system reliant, 2025
4	Document Management Processes	4.1	Formation of Position Descriptions for Volunteers - progressing.	Apr-22	CEO	Office of the CEO	Governance	Moderate	Adequate	URGENT - 1 to 6 months	YES	YES	1/07/2024	1/12/2024	Completed	95%	SOP's and Induction required for BFB Volunteers. Rolling out backend of 2025
		4.2	Record Keeping Plan undertaken	Jan-24	CEO	Office of the CEO	Governance	Moderate	Adequate	MODERATE - 1 year +	YES	YES	1/04/2025		*In Process*	25%	Due for review 2025. New reocrds officer revieiwing the plan
		4.3	Train internal Records Officer	Feb-25	CEO	Office of the CEO	Governance	High	Inadequate	URGENT - 1 to 6 months	YES	YES	1/12/2024		Completed	100%	Recruitment and selection for new records officer required, advertising commenced
		4.4	New Electronic Documents Records Management System (EDRMS) to be tendered and implemented	Feb-25	CEO	Office of the CEO	Governance	Moderate	Inadequate	HIGH - 6 to12 Months	YES	YES	1/02/2025		Completed	100%	Tender closed, Preferred vendor identified. Implemented
		4.5	Record Processes to be reviewed and processes and procedures for Team Members in executing to be instigated	Mar-25	CEO	Office of the CEO	Governance	Moderate	Inadequate	URGENT - 1 to 6 months	YES	YES	1/02/2025		*In Process*	50%	Aligned to system implementation. New records officer review underway
5	Employment Practices	5.1	HR Process Review	Apr-25	MFCS	Finance & Corporate Services	Human Resource	MODERATE	Adequate	MODERATE - 1 year +	YES	NO	1/03/2025		*In Process*	20%	Hire to Retire (H2R) review of all Policies, Processes, Procedures, Templates and Documentation. Newly appointed HR Coordinator reviewing HR framework
		5.2	Finalise EBA WASU	Dec-24	CEO	Office of the CEO	Human Resource	LOW	Effective	URGENT - 1 to 6 months	YES	YES	1/08/2024		*In Process*	30%	Commenced Negotiations. In principle agreement being drafted.
		5.3	Update & Standardise Templates for use	Dec-25	MFCS	Finance & Corporate Services	Human Resource	LOW	Adequate	MODERATE - 1 year +	YES	NO	1/03/2025		*Not Started*		Aligned HR Process review. Underway
		6.1	Stakeholder Engagement Plan to be created	Apr-25	CEO	Office of the CEO	Community	HIGH	Inadequate	URGENT - 1 to 6 months	YES	NO	1/02/2025		*In Process*	50%	CEO to create plan and present to Council. Stakeholder plan 50% completed

6	Engagement practices	6.2	Review Legislative requirement for Communications Plans	Feb-25	GRO	Office of the CEO	Community	MODERATE	Not Rated	URGENT - 1 to 6 months	YES	YES	1/12/2024		Completed	100%	CEO to progress and stakeholder plan to be established
7	Environment Management	7.1	NRM Committee Reestablished	Oct-24	CEO	Office of the CEO	Climate Resilience	MODERATE	Inadequate	HIGH - 6 to12 Months	YES	YES	1/09/2024	1/10/2024	Ongoing	100%	Committee reestablished and working on NRM Operational Plan
		7.2	Great Southern Climate Alliance Created and effective	Nov-24	CEO	Office of the CEO	Climate Resilience	LOW	Not Rated	HIGH - 6 to12 Months	YES	YES	1/10/2024	1/12/2024	Ongoing	100%	Climate Alliance established and strategies formed
8	Errors, Omissions and Delays	8.1	Implement an organisational processes & Policy review	Dec-25	CEO	Office of the CEO	Governance	MODERATE	Inadequate	MODERATE - 1 year +	YES	NO	1/01/2025		*In Process*	20%	Key areas being reviewed by relevant Managers
9	External Theft and Fraud (inc. Cyber Crime)	9.1	CCTV Project being Implemented	Feb-25	CEO	Office of the CEO	Community	MODERATE	Inadequate	HIGH - 6 to12 Months	YES	YES	1/10/2024		Completed	100%	CCTV Contractor implementing networks and cameras, expected Mid february completion as per contract
		9.2	Update fixed assets record (RAMM) to include Parks, Reserves, street furniture and signage and drainage infrastructure	Apr-25	MWI	Works & Infrastructure	Asset Management	MODERATE	Not Rated	MODERATE - 1 year +	NO	NO			*Not Started*		
		9.3	Managed Services Firewalls upgraded	Apr-24	CEO	Office of the CEO	Governance	EXTREME	Adequate	URGENT - 1 to 6 months	YES	YES	15/11/2024	1/12/2024	Completed	100%	Upgraded December 2024 - Outsourced to Ramped Technology. Refer to Cyber Report
10	Management of Facilities, Venues and Events	10.1	Draft improved Events planning process guidelines (including Planning Approvals, risk assessments, event management plans, food safety at stalls etc) - progressing	Apr-25	PMRS	Regulatory Services	Regulatory	MODERATE	Adequate	MODERATE - 1 year +	YES	NO	1/02/2025		*Not Started*		
		10.2	Develop post event procedures and event evaluation debrief - progressing	Apr-25	MPS	Property Services	Regulatory	MODERATE	Inadequate	MODERATE - 1 year +	YES	NO	1/03/2025		*Not Started*		
		10.3	Develop Lease agreements register for all Shire facilities - progressing community hall agreements, sporting group agreements	Jul-25	CEO	Office of the CEO	Governance	HIGH	Inadequate	URGENT - 1 to 6 months	YES	YES	1/10/2024		*In Process*	30%	Governance Officer and CEO have reviewed all Contracts and Leases and Agreements. Identifeid all actions and required renewals. Draft Sports leases drafted for CEO review
		10.4	Community education re public events on private property - progressing	Mar-25	PMRS	Regulatory Services	Regulatory	MODERATE	Inadequate	MODERATE - 1 year +	YES	NO	1/03/2025		*In Process*		
		10.5	Annual tenancy inspections for staff and public housing - scheduled & notice in writing	Mar-25	MPS	Property Services	Asset Management	MODERATE	Adequate	HIGH - 6 to12 Months	YES	YES	1/07/2024	1/07/2025	Ongoing	100%	MPS has undertaken inspections for the current year.
11	IT, Communication Systems and Infrastructure	11.1	Add additional generator input points (Admin building)	Jul-23	MPS	Property Services	Emergency Services	MODERATE	Inadequate	MODERATE - 1 year +	NO	NO			*Not Started*		
		11.2	Negotiate Service level agreement with Vendors - IT	Jun-22	CEO	Office of the CEO	ICT	HIGH	Adequate	URGENT - 1 to 6 months	YES	YES	1/07/2024	1/09/2024	Completed	100%	Tender closed, Preferred vendors identified
		11.3	ERP System Upgrade	Mar-25	CEO	Office of the CEO	ICT	HIGH	Adequate	MODERATE - 1 year +	YES	YES	1/09/2024		*In Process*	10%	Vendor Selected, agreement signed, PO issued, Project to be executed. Payroll module project has kicked off expected go live date July 2025.
		11.4	ICT Managed Service Upgrades	Oct-24	CEO	Office of the CEO	ICT	HIGH	Adequate	URGENT - 1 to 6 months	YES	YES	2/09/2024	1/02/2025	Completed	100%	Vendor selected, New Managed Service framework provision executed and supported
12	Misconduct	12.1	Hire to Retire (H2R) process review	Apr-25	MFCS	Finance & Corporate Services	Human Resources	MODERATE	Adequate	MODERATE - 1 year +	YES	YES	1/01/2025		*In Process*	65%	Advertised new Records and Human Resource Role, fully funded in budget. New HR Coordinator appointed and made headway on review.
		12.2	Implement user-friendly stock control and reconciliation (fuel) procedure - Finance to work with Depot	Mar-25	CEO	Office of the CEO	Finance	HIGH	Inadequate	URGENT - 1 to 6 months	YES	YES	1/01/2025		*In Process*	8%	MWI researching new control and storage systems for fuel management
13	Project/Change Management	13.1	Implement formal project management guidelines	May-25	CEO	Office of the CEO	Project Management	HIGH	Adequate	URGENT - 1 to 6 months	YES	YES	1/07/2024	1/02/2025	Completed	100%	PM Framework setup and implemented
		13.2	Train Team Members in Project Management Body of Knowledge	Jun-25	CEO	Office of the CEO	Project Management	MODERATE	Inadequate	URGENT - 1 to 6 months	YES	YES	1/02/2025		Ongoing	25%	Initial internal training of users underway
		13.3	Project Management Reporting to Council to commence	Feb-25	CEO	Office of the CEO	Project Management	HIGH	Inadequate	URGENT - 1 to 6 months	YES	YES	25/02/2025		Ongoing	50%	Draft reports established, Data collection underway
		14.1	Conduct annual evacuation drill at all facilities	Apr-25	CEO	Office of the CEO	Emergency Services	HIGH	Inadequate	URGENT - 1 to 6 months	YES	YES	1/01/2025		*In Process*	10%	

14	Safety and Security Practices	14.2	Process review for safety documentation	Dec-24	MWI	Works & Infrastructure	Safety	HIGH	Inadequate	HIGH - 6 to12 Months	YES	YES	1/08/2024		Ongoing	75%	Skytrust Integrated Safety Management System (ISMS) implemented, new document templates being uploaded, Team Members being trained in usage.
		14.3	Safety Culture change program developed	Dec-24	CEO	Office of the CEO	Safety	HIGH	Adequate	URGENT - 1 to 6 months	YES	YES	1/07/2024		Ongoing	75%	ISMS being rolled out, safety culture strategy plan set.
15	Supplier and Contract Management	15.1	Contract Management Framework Review and Implementation	Mar-25	PMRS	Office of the CEO	Safety	HIGH	Inadequate	MODERATE - 1 year +	YES	YES	1/07/2024		*In Process*	70%	Contract and Contractor Management framework reviewed and improvements identified
		15.2	WHS Contractor Handbook to be created and approved	Feb-24	PMRS	Office of the CEO	Safety	MODERATE	Inadequate	MODERATE - 1 year +	YES	YES	1/07/2024		*In Process*	85%	Completion of draft underway
		15.3	Induction process for Contractors	Dec-24	PMRS	Office of the CEO	Safety	HIGH	Adequate	MODERATE - 1 year +	YES	YES	1/07/2024		*In Process*	65%	Induction process being finalised
16	Financial & Process Sustainability Practices	16.1	Cash Flow Budget and reporting to be implemented	Jan-25	MFCS	Office of the CEO	ICT	MODERATE	Effective	URGENT - 1 to 6 months	YES	YES	1/10/2024		Completed	100%	Cashflow analysis and monitoring now underway on weekly basis
		16.2	Training Program for non financial Team Members	Sep-25	MFCS	Finance & Corporate Services	Finance	HIGH	Inadequate	MODERATE - 1 year +	YES	NO	1/03/2025		*Not Started*		
		16.3	Layered Auditing Program (internal) - PO's and other financial management controls	Sep-25	MFCS	Finance & Corporate Services	Finance	HIGH	Inadequate	HIGH - 6 to12 Months	YES	YES	1/07/2025		Ongoing	90%	Audit demonstrates new controls are implemnented, however there is still some work to be undertaken to improve financial controls
		16.4	Debtors Management	Nov-25	MFCS	Finance & Corporate Services	Finance	HIGH	Adequate	URGENT - 1 to 6 months	YES	YES	1/08/2024		Completed	100%	New Debtor Officer has implemented a new process for collecting and following up on outstanding debts.
		16.5	Leave Provision Management	Mar-25	MFCS	Office of the CEO	ICT	HIGH	Effective	URGENT - 1 to 6 months	YES	YES	1/01/2025		*Not Started*		ERP Vendor contracted

SHIRE OF KOJONUP

Business Continuity & Disaster Recovery Plan

MAY 20254

Contents

1. Key Contact Sheet

Person	Position	Mobile Number	Responsibilities Incident Response (IR) Team Leader
Grant Thompson	Chief Executive Officer	0419 903 363	IR Team Leader
~~Craig McVee~~Darryn Watkins	Manager Works ~~&~~ ~~Services~~and Infrastructure	~~0427 427 854~~ 0436 962 954	IR Team Member
~~Robert Jehu~~Estelle Lottering	Fire Warden – Shire Office	N/A	IR Team Member
	Fire Warden – Depot Office		IR Team Member
	~~Fire Warden – Springhaven Lodge~~	~~0417 994 608~~	~~IR Team Member~~
	Fire Warden – The Kodja Place	~~0417 987 237~~	IR Team Member
~~Tonya Pearce~~	~~IT Officer~~		~~IR Team Member~~
Cr Roger Bilney	Shire President	0428 341 012	Shire President

Contact List – External

Key contacts	Contact number/s
Police and Emergency Services	000
Kojonup Police Station	9831 2555
Ambulance	000
Kojonup Hospital	9831 2222
Security	ABA Security Albany – 9841 7828/BJ Systems – 9309 9595 (Complex)
Insurance company	LGIS – David Wood – 9483 8888
Key Suppliers	Albany Lock Service – Craig - 9842 9779
Electrician	BK Thompson – Ryan 98 31 1106
Plumber	Egabeva Plumbing – Derek – 9831 1213
Water and Sewerage	131375
Electricity	Western Power - 131351
Telephone	Telstra – Johnathan Thornton – 9726 7324
IT Provider~~Support~~	Ramped Technology - Garry Hammersley - 9892 2922
Primary Business System Software – IT Vision	9315 7000
Internet Service Provider – Optus	13 56 67
WA Local Government Association	9213 2000
ABC Radio Great Southern	9842 4011
Department of Transport Licensing (Albany)	13 11 56
State Records Office	9427 3600
Bank/Building Society	NAB – Matteo Libera– 9831 2700
Accountant (Auditor)	Lincoln's – ~~Russell Harrison~~ Thomas Warner – 9841 1200
Lawyer	McLeod's – 9383 3133

2. Introduction and Objectives

The purpose of developing a Business Continuity and Disaster Recovery Plan (Plan) is to ensure the capability of the Shire of Kojonup to continue to deliver its services at an acceptable level during or following a disruptive incident or disaster.

A disaster is defined as a serious disruption of the functioning of the Shire of Kojonup causing widespread human, economic or environmental loss or disturbance. Such disasters include incidents like fire, flood, earthquake, epidemic or pandemic.

A disaster recovery plan uses measures such as alternative premises or alternative service delivery and other facilities to ensure that a business can continue operations and if not, restore operations as quickly as possible after a calamity.

The objectives of this Plan enable the Shire to:

- Ensure we are prepared prior to an event
- Define prioritise and re-establish critical business functions as quickly and efficiently as possible;
- Follow a systematic plan for the management of any incident or disaster;
- Detail the immediate response to minimise damage or loss during a critical incident;
- Minimise the effect of an incident on the community, staff and Council; and
- Review and update this plan on a regular basis.

The Shire recognises that some events may exceed the capacity of routine management methods and structure. The Plan aims to provide a mechanism for the development of contingent capacity and logical plans that will enable management to focus on maintaining and resuming the Shire's most critical functions; whilst working in a practical way toward eventual restoration of operations and ensuring unaffected operations are able to continue.

This Plan reinforces and is reinforced by the Shire's Risk Management Framework and Risk Management Policy.

This Plan will be located on the Shire website – www.kojonup.wa.gov.au and Docs-on-Tap to ensure it is always available. Copies will also be placed in the Chief Executive Officer's vehicle, all Managers' vehicles and the fireproof cabinet within the Shire's Administration building.

3. Incident Response Plans

The following incident response plans present the Incident Response Team hierarchy that shall be employed in the event of an emergency. If under extreme circumstances the Chief Executive Officer or any member of the Senior Management Team is unavailable, then the team will consist of all the remaining available senior management.

The plans are not exhaustive, as any major incident will require more detailed and potential long-term considerations; however, the plans below provide a structured response to major incidents that are of the highest threat to service provision and Shire operations.

3.1. LOSS OF ADMINISTRATION BUILDING

Types of incidents include fire, flood and earthquake (Refer to Immediate Response Checklist).

TASK 1 - Immediate Response

This task provides the necessary command and control to enable the Shire of Kojonup's Incident Response Team to conduct an initial assessment of the disaster and to co-ordinate the Shire's initial response to the disaster.

Incident Response Team

Team Leader:	Chief Executive Officer
Team Members:	Property Services and Natural Resource Manager
	~~Risk Management Co-ordinator~~Governance and Rates Officer
	Fire Warden
	Shire President (Media Liaison)

Recovery Procedure
Incident Response Team Leader/Fire Warden to undertake the following steps:

- Ensure site has been evacuated and all personnel are accounted for
- Secure site and prevent access
- Contact Emergency Services and Police
- Identify any injuries and render assistance
- Engage Incident Response Team
- Undertake an initial assessment of damage and risks
- Call- Optus and arrange the diversion of phone lines to existing Shire mobiles
- Team Leader determines time frame to switch to disaster recovery site

Recovery Time Objective
Timeframe for this activity is within 24 hours of the incident

Recovery Location

Primary Site:	Memorial Hall
Secondary site:	Works Depot

Resource requirements
Mobile phones
iPads and laptops
Charging devices (regularly checked for charge)
Personnel

Other Considerations

1. Secure the affected area as necessary
2. Restrict access to the building/site
3. Liaise with Emergency Services and Police
4. Inform Local Government Insurance Services (LGIS)

5. Inform elected members and employees
6. Liaise with Shire President to make a press release
7. Inform community where possible

TASK 2 – Commence operations from Disaster Recovery Site

This task provides the necessary steps to commence core Shire operations from the Disaster Recovery site and commence the planning for restoration of services in the short and longer term.

Incident Response Team

Team Leader:	Chief Executive Officer
Team Members:	Property Services and Natural Resource Manager IT ~~Officer~~Provider

Recovery Procedure

Undertake the following steps:

- Establish the disaster recovery site – **Chief Executive Officer**
  - Layout workspace utilising tables and chairs from the Memorial Hall
  - Source telephones, establish communications and arrange to have calls directed to mobile telephones.
  - Allocate staff to customer service and disaster recovery assistance
  - Liaise with other Incident Response Team members to determine items to be immediately replaced and what is recoverable.
  - Contact IT Vision, Shire's IT supplier (Pre-emptive Strike), stationery supplier
  - Recover backup disks from external site
  - Cancel all forward bookings of the Memorial Hall.
- Assess damage and undertake salvage operations – **Chief Executive Officer, Property Services and Natural Resource Manager**
  - Undertake initial assessment of salvageable materials, items and records, etc.
  - Contact staff to remove items to the salvage site (Town Hall or Depot)
- Co-ordinate all communications, media and elected members, Local Government insurers and general co-ordination of recovery process – Chief Executive Officer
  - Liaise with Shire President to issue a media statement
  - Co-ordinate meetings of Incident Response team
  - Authorise all immediate purchasing requirements
  - Liaise with Shire's insurers
  - Oversee Assessment and Recovery

Recovery Time Objective

It is the aim of the Recovery Plan to achieve this task within 72 hours.

Resource Requirements

- Office furniture and stationery
- Administration staff

- IT hardware and software
- Communications (land line and internet)

TASK 3 – Assess damage and prepare medium term Recovery Plans

This task provides the necessary steps to commence planning for medium term operations from the Disaster Recovery Site.

Incident Response Team

Team Leader:	Chief Executive Officer
Team Members:	Property Services and Natural Resource Manager
	~~Risk Management Co-ordinator~~Governance and Rates Officer
	IT ~~Officer~~Provider

Recovery Procedure

Undertake the following steps:

- Establish the disaster recovery site for full operations in the medium to longer term – **Chief Executive Officer**
    - Recover data to pre disaster state
    - Bring all records up to date
    - Contact all necessary persons to inform of incident, expected delays and seek documentation where necessary
    - Establish necessary equipment and infrastructure requirements to provide full operations from recovery site including demountable buildings and other office accommodation.
- Finalise damage assessment and commence planning for re-establishing services through full or partial rebuild – **Chief Executive Officer, Property Services and Natural Resource Manager**
    - Undertake assessment of building and determine action to fully or partially rebuild and make recommendation to Council.
- Co-ordinate all communications, media and elected members, Local Government insurers and general co-ordination of recovery process – **Chief Executive Officer**
    - Oversee assessment and recovery
    - Co-ordinate meetings of Incident Response Team
    - Oversee planning for medium term operation from Disaster Recovery Site (6-12 months)

Recovery Time Objective

4 weeks

Resource Requirements

- IT contractors
- Additional infrastructure as identified
- Contractors to clean up disaster site

TASK 4 – Long term Recovery Plan and relocation to permanent Shire Office building

This task provides the necessary steps to finalise planning, rebuilding and recommencement of operation from the permanent Shire office building.

Incident Response Team

Team Leader:	Chief Executive Officer
Team Members:	Property Services and Natural Resource Manager IT ~~Officer~~Provider

Recovery Procedure

Undertake the following steps: **Chief Executive Officer**

- Establish working party to:
  - Review operations for location of new premises
  - Undertake design and tendering processes
  - Oversee construction of new premises
  - Oversee commissioning of new premises
- Present review findings to Council for decision
  - Appoint architect, exterior and interior designers, engineers and other necessary assistance to design, specify and document new premises
  - Issue tenders, appoint contractor and commence construction
  - Commission new premises and commence operations from new building

Recovery Time Objective

From the commencement of this task, 4 weeks after the incident, it is the target to have all Shire functions permanently operating from the rebuilt Shire offices in 12 months.

Resource Requirements

- Planning assistance
- Consultants/architects
- Contractors

3.2. COMPLETE IT HARDWARE FAILURE

This task provides the necessary steps to recover the Shire's IT system as a result of complete failure resulting in replacement of the IT system (Refer to Immediate Response Checklist).

Incident Response Team

Team Leader:	Chief Executive Officer
Team Members:	~~Risk Management Co-ordinator~~Governance and Rates Officer
	IT Provider
	~~IT Officer~~

Recovery Procedure

Undertake the following steps:

- Assess severity of outage through the Shire's IT provider and determine likely outage time
- Seek quotations and place orders for replacement components
- Contact Shire's insurers and Police if necessary
- Inform Council, community and business contacts (i.e.; banks, creditors and contractors) of potential delays in providing services
- Set up and install new hardware/install all software and restore from backups
- Reconcile and rebuild all data

Recovery Time Objective

2 weeks

Resource requirements

IT suppliers (hardware/software, Synergy Soft, Department of Transport, Police, etc.)

3.3. LOSS OF DEPOT BUILDINGS

Types of incidents include fire, flood and earthquake (Refer to Immediate Response Checklist).

TASK 1 - Immediate Response

This task provides the necessary command and control to enable the Shire of Kojonup's Incident Response Team to conduct an initial assessment of the disaster and to co-ordinate the Shire's initial response to the disaster.

Incident Response Team

Team Leader:	Chief Executive Officer
Team Members:	Manager Works and ~~Services~~Infrastructure Property Services and Natural Resource Manager ~~Risk Management Co-ordinator~~Governance and Rates Officer Fire Warden IT ~~Officer~~Provider

Recovery Procedure
Incident response Team Leader and Fire Warden to undertake the following steps:

- Ensure site has been evacuated and all personnel are accounted for
- Secure site and prevent access
- Contact Emergency Services and Police
- Identify any injuries and render assistance
- Engage Incident Response Team
- Undertake an initial assessment of damage and risks
- Team Leader determines time frame to switch to Disaster Recovery site
- Call Optus and arrange diversion of phone lines to existing Shire mobiles

Recovery Time Objective
Timeframe for this activity is within 24 hours of being called by the Incident Response Team Leader.

Recovery Location

Primary Site:	Shire Depot Site if depot site can be utilised
Secondary site:	Land adjacent to the current depot
Third Site:	Lay down area in Industrial Estate

Resource requirements
Mobile phones
Personnel
Equipment and Stores

Other Considerations

1. Secure the affected area as necessary
2. Restrict access to the building/site

3. Liaise with Emergency Services and Police
4. Inform Local Government Insurance Services (LGIS)
5. Inform Elected Members, employees
6. Liaise with Shire President to make a press release
7. Inform community where possible

TASK 2 – Commence operations from Disaster Recovery Site

This task provides the necessary steps to commence core Shire operations from the Disaster Recovery site and commence the planning for restoration of services in the short and longer term.

Incident Response Team

Team Leader:	Chief Executive Officer
Team Members:	Manager Works and ~~Services~~Infrastructure
	Property Services and Natural Resource Manager
	~~Risk Management Co-ordinator~~Governance and Rates Officer
	IT ~~Officer~~Provider

Recovery Procedure

Undertake the following steps:

- Establish the disaster recovery site – **Manager Works ~~& Services~~and Infrastructure**
    - Establish appropriate temporary depot site on land adjacent to the current depot
    - Administration function to resume from Shire office
    - Liaise with other Incident Response Team members to determine items to be immediately replaced and what is recoverable
- Assess damage and undertaken salvage operations – **Manager Works and ~~Services~~Infrastructure, Chief Executive Officer,~~-~~ Property Services and Natural Resource Manager**
    - Undertake initial assessment of salvageable materials, items and records, etc
    - Engage staff to remove items to the land adjacent to the current depot
- Co-ordinate all communications, media and elected members, Local Government insurers and general co-ordination of recovery process – **Chief Executive Officer**
    - Liaise with Shire President to issue a media statement
    - Oversee assessment and recovery
    - Co-ordinate meetings of Incident Response Team
    - Authorise all immediate purchasing requirements
    - Liaise with Shire's insurers

Recovery Time Objective

It is the aim of the Recovery Plan to achieve this task within 72 hours.

Resource Requirements

- Office furniture and stationery
- Depot Administration and Works staff
- IT hardware and software
- Communications (land line and internet)

TASK 3 – Assess damage and prepare medium term recovery plans

This task provides the necessary steps to commence planning for medium term operations from the Disaster Recovery Site.

Incident Response Team

Team Leader: Chief Executive Officer

Team Members: Manager Works and ~~Services~~Infrastructure
Property Services and Natural Resource Manager
~~Risk Management Co-ordinator~~Governance and Rates Officer
IT ~~Officer~~Provider

Recovery Procedure

Undertake the following steps:

- Establish the disaster recovery site for full operations in the medium to longer term – **Manager Works ~~& Services~~and Infrastructure, IT ~~Officer~~Provider**
    - Establish appropriate temporary depot site on land adjacent to the current depot
    - Administration function to resume from Shire office (or alternate site)
    - Contact all necessary persons to inform of incident, expected delays and seek documentation where necessary
    - Liaise with CEO to establish necessary equipment and infrastructure requirements to provide full operations from recovery site
- Finalise damage assessment and commence planning for re-establishing services through full or partial rebuild – **Manager Works and ~~Services~~Infrastructure, Chief Executive Officer,~~-~~ Property Services and Natural Resource Manager**
    - Undertake assessment of building and determine action to fully or partially rebuild and make recommendation to Council
- Co-ordinate all communications, media and elected members, Local Government insurers and general co-ordination of recovery process – **Chief Executive Officer**
    - Oversee assessment and recovery
    - Co-ordinate meetings of Incident Response Team
    - Oversee planning for medium term operation from Disaster Recovery Site (6-12 months)

Recovery Time Objective

4 weeks

Resource Requirements

- IT contractors
- Additional infrastructure as identified
- Contractors to clean up disaster site

TASK 4 – Long term Recovery Plan and relocation to permanent Shire Depot building

This task provides the necessary steps to finalise planning, rebuilding and recommencement of operation from the permanent Shire Depot building.

Incident Response Team

Team Leader:	Chief Executive Officer
Team Members:	Manager Works and ~~Services~~Infrastructure Property Services and Natural Resource Manager Working Party appointed by Council

Recovery Procedure

Undertake the following steps: **Chief Executive Officer, Manager Works and ~~Services~~Infrastructure**

- Establish working party to:
  - Review operations for location of new premises
  - Undertake design and tendering processes
  - Oversee construction of new premises
  - Oversee commissioning of new premises
- Present review findings to Council for decision
- Appoint architect, exterior and interior designers, engineers and other necessary assistance to design, specify and document new premises
- Issue tenders, appoint contractor and commence construction
- Commission new premises and commence operations from new building

Recovery Time Objective

From the commencement of this task, after 4 weeks from the incident, it is the target to have all Shire functions permanently operating from the rebuilt Shire Depot in 12 months.

Resource Requirements

- Planning assistance
- Consultants/architects
- Contractors

3.4. LOSS OF SPRINGHAVEN LODGE

Types of incidents include fire, flood and earthquake (Refer to Immediate Response Checklist). A separate appendix (Appendix 1) is attached being the Pandemic Response Plan for use during an epidemic/pandemic.

TASK 1 - Immediate Response

This task provides the necessary command and control to enable the Shire of Kojonup's Incident Response Team to conduct an initial assessment of the disaster and to co-ordinate the Shire's initial response to the disaster.

Incident Response Team

Team Leader:	Chief Executive Officer
Team Members:	~~Manager Springhaven~~
	Property Services and Natural Resource Manager
	~~Risk Management Co-ordinator~~Governance and Rates Officer
	Fire Warden
	IT ~~Officer~~Provider

Recovery Procedure

Incident Response Team Leader/Fire Warden to undertake the following steps:

- Ensure site has been evacuated and all personnel and residents are accounted for
- Transfer of residents to Kojonup Hospital or neighbouring facilities in the interim
- Secure site and prevent access
- Contact Emergency Services and Police
- Identify any injuries and render assistance
- Engage Incident Response Team
- Undertake an initial assessment of damage and risks
- Call Optus and arrange diversion of phone lines to existing Shire mobiles
- Team Leader determines time frame to switch to disaster recovery site

Recovery Time Objective

Timeframe for this activity is within 24 hours of being called by the Incident Response Team Leader.

Recovery Location

Primary Site:	Kojonup Hospital
Secondary site:	Katanning Hospital/Nursing facilities

Resource requirements

Mobile phones
Personnel

Other Considerations

1. Secure the affected area as necessary
2. Restrict access to the building/site
3. Liaise with Emergency Services and Police
4. Inform families of residents
5. Inform Local Government Insurance Services (LGIS)
6. Inform elected members and employees
7. Liaise with Shire President to make a press release
8. Inform community where possible

TASK 2 – Commence operations from Disaster Recovery Site and Relocate residents

This task provides the necessary steps to accommodate residents in other hospitals or nursing home facilities and commence the planning for restoration of services in the short and longer term.

Incident Response Team

Team Leader: Chief Executive Officer
Team Members: ~~Manager Springhaven~~
Manager Works and ~~Services~~Infrastructure
Property Services and Natural Resource Manager
~~Risk Management Co-ordinator~~Governance and Rates Officer

Recovery Procedure

Undertake the following steps:

- Establish facilities to transfer residents from Kojonup hospital if required
- Establish the disaster recovery site – **~~Manager Springhaven~~Chief Executive Officer**
    - Source telephones, establish communications and arrange to redirect calls to landline
    - Allocate staff to customer service and disaster recovery assistance
    - Liaise with other Incident Response Team members to determine items to be immediately replaced and what is recoverable.
- Assess damage and undertaken salvage operations – **Chief Executive Officer, ~~Manager Springhaven,~~ Manager Works and ~~Services~~Infrastructure, Property Services and Natural Resource Manager**
    - Undertake initial assessment of salvageable materials, items and records, etc.
    - Contact staff to remove items to the salvage site (Town Hall or Depot)
- Co-ordinate all communications, media and elected members, Local Government insurers and general co-ordination of recovery process **– Chief Executive Officer**
    - Liaise with Shire President to issue a media statement
    - Co-ordinate meetings of Incident Response team
    - Authorise all immediate purchasing requirements
    - Liaise with Shire's insurers.

Recovery Time Objective

It is the aim of the Recovery Plan to achieve this task within 72 hours.

Resource Requirements

- Office furniture and stationery
- Administration and Works staff
- IT hardware and software
- Communications (land line and internet)

TASK 3 – Assess damage and prepare medium term Recovery Plans

This task provides the necessary steps to commence planning for medium term operations from the Disaster Recovery Site.

Incident Response Team

Team Leader:	Chief Executive Officer
Team Members:	~~Springhaven Manager – Registered Nurse~~ Manager Works and ~~Services~~Infrastructure Property Services and Natural Resource Manager ~~Risk Management Co-ordinator~~Governance and Rates Officer IT ~~Officer~~Provider

Recovery Procedure

Undertake the following steps:

- Establish the disaster recovery site for full operations in the medium to longer term – ~~Springhaven **Manager – Registered Nurse**~~ **Chief Executive Officer**
  - Recover data to pre disaster state
  - Bring all records up to date
  - Contact all necessary persons to inform of incident, expected delays and seek documentation where necessary
  - Establish necessary equipment and infrastructure requirements to provide full operations from recovery site including demountable buildings and other office accommodation
- Finalise damage assessment and commence planning for re-establishing services through full or partial rebuild – **Chief Executive Officer,** ~~**Manager Springhaven,**~~ **Manager Works and** ~~**Services**~~Infrastructure**, Property Services and Natural Resource Manager**
  - Undertake assessment of building and determine action to fully or partially rebuild and make recommendation to Council.
- Co-ordinate all communications, media and elected members, Local Government insurers and general co-ordination of recovery process – **Chief Executive Officer**
  - Oversee assessment and recovery

    - Co-ordinate meetings of Incident Response Team
    - Oversee planning for medium term operation from Disaster Recovery Site (6-12 months)

Recovery Time Objective
4 weeks

Resource Requirements

- IT contractors
- Additional infrastructure as identified
- Contractors to clean up disaster site

TASK 4 – Long term Recovery Plan and relocation to permanent Premises

This task provides the necessary steps to finalise planning, rebuilding and recommencement of operation from the permanent Shire office building.

Incident Response Team

Team Leader:	Chief Executive Officer
Team Members:	~~Manager Springhaven~~
	Manager Works and ~~Services~~Infrastructure
	Property Services and Natural Resource Manager
	Shire President

Recovery Procedure
Undertake the following steps: **Chief Executive Officer**

- Establish working party to:
    - Review operations for location of new premises
    - Undertake design and tendering processes
    - Oversee construction of new premises
    - Oversee commissioning of new premises
- Present review findings to Council for decision
- Appoint architect, exterior and interior designers, engineers and other necessary assistance to design, specify and document new premises
- Issue tenders, appoint contractor and commence construction
- Commission new premises and commence operations from new building

Recovery Time Objective
From the commencement of this task, after 4 weeks from the incident, it is the target to have all Shire functions permanently operation from the rebuilt Springhaven Lodge in 12 months.

Resource Requirements

- Planning assistance

- Consultants/architects
- Contractors

3.5. LOSS OF THE KODJA PLACE

Types of incidents include fire; flood and earthquake (Refer to Immediate Response Checklist).

TASK 1 - Immediate Response

This task provides the necessary command and control to enable the Shire of Kojonup's Incident Response Team to conduct an initial assessment of the disaster and to co-ordinate the Shire's initial response to the disaster.

Incident Response Team

Team Leader:	Chief Executive Officer
Team Members:	Manager Works and ~~Services~~Infrastructure
	Property Services and Natural Resource Manager
	~~Risk Management Co-ordinator~~Governance and Rates Officer
	Fire Warden

Recovery Procedure
Incident Response Team Leader to undertake the following steps:

- Ensure site has been evacuated and all personnel and visitors/customers are accounted for
- Secure site and prevent access
- Contact Emergency Services and Police
- Identify any injuries and render assistance
- Undertake an initial assessment of damage and risks
- Call Optus and arrange diversion of phone lines to existing Shire mobiles
- Determine time frame to switch to disaster recovery site

Recovery Time Objective
Timeframe for this activity is within 24 hours of the incident

Recovery Location

Primary Site:	RSL Hall
Secondary site:	Town Hall

Resource requirements
Mobile phones

Other Considerations

1.Liaise with Emergency Services and Police
2 Inform elected members and employees
3 Inform Press and community where possible
4 Inform Local Government Insurance Services

TASK 2 – Commence operations from Disaster Recovery Site

This task provides the necessary steps to commence core Kodja Place/Visitor Centre operations from the Disaster Recovery site and commence the planning for restoration of services in the short and longer term.

Incident Response Team

Team Leader: Chief Executive Officer
Team Members: Manager Works and ~~Services~~Infrastructure
Property Services and Natural Resource Manager
~~Risk Management Co-ordinator~~Governance and Rates Officer

Recovery Procedure

Undertake the following steps:

- Establish the disaster recovery site – **Chief Executive Officer**
  - Source telephones, establish communications and arrange to redirect calls to landline
  - Allocate staff to customer service and disaster recovery assistance
  - Liaise with other Incident Response Team members to determine items to be immediately replaced and what is recoverable.
- Assess damage and undertaken salvage operations – **Chief Executive Officer, Manager Works and ~~Services~~Infrastructure, Property Services and Natural Resource Manager**
  - Undertake initial assessment of salvageable materials, items and records, etc.
  - Contact staff to remove items to the salvage site (RSL or Town Hall)
- Co-ordinate all communications, media and elected members, Local Government insurers and general co-ordination of recovery process **– Chief Executive Officer**
  - Liaise with Shire President to issue a media statement
  - Co-ordinate meetings of Incident Response team
  - Authorise all immediate purchasing requirements
  - Liaise with Shire's insurers

Recovery Time Objective

It is the aim of the Recovery Plan to achieve this task within 72 hours.

Resource Requirements

- Office furniture and stationery
- Administration and Works staff
- IT hardware and software
- Communications (land line and internet)

TASK 3 – Assess damage and prepare medium term Recovery Plans

This task provides the necessary steps to commence planning for medium term operations from the Disaster Recovery Site.

Incident Response Team

Team Leader:	Chief Executive Officer
Team Members:	Manager Works and ~~Services~~Infrastructure
	Property Services and Natural Resource Manager
	~~Risk Management Co-ordinator~~Governance and Rates Officer

Recovery Procedure

Undertake the following steps:

- Establish the disaster recovery site for full operations in the medium to longer term – **~~Manager Regulatory Services~~Chief Executive Officer**
  - Recover data to pre disaster state
  - Bring all records up to date
  - Contact all necessary persons to inform of incident, expected delays and seek documentation where necessary
  - Establish necessary equipment and infrastructure requirements to provide full operations from recovery site including demountable buildings and other office accommodation
- Finalise damage assessment and commence planning for re-establishing services through full or partial rebuild – **Chief Executive Officer, Manager Works and ~~Service~~Infrastructure, Property Services and Natural Resource Manager**
  - Undertake assessment of building and determine action to fully or partially rebuild and make recommendation to Council
- Co-ordinate all communications, media and elected members, Local Government insurers and general co-ordination of recovery process – **Chief Executive Officer**
  - Oversee assessment and recovery
  - Co-ordinate meetings of Incident Response Team
  - Oversee planning for medium term operation from Disaster Recovery Site (6-12 months)

Recovery Time Objective

4 weeks

Resource Requirements

- IT contractors
- Additional infrastructure as identified
- Contractors to clean up disaster site

TASK 4 – Long term Recovery Plan and relocation to permanent office building

This task provides the necessary steps to finalise planning, rebuilding and recommencement of operation from the permanent office building.

Incident Response Team

Team Leader:	Chief Executive Officer
Team Members:	Manager Works and ~~Services~~Infrastructure Property Services and Natural Resource Manager Shire President

Recovery Procedure

Undertake the following steps: **Chief Executive Officer**

- Establish working party to:
  - Review operations for location of new premises
  - Undertake design and tendering processes
  - Oversee construction of new premises
  - Oversee commissioning of new premises
- Present review findings to Council for decision
- Appoint architect, exterior and interior designers, engineers and other necessary assistance to design, specify and document new premises
- Issue tenders, appoint contractor and commence construction
- Commission new premises and commence operations from new building

Recovery Time Objective

From the commencement of this task, after 4 weeks from the incident, it is the target to have all Kodja Place precinct functions permanently operational from the rebuilt Kodja Place in 12 months.

Resource Requirements

- Planning assistance
- Consultants/architects
- Contractors

Immediate Response Checklist

INCIDENT RESPONSE	√	ACTIONS TAKEN
Have you: • assessed the severity of the incident?	❑	
• evacuated the site if necessary?	❑	
• accounted for everyone?	❑	
• identified any injuries to persons?	❑	
• contacted Emergency Services?	❑	
• implemented your Incident Response Plan?	❑	
• started an Event Log?	❑	
• activated staff members and resources?	❑	
• appointed a spokesperson?	❑	
• gained more information as a priority?	❑	
• briefed team members on incident?	❑	
• allocated specific roles and responsibilities?	❑	
• identified any damage?	❑	
• identified critical activities that have been disrupted?	❑	
• kept staff informed?	❑	
• contacted key stakeholders?	❑	
• understood and complied with any regulatory/ compliance requirements?	❑	
• initiated media/public relations response?	❑	

4. Event Log

The Event Log is to be used to record information, decision and actions in the period immediately following the critical event or incident.

Date	Time	Information/Decisions/Actions	Initials

5. Register of Initials

Name:	Initial:	Signed:

6. Incident Recovery Checklist

INCIDENT RESPONSE	√	ACTIONS
Now that the crisis is over, have you: • refocused efforts towards recovery?	❑	
• deactivated staff members and resources as necessary?	❑	
• continued to gather information about the situation as it affects you?	❑	
• assessed your current financial position?	❑	
• reviewed cash requirements to restore operations?	❑	
• contacted your insurance broker/company?	❑	
• developed financial goals and timeframes for recovery?	❑	
• kept staff informed?	❑	
• kept key stakeholders informed?	❑	
• identified information requirements and sourced the information?	❑	
• set priorities and recovery options?	❑	
• updated the Recovery Plan?	❑	
• captured lessons learnt from your individual, team and business recovery?	❑	

7. Evacuation Procedures

Relevant procedures and plans have been developed and are displayed in accordance with Council's ~~OSH~~ WHS policy and procedures in positions easily accessible to staff and customers.

8. Emergency kit

In the event of evacuation or damage to the Administration building, Works Depot, Springhaven Lodge or The Kodja Place and relocation of the unit to a Disaster Recovery Site two emergency kits have been made up.

The kits are located at:

- ➢ The Administration Building, in the server room; and
- ➢ The Kodja Place, behind the main desk.

The Risk Management Coordinator is responsible for annually checking and updating the kits.

The items and documents included in the emergency kit are:

- Business Continuity Plan and Disaster Recovery Plan incorporating contact lists
- List of staff names and contact numbers
- Councillor contact details
- Copy of Shires templates and forms (on a USB)
- Basic stationery
- One ream of Council Letterhead
- Box of envelopes

9. Pandemic Response Plan

See Pandemic Response Plan – Appendix 1

10. Review and Maintain

It is critical that this plan is regularly reviewed to ensure that it remains relevant, accurate and useful. The Risk Management Co-ordinator is responsible for reviewing and maintaining the plan including annual updating of all the contact and insurance lists. This maintenance is a key factor in the successful implementation of the plan during an emergency.

The plan should use staff titles rather than names and any organisational structure changes must be reviewed with the plan.

After an event it is important to assess the performance of the plan, highlighting what was handled well and what could be improved upon next time.

Each workplace fire warden will develop an evacuation process which will be laminated and displayed clearly for staff and visitors to access.

LGIS Insurance Policies

Insurance type	Policy coverage	Policy exclusions	Insurance company and contact	Last review date	Payments due
Business Interruption	*Business interruption due to:* - *Fire* - *Flood* - *Theft*	- *Terrorism* - *Tsunami* - *Landslide*	*LGIS – David Wood (9483 8888)* *Policy No V01.2014*	*30 June Annually*	*Annually*
Motor Vehicle	*All motor vehicles and trailers*	**Section 1 Loss or damage to vehicles as per Interest Insured.** Current market value at the time of loss or damage or sum insured value specified in the Declaration of vehicles, whichever is the lesser, but limited per council to $20,000,000 any one event. **Section 2 Cover for Third Party Liability** $35,000,000 but limited to $5,000,000 for any dangerous goods carrying vehicles, for all claims arising from the one accident or series of accidents resulting from the one original cause (as defined in this section of the policy).	*LGIS – David Wood (9483 8888)* *Zurich 002152*	*30 June Annually*	*Annually*
Personal Accident	*The Mayor, Chairperson, Elected Members, Councillors, Commissioners, Employees of the Insured, Accompanying Partners/Spouses of the Covered Persons above,* *Voluntary Workers, Members of any Committees and Trusts.* *Other Persons where the Insured is required to provide coverage whilst such persons are engaged in any Government Labour Market, Training or Job Creation Projects.*	*Covering Insured Persons whilst engaged in a Journey and any* *other activity directly or indirectly connected with or on behalf of the Authority and Insured Persons whilst engaged in any activity directly or indirectly connected with or on behalf of the Authority.*	*LGIS – David Wood (9483 8888)* *Policy No 93130605*	*30 June Annually*	*Annually*

Insurance type	Policy coverage	Policy exclusions	Insurance company and contact	Last review date	Payments due
Public liability	*100% protection*	*None*	*LGIS – David Wood (9483 8888)* *Policy No 000114*	*30 June Annually*	*Annually*
Workers Compensation	*100% protection* *Lump Sum $300,000* *Weekly $2,500*	*None*	*LGIS – David Wood (9483 8888)* *Policy No 000121*	*30 June Annually*	*Annually*
Buildings – Shire office	*$4,079,250 - industrial special risks, machinery breakdown, electronic equipment, general property, includes physical loss, destruction or damage to property*	*None – excess only*	*LGIS – David Wood (9483 8888)* *Policy No 114*	*30 June Annually*	*Annually*
Contents – Shire office	*$500,000*	*None – excess only*	*LGIS – David Wood (9483 8888)* *Policy No 114*	*30 June Annually*	*Annually*
Building – Springhaven Lodge	*$5,953,500 – industrial special risks, machinery breakdown, electronic equipment, general property, includes physical loss, destruction or damage to property*	*None – excess only*	*LGIS – David Wood (9483 8888)* *Policy No 114*	*30 June Annually*	*Annually*
~~*Contents – Springhaven Lodge*~~	~~*$420,000*~~	~~*None – excess only*~~	~~*LGIS – David Wood (9483 8888)*~~ ~~*Policy No 114*~~	~~*30 June Annually*~~	~~*Annually*~~
Fidelity Guarantee	*Loss as a result of an act or acts of employee dishonesty ($400K)*	*$50,000 excess*	*LGIS – David Wood (9483 8888)* *Policy No 05CH005846*	*30 June Annually*	*Annually*
Building – Kodja Place	*$4,704,100 - industrial special risks, machinery breakdown, electronic equipment, general property, includes physical loss, destruction or damage to property*	*None – excess only*	*LGIS – David Wood (9483 8888)* *Policy No 114*	*30 June Annually*	*Annually*
Contents – Kodja Place	*$250,000*	*None – excess only*	*LGIS – David Wood (9483 8888)* *Policy No 114*	*30 June Annually*	*Annually*
Management Liability Councillors and Officers	*$4,000,000*		*LGIS – David Wood (9483 8888)* *Chubb 001877*	*30 June Annually*	*Annually*

Insurance type	**Policy coverage**	**Policy exclusions**	**Insurance company and contact**	**Last review date**	**Payments due**
Bush Fire *Volunteer Bush Fire Brigade Members*	*$20,000,000 for all claims arising from one event* *$750,000 Annual aggregate stop loss limit*	*None*	*LGIS – David Wood (9483 8888)* *LGIS 000114*	*30 June Annually*	*Annually*
~~*Medical Malpractice*~~	~~*$20,000,000*~~	~~*$1,000 excess*~~	~~*Vero Insurance*~~ ~~*LPP 104157341*~~	~~*30 June Annually*~~	~~*Annually*~~
Commercial Crime and Cyber Liability	*$500,000* *Internal Crime* *External Crime* *Theft* *Physical Loss or Damage*	*$1,000 excess*	*David Wood (9483 8888)* *LGIS 001877* *Chubb Australia*	*30 June Annually*	*Annually*

11. Data Security and Backup Strategy

The Shire of Kojonup **protects our data and our network** (e.g.; virus protection, secure networks and firewalls, secure passwords and data backup procedures). For security reasons, specific details of these processes are not included in this publicly available plan, but are available from the Chief Executive Officer when required.

12. Business Impact Analysis

*As part of the **Business Continuity Plan** the Shire has undertaken a **Business Impact Analysis** which will use the information in the Risk Management Plan to assess the identified risks and impacts in relation to critical activities of the Shire operations and determine basic recovery requirements.*

Critical Business Activity

The following table lists the critical business activities that must be performed to ensure the Shire's business continues to operate effectively.

General Risk Area 1

Finance and Accounting
Payroll
Environmental Health

General Risk Area 2

Road construction and maintenance
Public Conveniences
Waste Management

Business Impact Analysis

Critical Business Activity	**Description**	**Priority**	**Impact of loss** *(losses in terms of financial, staffing, reputation etc.)*	**RTO** *(critical period before business losses occur)*
General Risk Area 1	All critical activities to manage Council's key administrative and governance processes: • Finance and Accounting • Payroll • Environmental Health	High	• Staffing numbers will not change; however, there will be an impact on productivity levels as functions are completed manually or resources are redirected to the recovery process • Continuing payment of permanent and part time Springhaven staff whilst residents accommodated elsewhere and until new building completed – cost of wages v no income from facility • The urgent re-establishment of these critical needs may result in Council breaching various statutory and service requirements • There will be a minor impact on customer services which may temporarily reflect upon Council poorly • The re-establishment of the service will depend on many alternate suppliers, such as IT and Communication suppliers, electricity and software providers	72 hours

Critical Business Activity	**Description**	**Priority**	**Impact of loss** *(losses in terms of financial, staffing, reputation etc.)*	**RTO** *(critical period before business losses occur)*
General Risk Area 2	All critical activities to manage Council's on ground, engineering and maintenance services: • Road construction and maintenance • Public conveniences	High	• Re-establishment/incremental costs: ○ Machinery at hire rates ○ Public conveniences – no impact • Staffing numbers will not change; however, there will be an impact on productivity levels as functions are completed manually or resources are redirected to the recovery process • There will be minor impact on customer services which may temporarily reflect upon Council poorly • The urgent re-establishment of these critical needs may result in Council temporarily breaching various statutory and service requirements	72 hours

13. Action Plan for Implementation

Action	Responsible Officer	Timeframe
Commence planning and undertake test of documented incident plans	SMT & Risk management Co-ordinator	
Review document as a result of test and in preparation for Council	SMT & Risk management Co-ordinator	Reviewed annually: May 2019 April 2020 September 2021 May 2023
Prepare Emergency Kit as identified in this Plan	Risk management Co-ordinator	Prepared and reviewed annually
Educate and train all staff on the plan	Risk management Co-ordinator	Distribute after each review
Investigate contractual requirements for radio failure and alternative contingency plans for methods of communications for works staff	Manager Works ~~& Services~~and Infrastructure Chief Executive Officer	

14. Glossary

Business Continuity Planning	A process that helps develop a plan document for a business to ensure that it can operate to the extent required in the event of a crisis/disaster.
Business Continuity Plan	A document containing all of the information required to ensure that the business is able to resume critical business activities should a crisis/disaster occur.
Business Impact Analysis	The process of gathering information to determine basic recovery requirements for our key business activities in the event of a crisis/disaster.
Key business activities	Those activities essential to deliver outputs and achievement of business objectives.
Recovery Time Objective (RTO)	The time from which you declare a crisis/disaster to the time that the critical business functions must be fully operational in order to avoid serious financial loss.
Resources	The means that support delivery of an identifiable output and/or result. Resources may be money, physical assets, or most importantly, people.
Risk Management	Is the process of defining and analysing risks, and then deciding on the appropriate course of action in order to minimise these risks, whilst still achieving business goals.

15. Appendix

Pandemic Response Plan

11 April 2025

Shire of Kojonup
93-95 Albany Highway
Kojonup
WA 6395

Attention : The Chief Executive Officer E: ceo@kojonup.wa.gov.au

Dear Sir,

I note the following:

Background

- Fresh Fields Management (NSW) No 2 Pty Ltd (**FFM**) operates the Springhaven aged care business (**AC Business**).
- FFM operates the AC Business from a leasehold property leased by FFM from the Shire of Kojonup (**Lessor**) under a lease dated 14 October 2024 (**Lease**).
- FFM also leases various residential properties from the Lessor (being the **Residential Leases** in this email) dated on or about the same date.

Proposed Transaction

- FFM proposes transferring the AC Business and assigning the Lease and the Residential Leases to Fresh Fields Aged Care Pty Ltd (**FFAC**) as part of its current group restructure.
- The proposed transfer date is no later than 30 June 2025.
- FFAC is a well-established wholly owned approved provider entity within the Hall & Prior Group holding a number of assets in its own name.
- The restructure is driven largely by a desire on the part of the Group directors to simplify and streamline the Group structure.
- The restructure will not result in a change in control of either FFM or FFAC within the Hall & Prior Group.

RAC Lease Assignment Position

- Under the Lease, the consent of the Lessor is not required to transfer the Lease to a **Related Person,** subject to the lessee not being in default and the assignee signing a Landgate transfer form to give effect to the assignment. The Lessor needs also to be given reasonable prior notice of the assignment. In addition, FFM can obtain an absolute release under the Lease on the assignment occurring, provided that FFM can demonstrate to the reasonable satisfaction of the Lessor that the assignee has the ability to meet the financial obligations under the Lease and to carry on the Permitted Use from the premises , and the requirements of clause 12.5(d) of the Lease are complied with by the assignee.
- FFAC is a Related Person of FFM, as defined in the Lease, and meets the above tests. In that regard I attach the audited financial statements for FFAC for FY23/24.
- Attached is also a simplified Hall & Prior corporate structure diagram, which shows the relationship of FFM and FFAC to each other within the Group
- Clause 12.1 of the Lease does not apply as the proposed assignment will occur under clause 12.5 of the Lease.

Residential Leases Assignment Position

- Under the Residential Leases, FFM can assign the Residential Leases without the Lessor's consent if (amongst other things) the leases in question are being assigned to what is defined as a **Springhaven Assignee.**
- A Springhaven Assignee is a person that the Lessor "has approved as an assignee under the Springhaven Lease".
- On the assumption that Lessor accepts FFAC as a suitable assignee of the Lease as outlined above, with the result that FFM is released under the Lease, FFM proposes assigning the Residential Leases to FFAC in addition.

The purpose of this email is as follows :

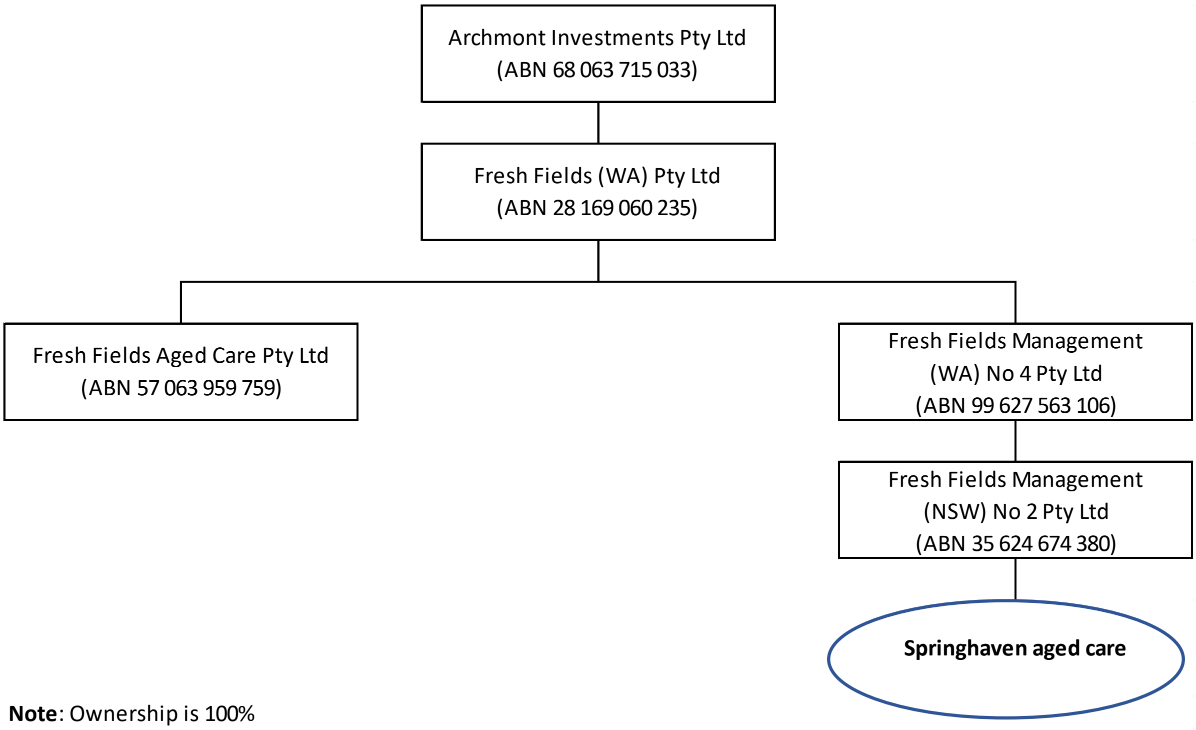
- To provide formal notice to the Lessor of the proposed assignment of the Lease as identified in this email.
- To seek the Lessor's absolute release of FFM under the terms of the Lease effective from the date of the assignment (to be advised but no later than 30 June 2025), noting the requirements of the Lease as summarised above and as may otherwise be applicable.
- To advise the Lessor of FFM's intention to assign the Residential Leases to FFAC at the same time as the assignment of the Lease.

To the extent that the Lessor needs additional information to consider the above, please advise me as soon as possible, and I'll endeavour to provide that information to you quickly.

Yours sincerely

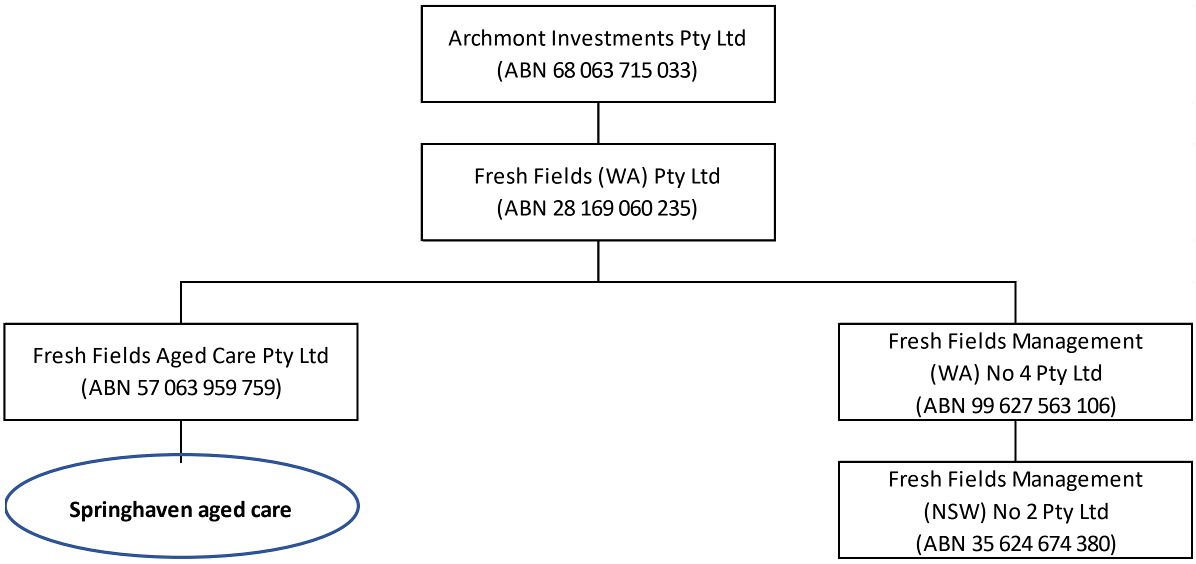
Alan Churley
Special Counsel

Simplified Corporate Structure immediately BEFORE the Proposed Lease Assignment



Note: Ownership is 100%

Simplified Corporate Structure immediately AFTER the Proposed Lease Assignment



Note: Ownership is 100%

Cyber Hygiene Improvement Programs (CHIPs)

Addressing Cyber Hygiene in Australia

asd.chips@defence.gov.au

Quarterly Report - February 2025

Shire of Kojonup (WA)

FOI STATEMENT: This document, including any summary or extract of information from it, is exempt from disclosure under FOI (section 7 of the Freedom of Information Act 1982). The Australian Signals Directorate must be consulted prior to responding to any FOI request relating to this document or its information.

Table of contents

1. Executive Summary

Introduction

This report is optimised for readers already familiar with CHIPs. For information about CHIPs, hygiene indicators and advice refer to the Background section.

This report provides the quarterly update of your organisation's performance against the hygiene indicators as assessed by the Australian Signals Directorate (ASD) in the first week of February 2025.

Hygiene indicators are ordered from most to least important. For further information, refer to the Background section.

Key insights

Critical Vulnerabilities

Open at last scan: 0
Resolved/Mitigated: 0
New – Existing Host: 0
New – New Attribution: 9
Current: 9

✗

Service Visibility

Open at last scan: 0
Resolved/Mitigated: 0
New – Existing Host: 0
New – New Attribution: 0
Current: 0

✓

Admin Consoles

Open at last scan: 1
Resolved/Mitigated: 1
New – Existing Host: 0
New – New Attribution: 0
Current: 0

✓

MFA

Open at last scan: 1
Resolved/Mitigated: 1
New – Existing Host: 0
New – New Attribution: 0
Current: 0

✓

Dormant Websites

Open at last scan: 2
Resolved/Mitigated: 2
New – Existing Host: 0
New – New Attribution: 0
Current: 0

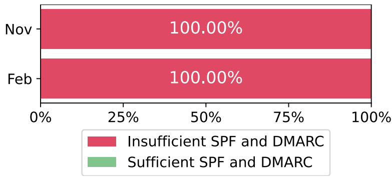
✓

DNS Hygiene

Open at last scan: 0
Resolved/Mitigated: 0
New – Existing Host: 0
New – New Attribution: 0
Current: 0

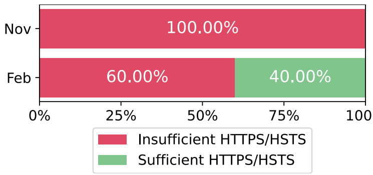
✓

Email Security



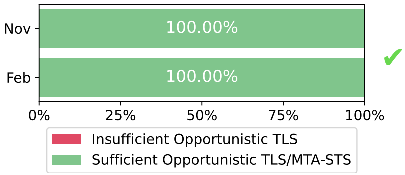
●

Website Encryption



+

Email Encryption



✓

2. What's New

Welcome to the February 2025 CHIPs report.

Major changes this quarter

- Many small improvements to Critical Vulnerabilities, Admin Consoles and other scanners.
- Adjustments to all CSV files and our new CSV changelog.
- Simplification of Web Encryption scoring.
- Breach Log Testing (BLT with CHIPs) pilot kicks off.

Scanner updates

Critical Vulnerabilities

Improved the scanner's performance and added the following detections:

- Exim SMTP (CVE-2023-42114, CVE-2023-42115, CVE-2023-42116, CVE-2023-42117, CVE-2023-42118).
- Crush FTP (CVE-2024-4040).
- Wordpress plugin - Hash Form (CVE-2024-5084).
- Wordpress plugin - LiteSpeed Cache (CVE-2024-44000, CVE-2024-28000).
- Issue fixed in Wordpress Plugin - Elementor (CVE-2023-48777).

Admin Consoles

Added many additional administrative/management interfaces. Changes:

- Added new detections for admin interfaces on: cPanel, Django, FortiManager, GoAnywhere, Jenkins, OpenVPN, and Palo Alto products.
- Added for the FGFM (FortiGate/FortiManager) protocol.
- Improvements to FortiGate and FortiMail detections.
- Fixed false positives in UniFi detections.

Multi-Factor Authentication

Updates to many detection plugins. Additional detections are now in place for:

- Citrix products.
- Cisco ASA products.
- Palo Alto GlobalProtect products.
- Microsoft 365 solutions and products.

Service Visibility

Minor changes to improve visibility and reduce false positives:

- Better handling of non-default port/protocol setups.
- Improved logic to detect and exclude ports from CDN infrastructure.

DNS Hygiene

- Significant expansion of the number and types of dangling hostnames detected. These are critical issues when reported.
- Now excludes results with no DNS records, and ensures the 'Issues' column (in the CSV) is ordered consistently for easier filtering.

We acknowledge expanding our detections is both positive and negative for customers - it's better to know, but new issues are often extra work.

A reminder that the churn table, beneath the graphic for each of the hygiene metrics, provides quick insight into how many new issues are on hosts that CHIPs already reports to you about, versus how many issues are on hosts newly discovered this quarter.

Adjustments to all CSV files and our new CSV changelog

From this quarter onwards, CHIPs will provide a changelog with the CSV data files that will explain any changes to CSV formats.

The CHIPs team is thrilled to learn of the number of customers that find the data worth ingesting into other reporting systems. We acknowledge the feedback that not announcing and describing changes to CSV data formats can create confusion.

Changes this quarter to CSV files include:

- All CSV files have had the first column, 'Group' removed.
- Updates to the Domain Visibility page and CSV to help distinguish active from inactive domains and which are apex domains.
- For Web Encryption, we have simplified the CSV scoring information. Scoring and reasons will now be presented in two columns, instead of six.
- For API Detection, we have added a new column to the CSV for status code.

More details are available in csv_changelog.txt in your report pack.

Simplification of Web Encryption scoring

The detailed output from Web Encryption has been simplified in the CSV file to make it consistent with other phases. Thank you to customers that brought this to our attention.

Breach Log Testing (BLT with CHIPs) pilot kicks off

During January, CHIPs began its pilot of Breach Log Testing (BLT with CHIPs) with a small set of customers.

The pilot has gone well. Results have been encouraging with most participants providing positive feedback. We also appreciate the feedback we received on some things to improve.

In particular, we liked: *"Our team thought it was an interesting, engaging, and fun exercise and was helpful to test and reinforce analyst/IR skills in a simulated real-world example. The exercise was a useful opportunity to ensure our logging controls are in place and are working as expected. Also, as it was a simulated exercise with real traffic, it offered a good example to show newer team members how internet traffic flows into our systems and how the logs are ingested from those systems. The team also enjoyed the opportunity to refresh skills with* ***spoilers****. The* ***spoilers*** *were a nice touch and gave the team an opportunity to use other tools to do the* ***spoilers****."*

As previously advised, BLT is an exercise designed to help organisations check that their Security Operations Centres (SOCs) have access to the necessary log files and other information that might assist them in detecting and responding to potential compromises.

The pilot was just one of the exercises we have planned under BLT, with more to come.

At this stage we are anticipating opening the program up to all customers that wish to participate in March. Keep an eye out for the email.

Reminders

Feedback

We love hearing your ideas and feedback (good and bad). You can reach us at: asd.chips@defence.gov.au and a real person will answer your email.

Clinics

A reminder to all customers about our quarterly clinics. The clinics are designed for both new and existing CHIPs customers and is an opportunity for you to ask any questions about this report and the CHIPs program more generally. The clinics are typically run two weeks after the reports are released. Keep an eye on your email for your invitation to our next round of clinics.

ASD Partnership Program

If your organisation is interested in becoming an ASD partner, please check out our Partnership Program.

In other news

Large Language Models (LLMs) such as ChatGPT, Gemini, Claude, and more recently DeepSeek, and some other amazing AI based technologies, are certainly throwing up some interesting challenges and opportunities in technology and more specifically cyber security. It's too early to tell what the big changes will be, but here's some interesting stuff we have already seen.

There is already widespread reporting on how LLMs have enabled less capable actors to drastically improve their catch rate by editing/refining the language they use in their phishing lures. Now, more than ever, "blaming the victim" for being taken in by phishing emails is unfair, counter-productive and arguably an abrogation of responsibility for implementing controls. Instead, the technical controls we have been speaking about (forever), like email filtering and application control are still critically important. Likewise, decent, ideally phishing-resistant, MFA, should also be implemented. Particular scams, like business email compromise where invoices have bank account numbers altered, should be addressed through specific training for finance staff.

Even more alarmingly - yet impressively - deepfake technology can now generate real-time avatars of real people, perfectly mimicking a fraudster's facial expressions, lip movements, and voice to deceive others in interactive video conferences. This technology was at the edge of what was possible back in 2020, but is now entirely run of the mill with open source demonstrator projects and point and click installable software. Perhaps more bewilderingly is how this tech is being used by some serious actors. There is open source reporting about it being used for employment fraud by North Korean actors. When you can find point and click software like this we are in for an interesting ride.

We also thought this recent blog post by the Google Threat Intelligence Centre examined a lot of misuse of AI by malicious cyber actors, and is certainly worth a look. Much of the activity is, in many respects, standard application development style tasks, even if targeted at malware. Interestingly, near the end we note it says that Russian Information Operators have used the Google LLM to "Explain subscription plans and API details for online services". We also hate reading that information too - so if LLMs can help decode the bewildering variety of plans and features that can't be all bad.

Finally and perhaps most importantly though is to understand that staff in your organisation are almost certainly experimenting with and using AI - even if they don't realise it. And there might be good reason to encourage them, provided they understand how to use it safely. For example, we have some incredibly talented people working at CHIPs, and while they can write advanced SQL queries, LLMs can often help refine them to be even more efficient and reliable. Likewise, summarising documents, generating responses, and proofreading are tasks that LLMs can be very effective at with one big caveat - provided you know where the data you put into the LLM ends up.

Recently DeepSeek attracted plenty of attention for good and bad reasons. The efficiency of the training model was seen as a big plus including some innovative self-improvement techniques that many other LLMs have already adopted. On the bad, people noted that information that you entered into DeepSeek is now out of your control. But of course, that problem is far from unique to DeepSeek (even if it seemed like a bigger problem given the geopolitics).

For CHIPs, the approach we are taking is running our own versions of open source models internally on hardware we control, or alternatively ensuring any sensitive or proprietary information is stripped before loading it into online models.

3. Coming Up

Scanner improvements

The work of improving each of the individual scanners is ongoing. In addition to a backlog of detections that we work through every quarter, the CHIPs team will also adjust scanners based on new vulnerabilities and other issues that come to light before the next scan.

Breach Log Testing (BLT)

The "What's new" section of this report discusses the outcomes of the BLT pilot.

At this stage we are anticipating opening the program up to all customers that wish to participate in March. Keep an eye out for the email.

Additional CSV files

Based on customer requests we are working on adding two new CSV files. These CSV files won't contain any new scan data. Rather they will help in summarising and comparing your CHIPs information.

The first new CSV file will provide the scores across all assessed metrics for each host/IP in your environment.

The second new CSV will provide the summary scores for your organisation for each metric, for each quarterly scan, with as much of your history as we have in our database.

We expect to provide these to you in the May report.

If you have other suggestions on how we could conveniently group data for you, using standard outputs like CSV, please let us know.

Product Vsibility

Understanding what systems and software you have facing the internet is critically important to securing your organisation.

Product Visibility will help organisations understand more about their internet-facing edge, and the systems and software that can be found there. This will be an "information only" capability.

We hope to ship a Minimum Viable Product with the May report and will work to refine it over time.

Reports data comparison

We are working on how we can improve aspects of the CHIPs report that compare your organisation's performance to peers. Stay tuned.

Further Out

Operation Technology Scanning

CHIPs is researching how we can better detect operational technology (OT) exposed to the internet. Some OT is already reported in Service Visibility, but we wish to increase our coverage.

OT presents some unique challenges to the existing CHIPs processing models. We will work through these to provide organisations with as much useful information as possible.

CHIPs Dashboard

CHIPs acknowledges the requests it has received for more graphical/visual ways of showing CHIPs data.

We are investigating the possibility of building dashboard tooling that customers can run in their own environment using PowerBI.

A note on the deadline for attribution changes

A reminder that the cut-off for scanning and attribution updates is ten business days prior to scanning on or about the 20th of January, April, July and October. Any attribution changes requested by customers after this date will be updated in the next report run.

Reach out

This report is designed to serve you and the CHIPs team is here to help. Your engagement, questions, feedback, and advice assists us in this task.

You can reach us by phone on +61 2 6243 0435 (business hours, Canberra time) or by email at asd.chips@defence.gov.au.

4. Using This Report

This report provides a summary of your organisation's internet-facing cyber security posture against cyber hygiene indicators tracked by CHIPs. ASD provides this report to assist staff monitoring and managing the performance of the organisation against these cyber hygiene indicators.

The metrics in the report appear in order of importance:

1. Critical Vulnerabilities (most important)
2. Service Visibility
3. Administration Consoles
4. Multi-Factor Authentication
5. Dormant Websites
6. Email Security
7. Website and Email Encryption
8. API Detection
9. Route Security
10. DNS Hygiene
11. HOT CHIPs
12. Breach Data
13. Domain Visibility

CHIPs recommends following this priority order when addressing issues. All metrics in the report are important, but other cyber security concerns may take priority in your organisation.

Interpreting and actioning the data presented in your organisation's CHIPs report will likely not be a seamless process. It may take cooperation between stakeholders and more than one attempt to remediate issues.

The following is a high-level process CHIPs suggests for remediation:

1. Identify the highest priority services and assessments.
    - While this report suggests an order of importance, each organisation will have different priorities and resources.
2. Find the owners of systems and owners of the risks.
    - System owners and risk owners are not always the same.

3. Brief owners, risk owners, and related stakeholders on issues.
    - Communicate CHIPs findings to them, and the implications - the background appendix section of this report explains what each metric measures, and why it matters.
    - Technical stakeholders should not be left out of this process.
4. Work with technical staff to build a remediation plan.
    - These plans do not always work on first attempt. Prepare management for the possibility that remediation may take repeated attempts.
5. Implement plan.
6. Measure whether change was effective.
    - If it was not, try another approach.

The attached CSV files contain a detailed breakdown for the domains that ASD understands are part of your organisation.

ASD will provide an updated report, and accompanying data files every quarter (February, May, August, November) for your visibility. ASD encourages your organisation to make improvements against CHIPs in line with your organisation's risk management and continuous improvement policies.

For more information see Aims under Appendix - Background.

Distributing reports

Cyber security teams should distribute this information to their technical staff for remediation as soon as practicable. Sharing the report and data files will assist technical staff in prioritising remediation actions.

Handling information

All intellectual property rights associated with this report, or the activity that creates it, is owned by the Australian Government.

This CHIPs report has been given a traffic light protocol (TLP) rating of TLP:AMBER, meaning it is restricted to internal access and use only (see appendix for more details on TLP ratings).

CHIPs reports can be disclosed to your employees, contractors and/or agents on a need-to-know basis for the protection of your ICT systems.

The above does not prevent disclosure of this document or its information:

a. To another Australian Government entity (federal, state, territory or local), where this serves government's legitimate interests;

b. In response to any request by a minister, or a house or committee of the parliament of the jurisdiction in question; or

c. When required by federal, state or territory law.

This document, including any summary or extract of information from it, is exempt from disclosure under FOI (section 7 of the Freedom of Information Act 1982). The Australian Signals Directorate must be consulted prior to responding to any FOI request relating to this document or its information.

5. Critical Vulnerabilities

Critical Vulnerabilities helps organisations identify systems that are trivially vulnerable to attack from the internet and should be investigated and remediated as number ONE priority issues. Refer to Background for more information.

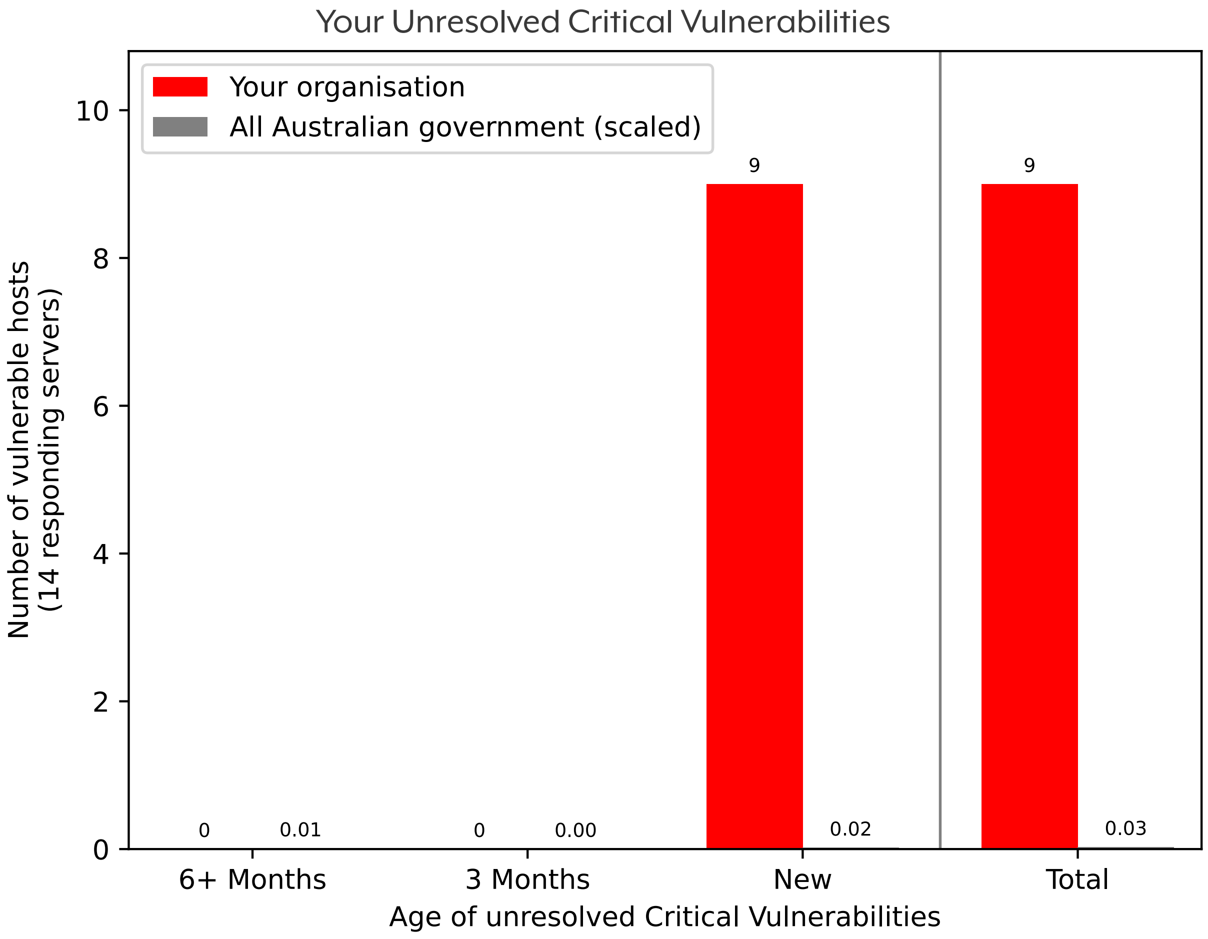


Figure 5.1 Open issues by age

Issues Nov-24: 0	New (existing hosts): 0	New: +9	Issues Feb-25: 9
	Resolved/Mitigated: 0	Removed: 0	

Figure 5.2 Change in open issues since last quarter

6. Service Visibility

Service Visibility allows organisations to track attack surface by identifying hosts with services open to the internet.

Refer to Background for more information.

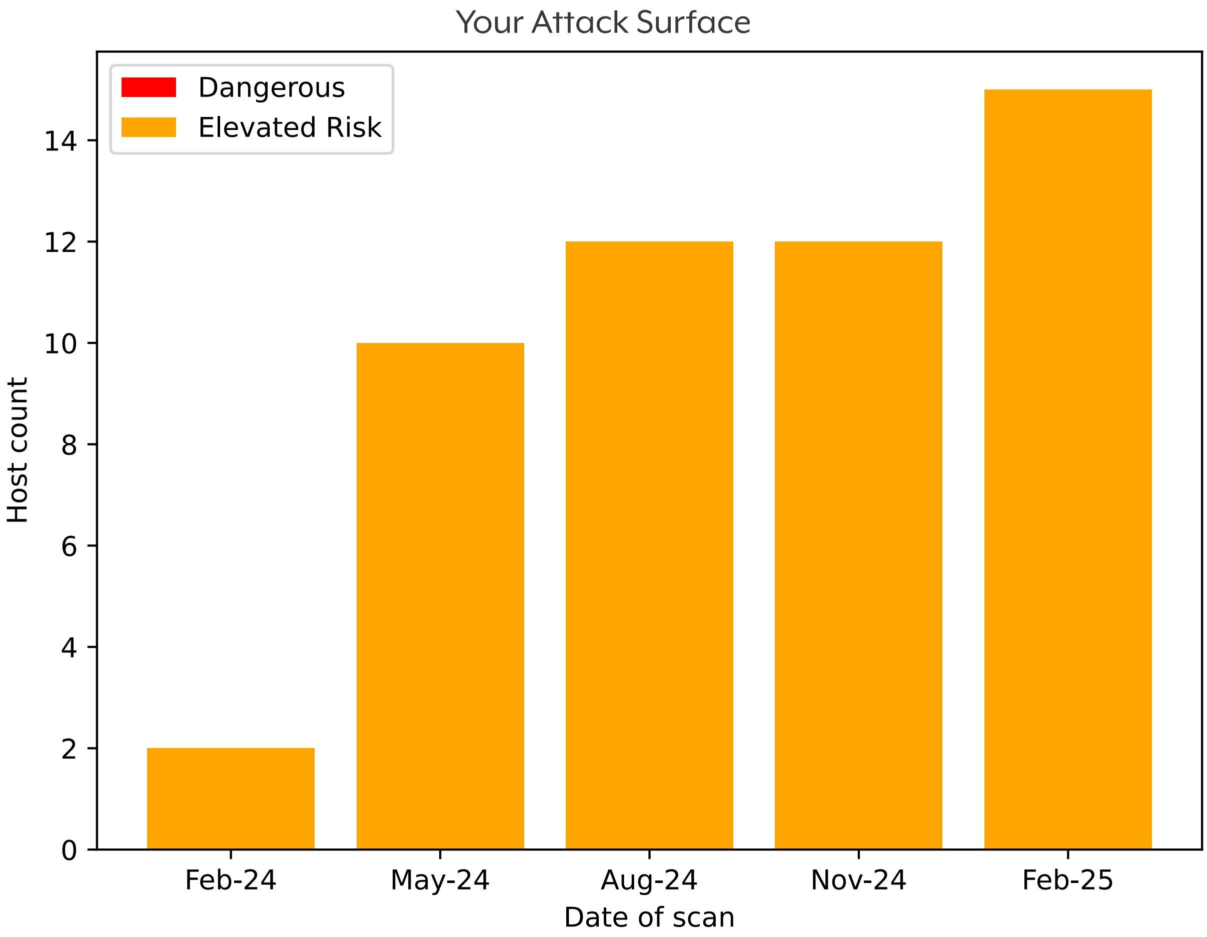


Figure 6.1 Hosts with service visibility issues over recent quarters

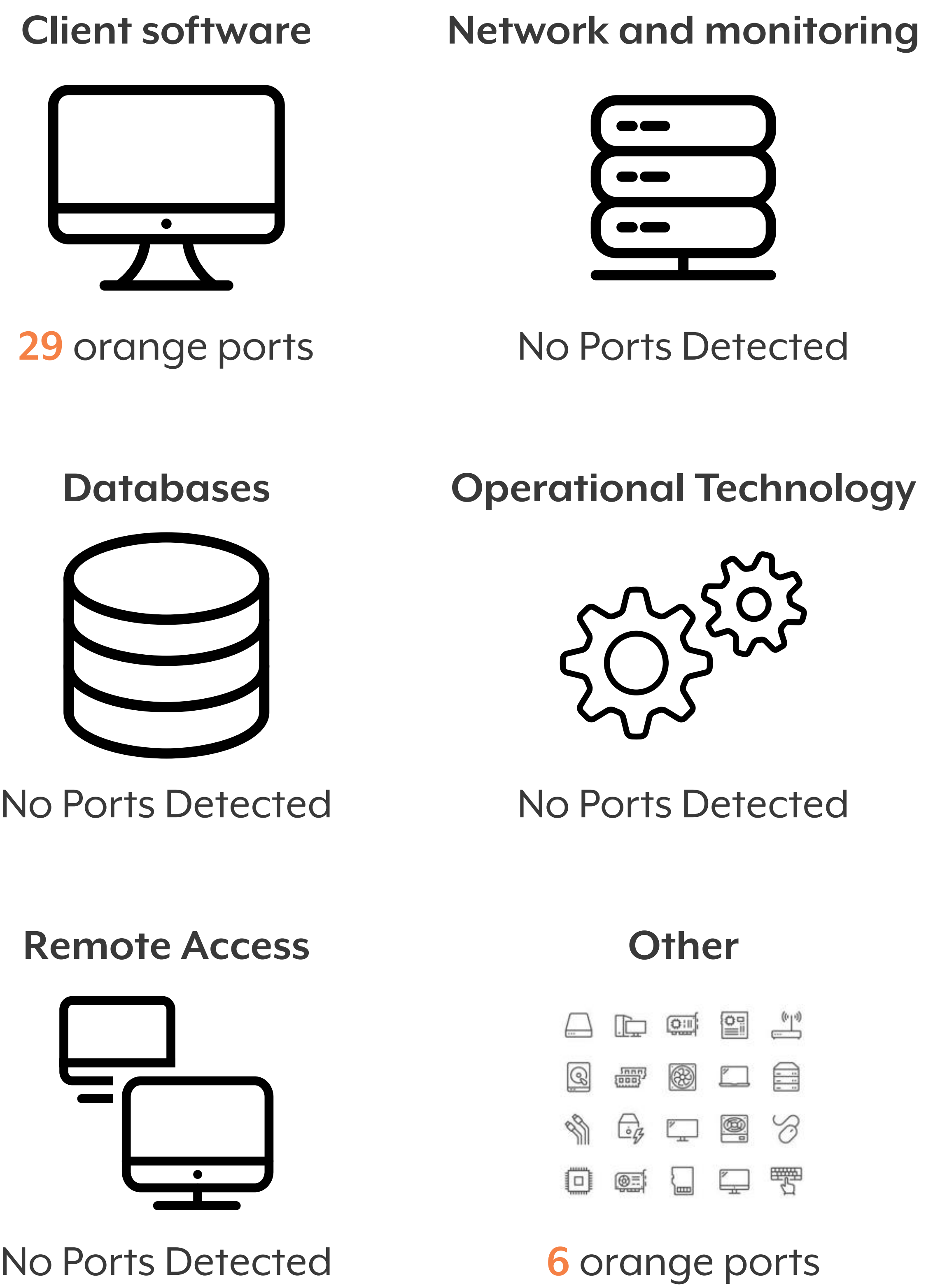
Issues Nov-24: 0	New (existing hosts): 0	New: 0	Issues Feb-25: 0
	Resolved/Mitigated: 0	Removed: 0	

Figure 6.2 Change in hosts with red ports since last quarter

Issues Nov-24: 12	New (existing hosts): 0	New: +3	Issues Feb-25: 15
	Resolved/Mitigated: 0	Removed: 0	

Figure 6.3 Change in hosts with orange ports since last quarter

Visible Network Ports by Category



Client software

29 orange ports

Network and monitoring

No Ports Detected

Databases

No Ports Detected

Operational Technology

No Ports Detected

Remote Access

No Ports Detected

Other

6 orange ports

Figure 6.4 Open ports by category

7. Administration Consoles

Administration consoles (super-user interfaces to systems) allow privileged users to adjust the configuration and operation of systems. Leaving administration consoles of systems exposed to the internet increases the risk of systems being compromised.

Refer to Background for more information.

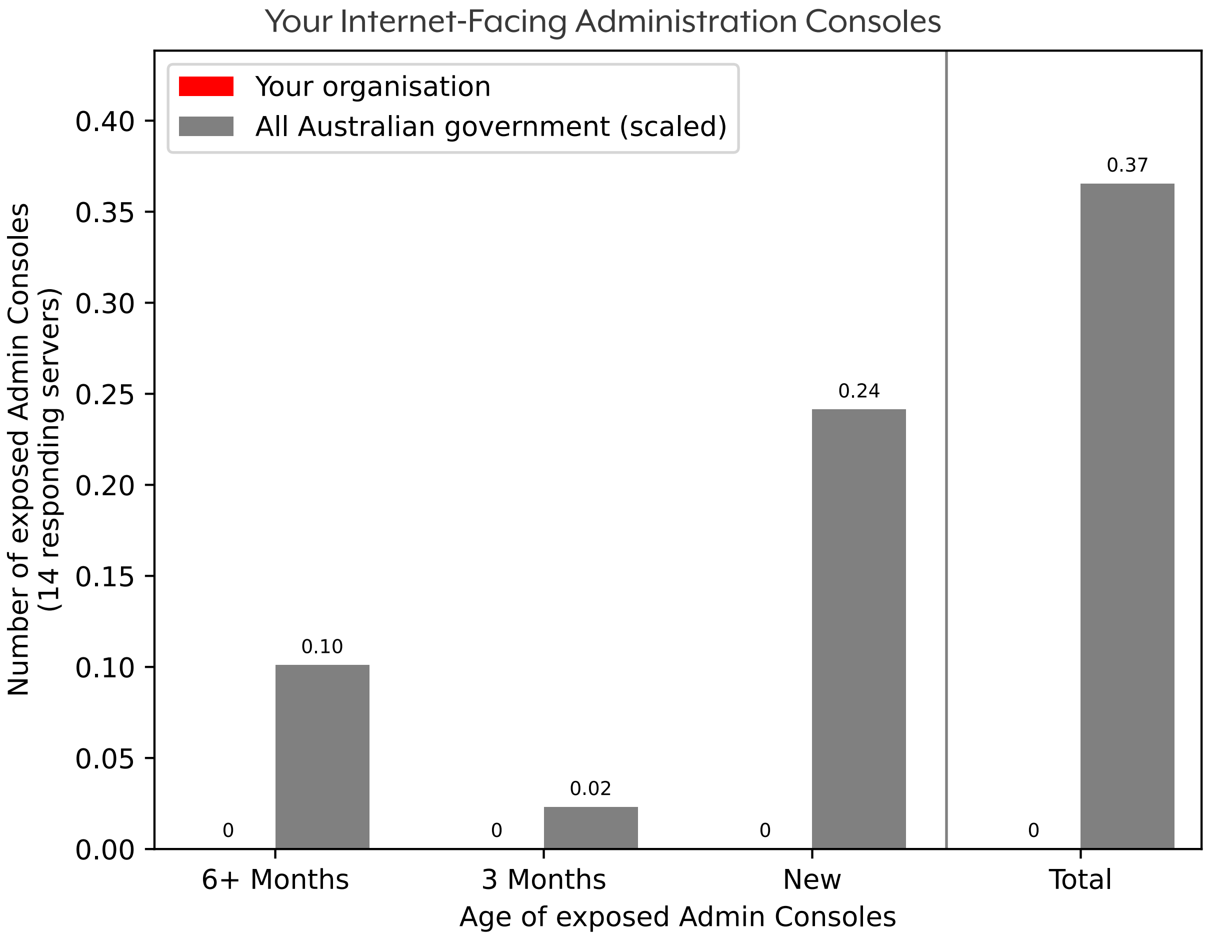


Figure 7.1 Open issues by age

Issues Nov-24: 1	New (existing hosts): 0	New: 0	Issues Feb-25: 0
	Resolved/Mitigated: -1	Removed: 0	

Figure 7.2 Change in open issues since last quarter

Assessed against the limited number of administration consoles that CHIPs can detect. Refer to Background for more information.

8. Multi-Factor Authentication

Multi-factor authentication (MFA) is a highly effective strategy to prevent adversaries gaining unauthorised access. This hygiene indicator identifies internet-facing remote desktop, virtual desktop, virtual private network and corporate email interfaces that do not offer MFA.

Refer to Background for more information.

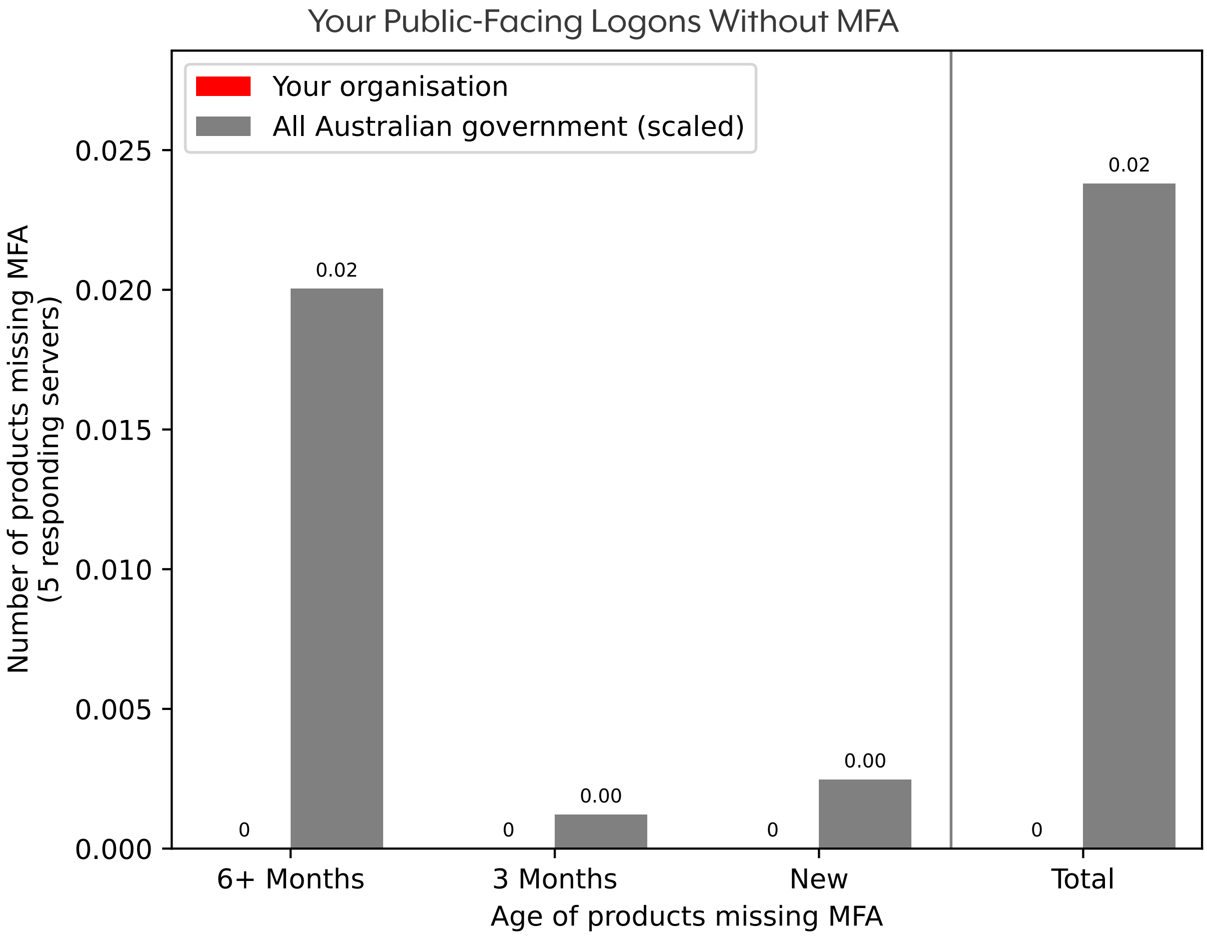


Figure 8.1 Open issues by age

Issues Nov-24:	New (existing hosts): 0	New: 0	Issues Feb-25:
1	Resolved/Mitigated: 0	Removed: -1	0

Figure 8.2 Change in open issues since last quarter

Assessed against the limited number of MFA providers that CHIPs can detect. Refer to Background for more information.

9. Dormant Websites

Dormant Websites assists organisations in identifying websites that may have been forgotten or are not receiving regular support and updates.

Refer to Background for more information.

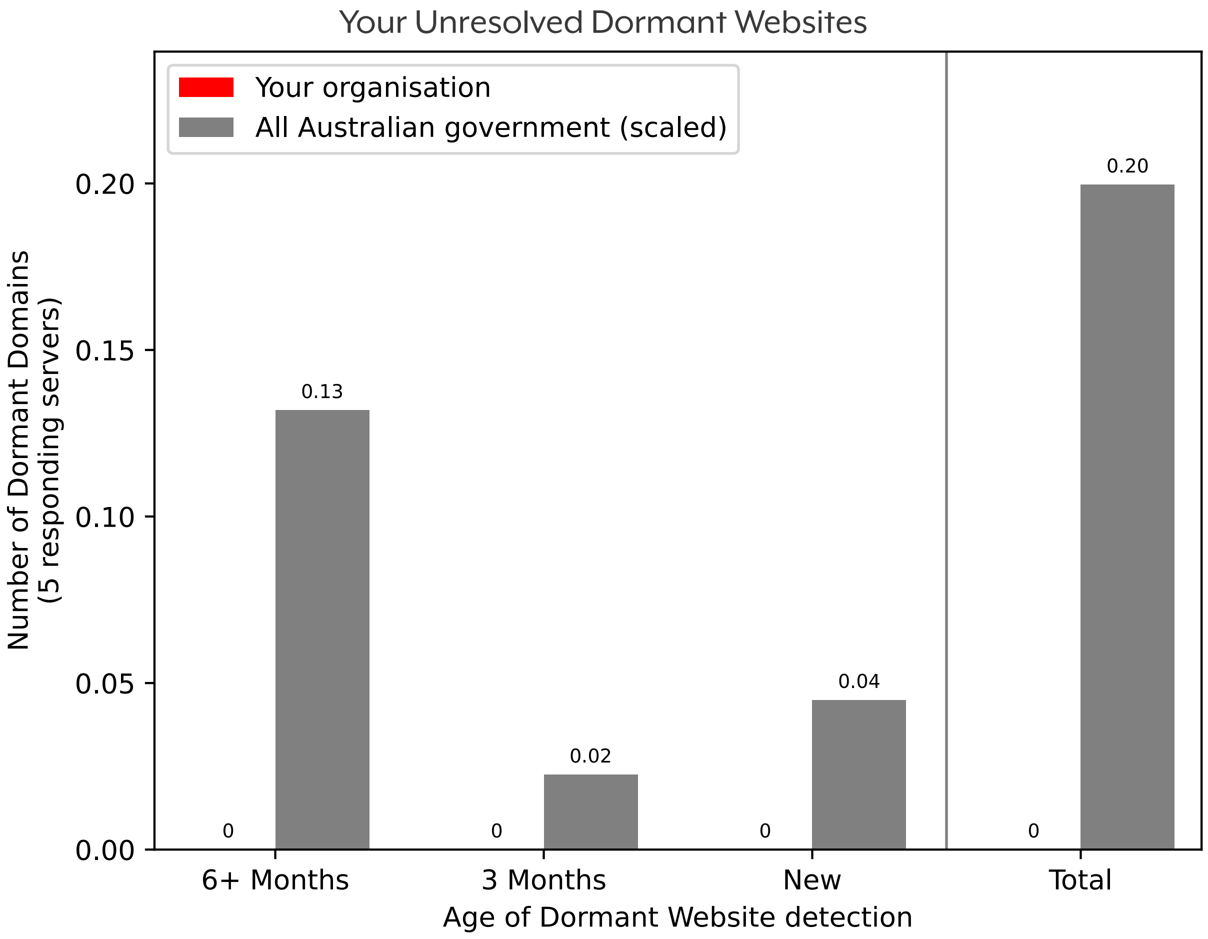


Figure 9.1 Open issues by age

Issues Nov-24: 2	New (existing hosts): 0	New: 0	Issues Feb-25: 0
	Resolved/Mitigated: 0	Removed: -2	

Figure 9.2 Change in open issues since last quarter

Examples of Dormant Websites

No samples of dormant websites available for this quarter.

10. Email Security

Email Security helps organisations identify if they have protected their domains from being used in email spoofing attacks against other organisations and citizens.

Currently, **100.00%** of your email domains do not have adequate protection.

Refer to Background for more information.

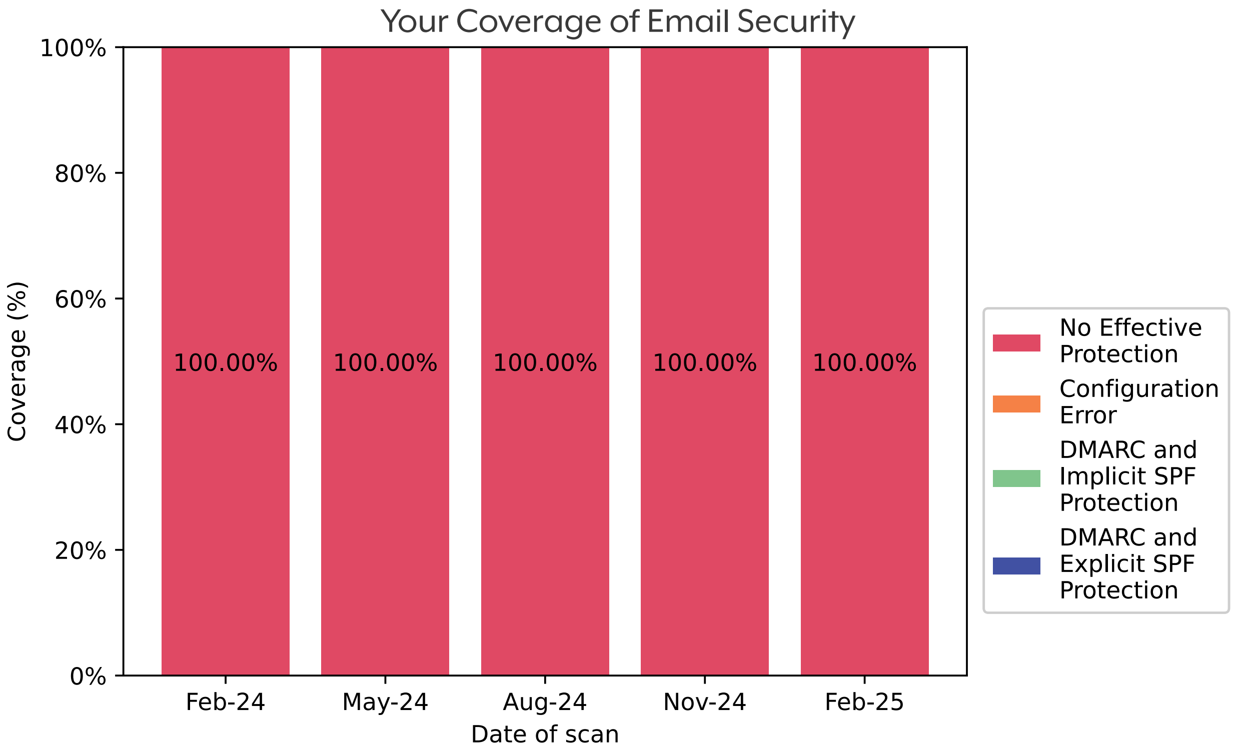


Figure 10.1 Your coverage of Email Security over time

Issues Nov-24: 12	New (existing hosts): 0	New: +4	Issues Feb-25: 16
	Resolved/Mitigated: 0	Removed: 0	

Figure 10.2 Change in open issues since last quarter

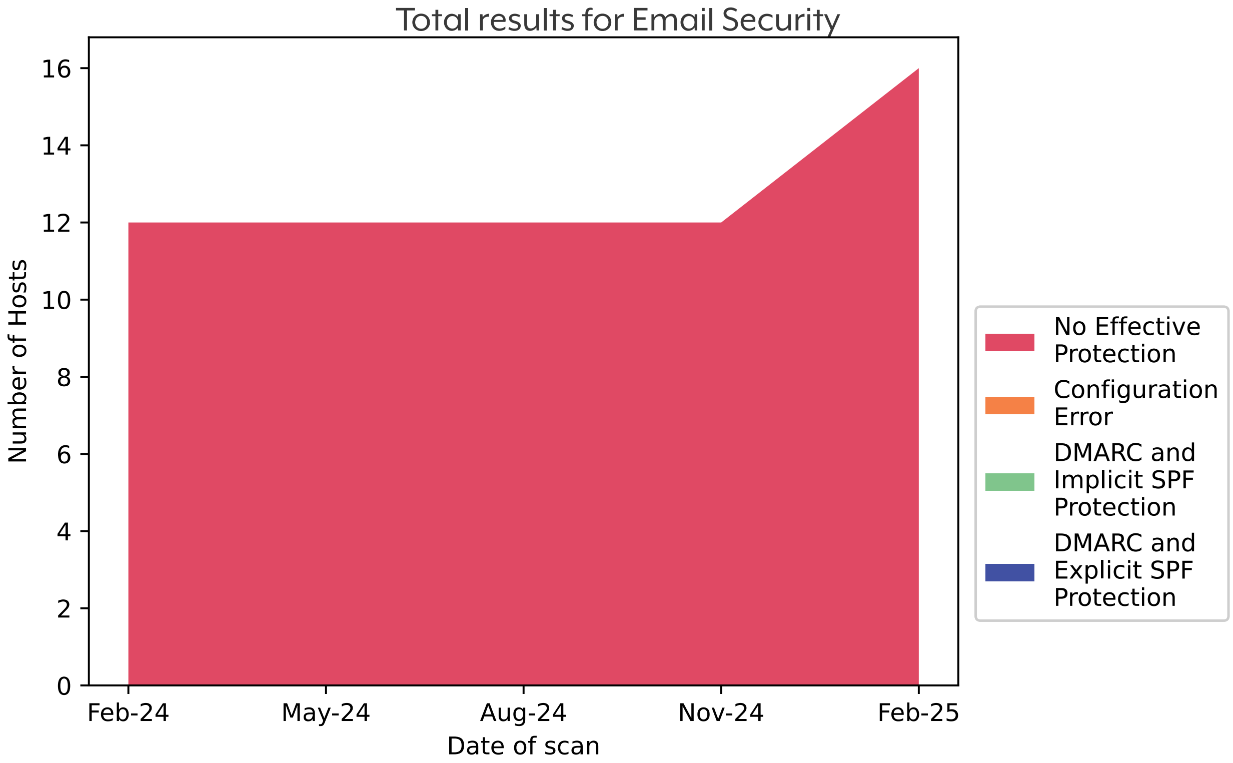


Figure 10.3 Your totals for Email Security over time

Coverage of All Australian government

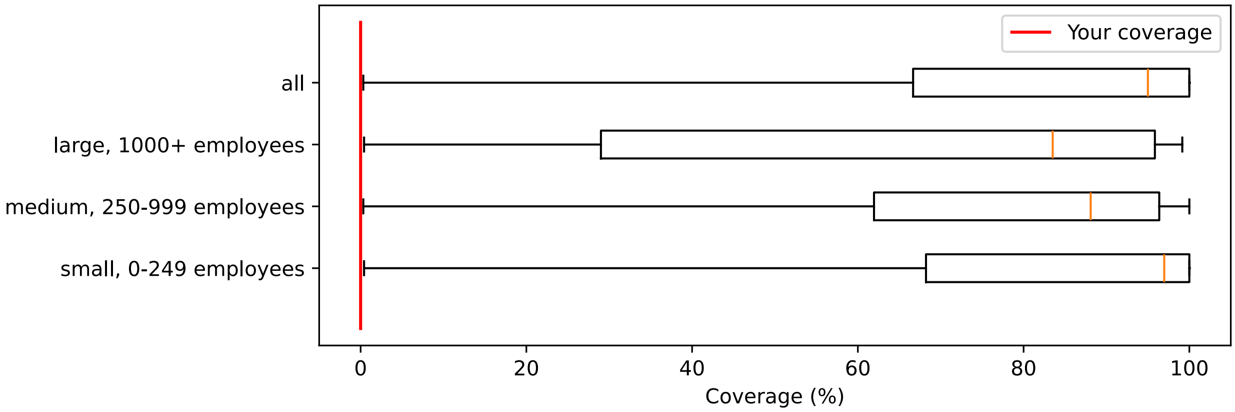


Figure 10.4 Comparison of email security results

Note: For information on this graph see 'Box plots' in Methodology.

11. Website Encryption

Website Encryption identifies websites which are not using encryption in line with the ISM or other relevant contemporary standards. ASD approved TLS1.2 ciphers are in Annex A and B here.

Currently, **60.00%** of your websites do not have adequate encryption.

Refer to Background for more information.

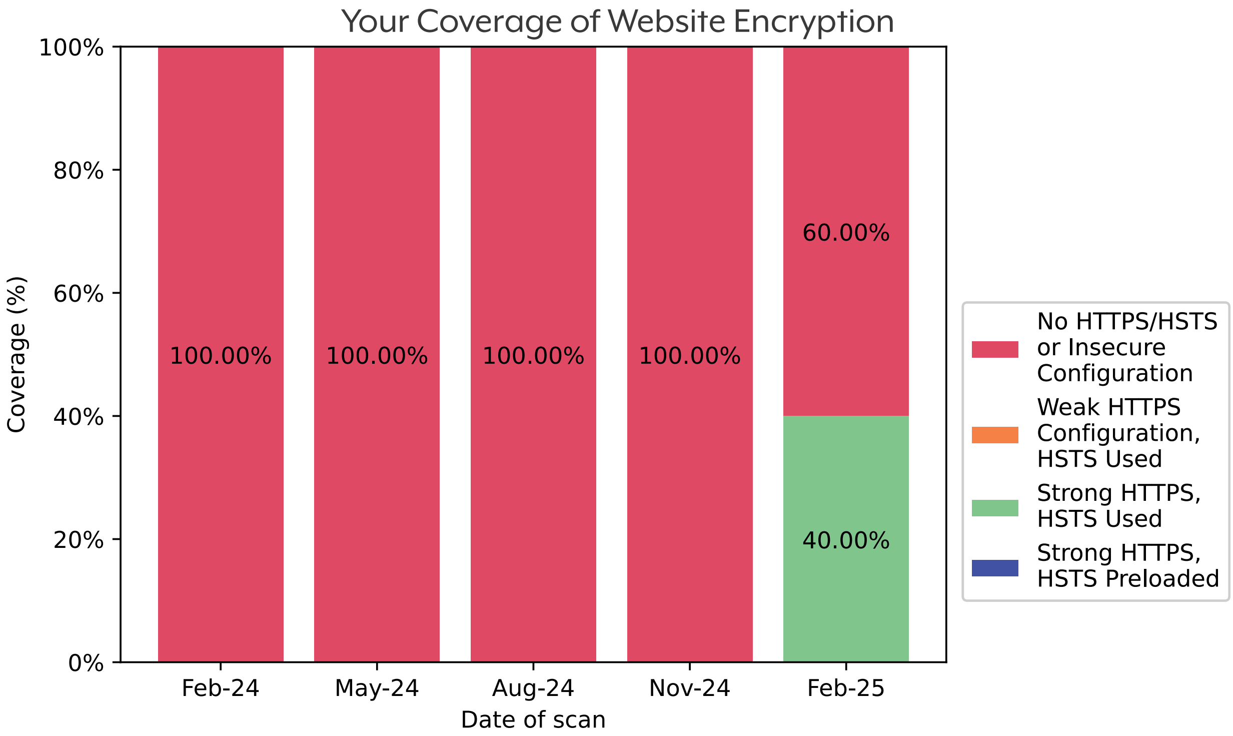


Figure 11.1 Your coverage of Website Encryption over time

Issues Nov-24: 12	New (existing hosts): 0	New: +1	Issues Feb-25: 3
	Resolved/Mitigated: 0	Removed: -10	

Figure 11.2 Change in open issues since last quarter

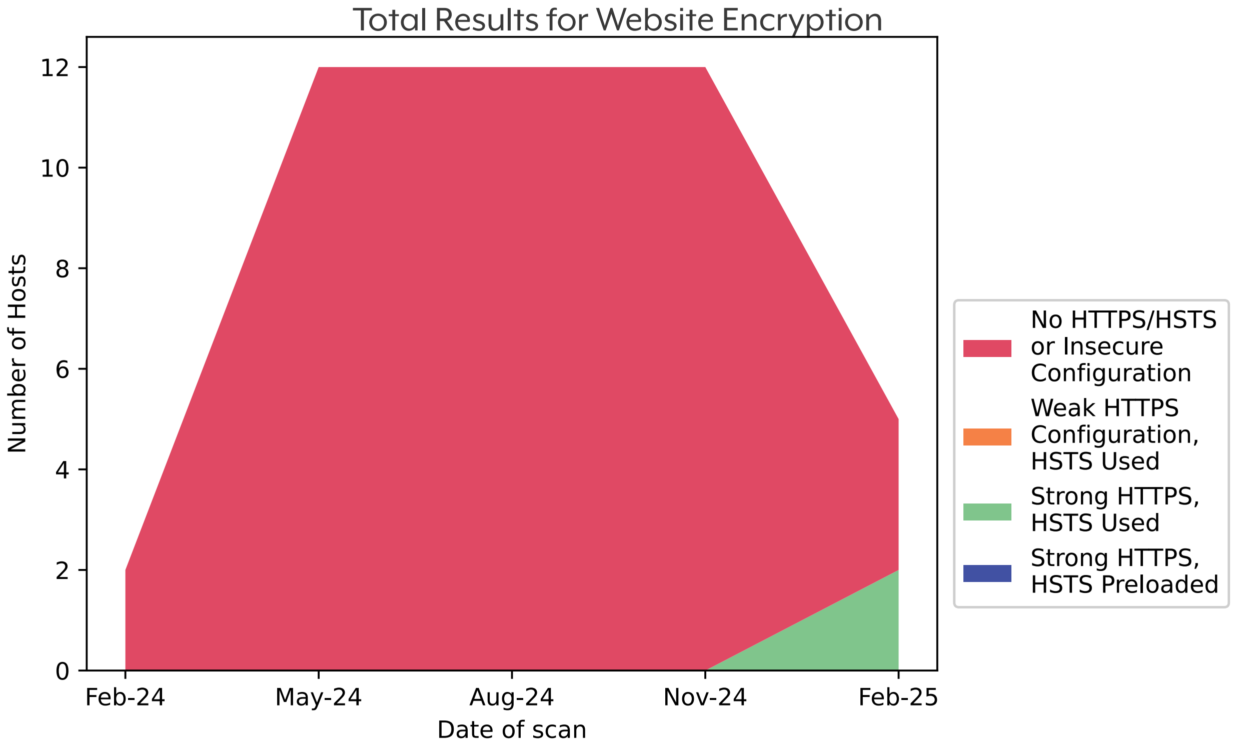


Figure 11.3 Your total results for website domains over time

Coverage of All Australian government

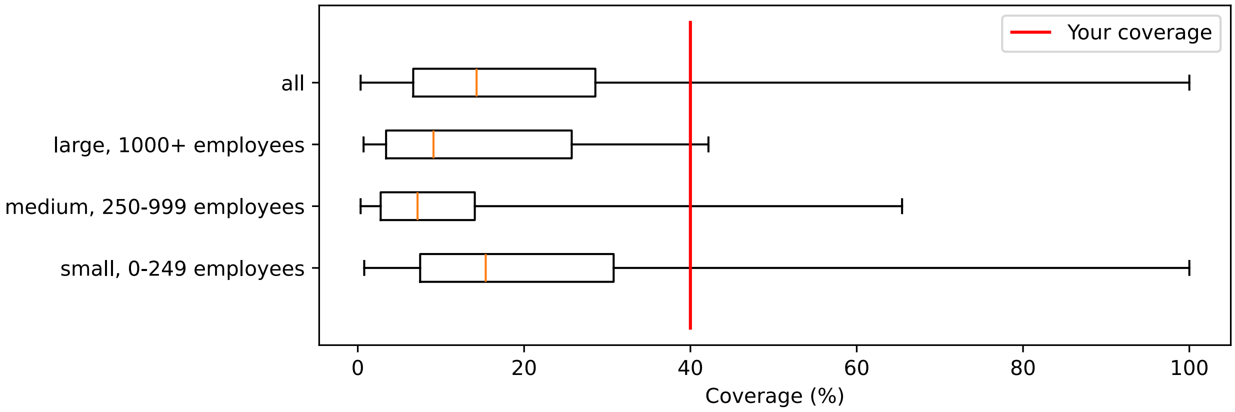


Figure 11.4 Comparison of website encryption results

Note: For information on this graph see 'Box plots' in Methodology.

12. Email Encryption

Email Encryption identifies if your email servers support appropriate encryption protocols and ciphers.

Currently, **0%** of your email servers do not have adequate encryption.

Refer to Background for more information.

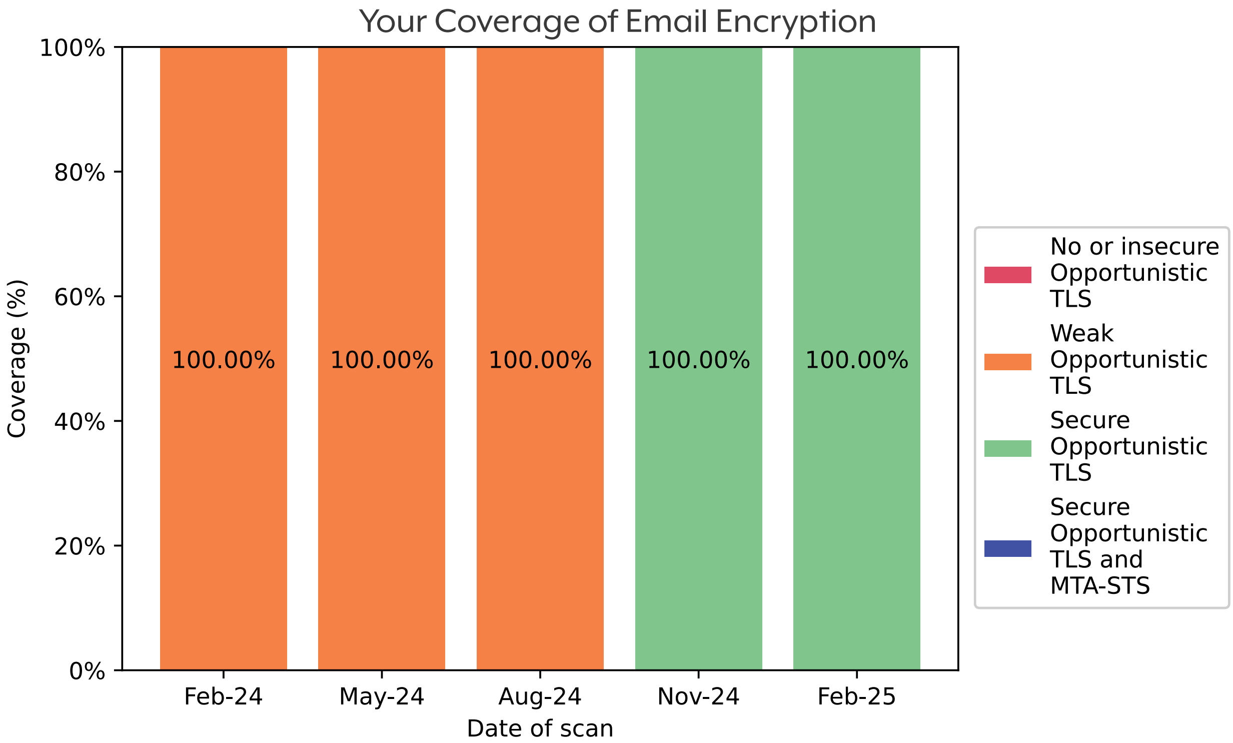


Figure 12.1 Your coverage of Email Encryption over time

Issues Nov-24: 0	New (existing hosts): 0	New: 0	Issues Feb-25: 0
	Resolved/Mitigated: 0	Removed: 0	

Figure 12.2 Change in open issues since last quarter

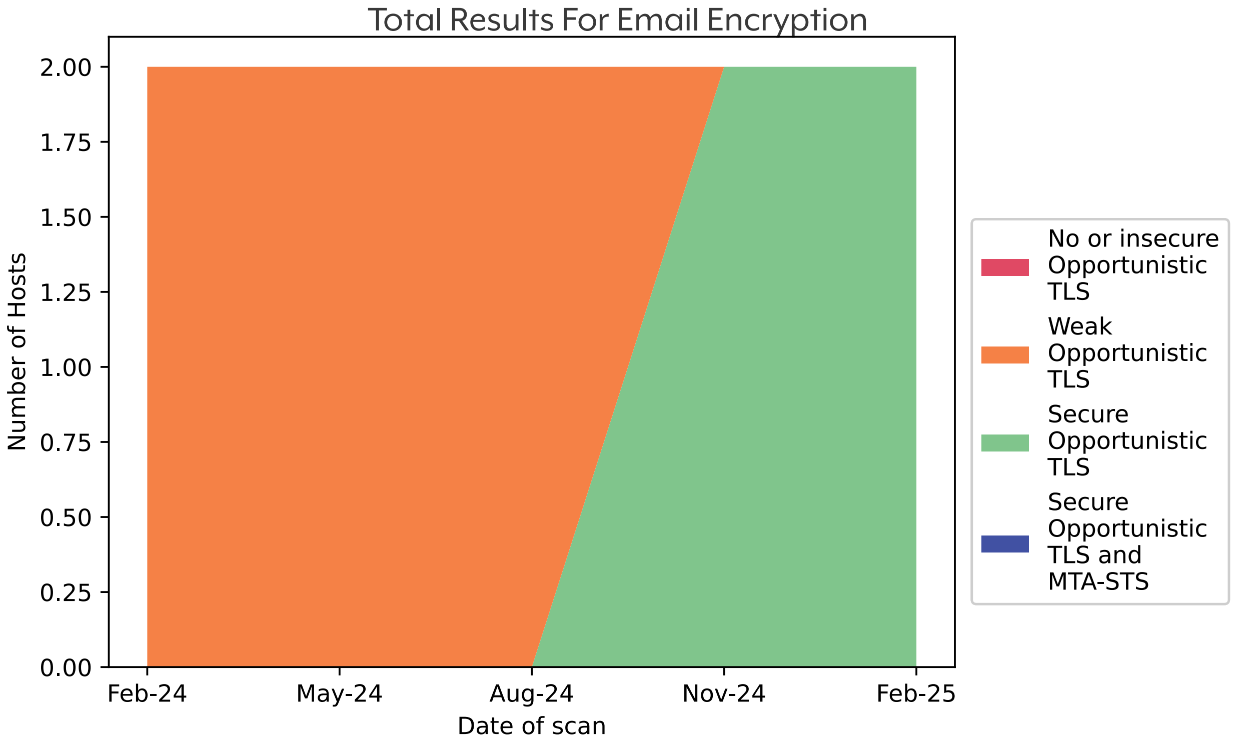


Figure 12.3 Your total results for email domains over time

Coverage of All Australian government

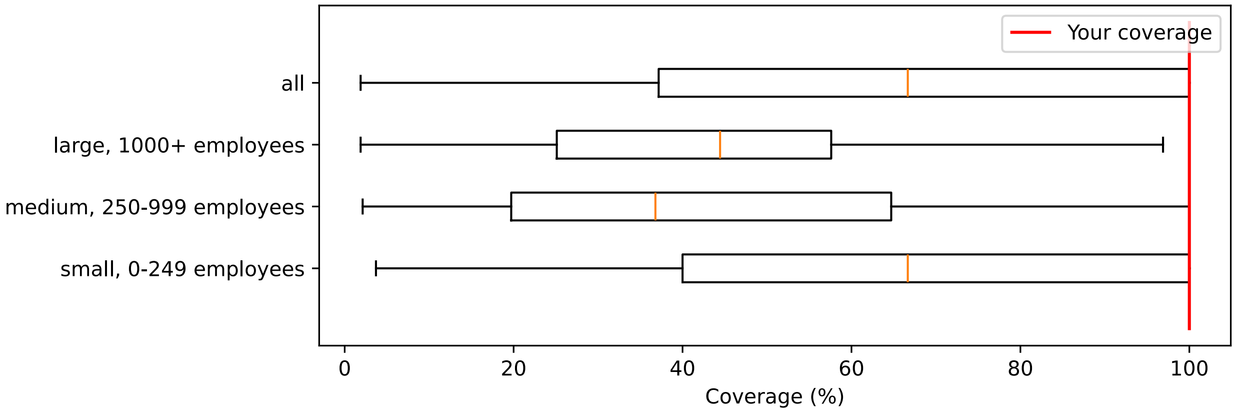


Figure 12.4 Comparison of email encryption results

Note: For information on this graph see 'Box plots' in Methodology.

13. Route Security

Route Security identifies whether an organisation's IP addresses are protected by ROA records to help mitigate route hijacking.

Currently, 9.09% of your IP addresses do not have adequate protection against route hijacking.

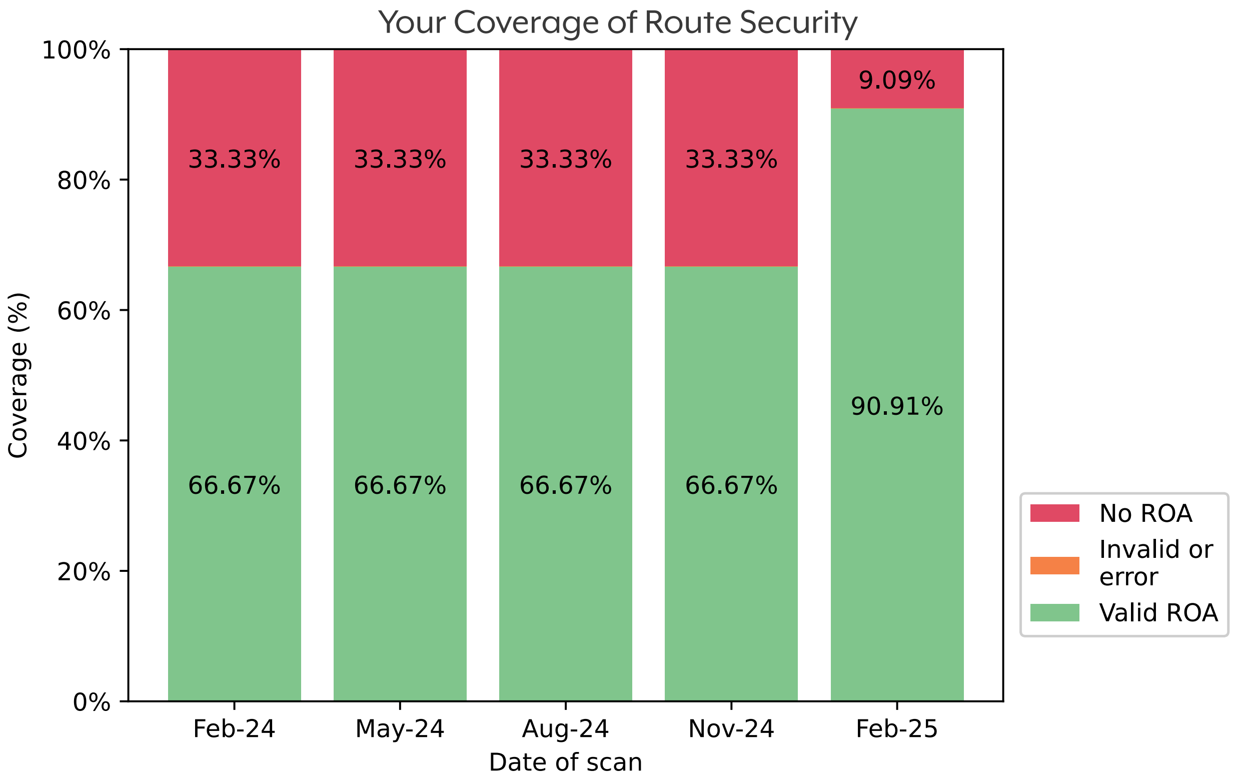


Figure 13.1 Your Coverage of Route Security over time

Issues Nov-24: 8	New (existing hosts): 0	New: +1	Issues Feb-25: 9
	Resolved/Mitigated: 0	Removed: 0	

Figure 13.2 Change in open issues since last quarter

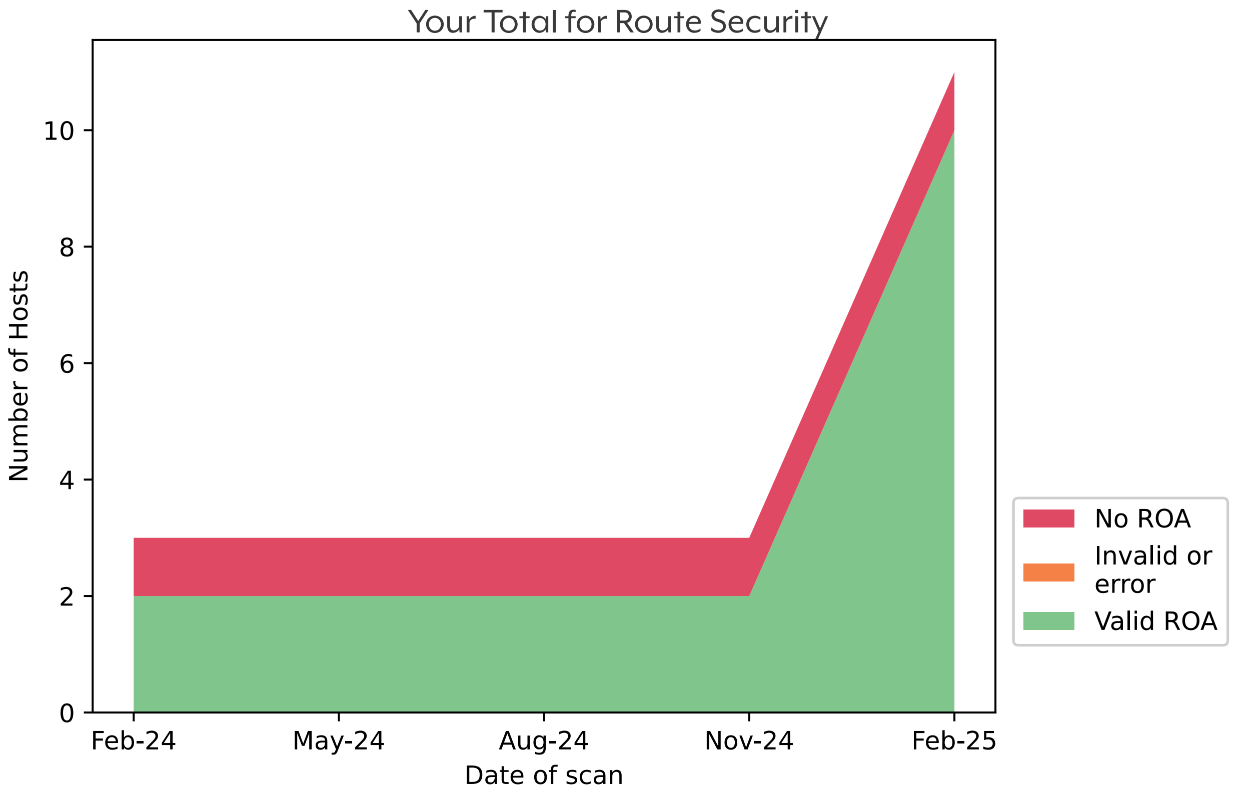


Figure 13.3 Your total results for Route Security over time

Coverage of All Australian government

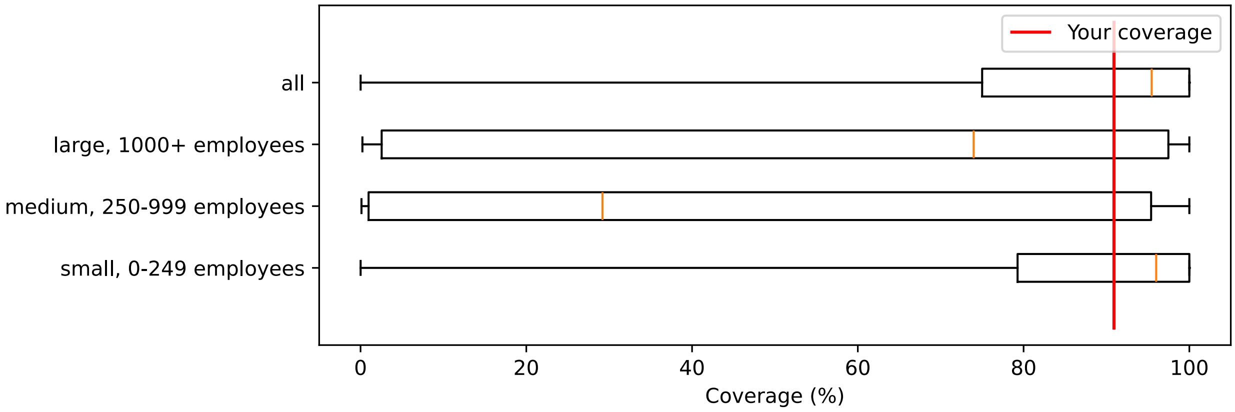


Figure 13.4 Comparison of route security results

Note: For information on this graph see 'Box plots' in Methodology.

14. API Detection

API Detection identifies possible Application Programming Interfaces (APIs) on your internet-facing infrastructure. These may often service mobile and desktop applications, or provide controlled access to your data. Like websites, it is common for APIs to accumulate over time, and it is good practice to ensure each is being actively maintained.

These detections are information-only without scoring. Refer to Background for more information.

Summary of APIs

No API end points were detected in our scan.

Examples of APIs in your environment

No API end points were detected in our scan.

See the attached CSV for a complete listing.

Found Nov-24: 0	New Finds (known hosts): 0	New Hosts: 0	Found Feb-25: 0
	Disabled: 0	Host Removed: 0	

Figure 14.1 Change in visible APIs since last quarter

Note: This table counts hostnames which may host multiple APIs.

15. DNS Hygiene

DNS Hygiene identifies possible misconfigurations in an organisation's Domain Name System records. These issues can lead to host and domain hijacking, information leakage, broken sites, and other issues. DNS Hygiene also reports on the adoption of DNSSEC.

Refer to Background for more information.

Issues Nov-24: 0	New (existing hosts): 0	New: 0	Issues Feb-25: 0
	Resolved/Mitigated: 0	Removed: 0	

Figure 15.1 Change in misconfigurations of your DNS since last quarter

Information about your DNS

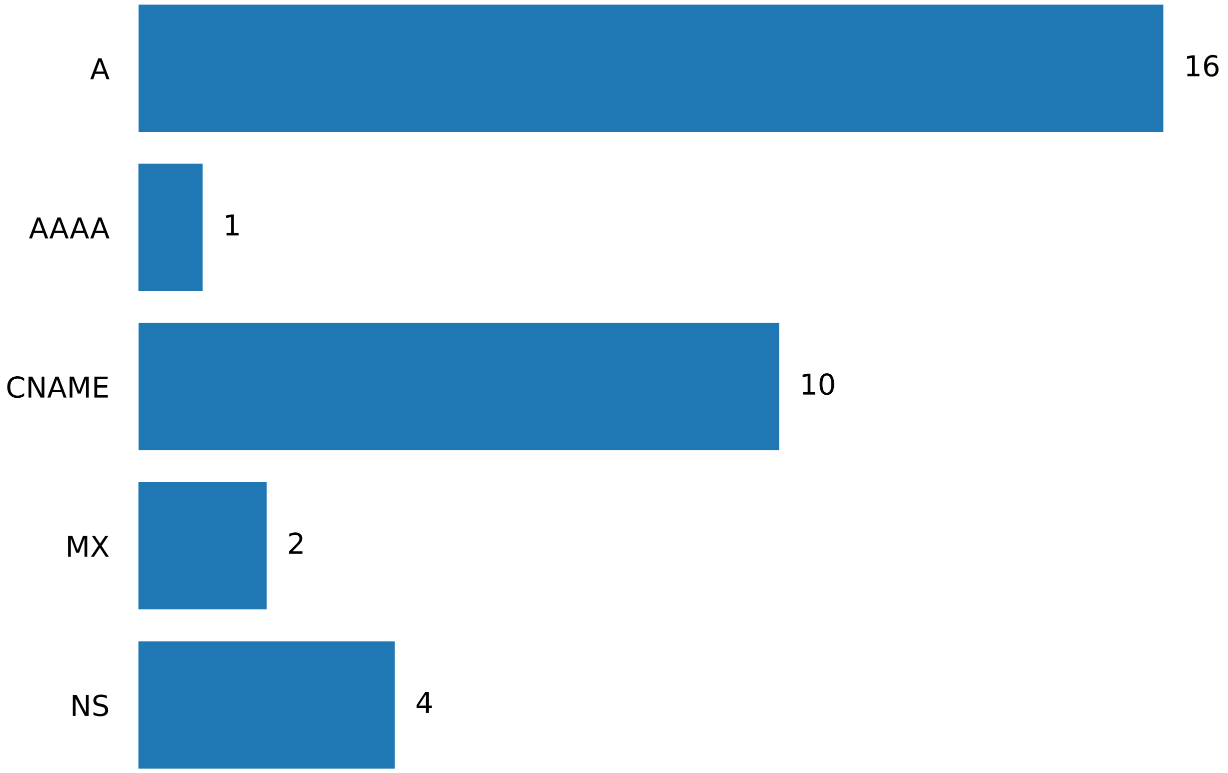


Figure 15.2 DNS record counts by record type

Your organisation DNS results:

- **0** red
- **0** orange
- **0** infomational
- **0** of **2** domains covered with DNSSEC

16. HOT CHIPs Notifications

High-Priority Operational Tasking (HOT) CHIPs informs you of the latest exploits that may affect your internet assets. HOT CHIPs notifications are sent as soon as possible to organisations directly.

Note: If you requested an attribution change based off the HOT CHIPs notifications, these changes are reflected in future notifications. You may still have the incorrect attribution in the below tables, as they are point-in-time assessments.

In the past quarter, HOT CHIPs notified on **0** at-risk systems believed to be associated with your organisation.

NIBBLIES Notifications

In the past quarter you received

- 1 HIBP notifications, affecting 1 email addresses.

17. Third-Party Data Breaches

Third-party data breaches refers to data breaches on third party systems where some of the data disclosed is yours. CHIPs partners with 'Have I Been Pwned' to identify when email addresses associated with your domains come up in data breaches.

Note: This is not a reflection of the security of your organisation's systems, but there are potential risks that you may need to manage. Refer to Background for more information on third-party breaches and what can be done to manage risk.

CHIPs will routinely show any data breaches detected through 'Have I Been Pwned' in the last reporting period.

Breach		Exposed Accounts
	Hopamedia	**2**

Figure 17.1 Third-Party Data Breaches

18. Domain and IP Visibility

Domain Visibility

This data shows changes to your internet footprint for domains.

Note: CHIPs sometimes refers to domains and hostnames as "domains" although they are slightly different things. In most cases the distinction is not meaningful.

Refer to Background for more information.

Active Domains Visible Nov-24	Change	Active Domains Visible Feb-25
12	+4	16
	-0	

Figure 18.1 Active Domains added or removed

Inactive Domains Visible Nov-24	Change	Inactive Domains Visible Feb-25
1	+0	1
	-0	

Figure 18.2 Inactive Domains added or removed

Your organisation has **2** active and **0** inactive organisational level domains (apex domains).

IP Visibility

Changes to the number of IPv4 addresses associated with your organisation and scanned by CHIPs. We also display the number of IPv6 addresses associated.

Refer to Background for more information.

IPv4 addresses attributed to your organisation	0
Live IPv4 addresses	0
IPv6 addresses attributed to your organisation	0

Figure 18.3 Associated IP addresses

19. Appendix - Background

The Cyber Hygiene Improvement Programs (CHIPs) are a series of campaigns to improve cyber security posture across Australia.

About CHIPs

CHIPs focuses on areas of cyber security that are internet-facing and measurable, providing stakeholders with objective data and metrics on the cyber hygiene of their internet-facing systems. This information facilitates better decision-making to improve cyber posture.

Aims

CHIPs aims to increase the awareness of organisations to the configuration of their internet-facing systems and improve their performance by providing regular reporting on hygiene to senior responsible officers.

CHIPs uses no classified intelligence product as input to its reports. All information is gathered from open sources and represents a fraction of the visibility adversaries are able to maintain on organisations internet-facing systems.

New hygiene indicators are regularly added for CHIPs reporting.

History

- In 2018 an open source intelligence assessment of government cyber hygiene identified widespread deviation from ISM guidance and advice.
- CHIPs scans began in December 2018 for federal government organisations.
- CHIPs scans have continued quarterly since February 2019 with additional measurement capability added every three months.
- States and territories have been included in the CHIPs program since November 2019.
- In 2023 CHIPs expanded to begin including industry and critical infrastructure organisations in Australia.
- In 2024 CHIPs doubled the size of the program, crossing 3,500 organisations.

Scale and capabilities

At 01 February 2025, CHIPs:

- Tracks 923,317 active domains and 17,482,164 IP addresses across Australia.
- Reports to over 3,800 organisations.

- Provides visibility on:
  - Critical vulnerabilities on internet exposed systems.
  - Open services (service visibility).
  - Configuration interfaces exposed to the internet (admin consoles).
  - Corporate email and VPN/VDI style interfaces without Multi-factor Authentication (no MFA).
  - Unmaintained websites (dormant websites).
  - Encryption configurations (for websites and email).
  - Anti-spoofing protection on domains (email security).
  - Third-party data breaches involving government domains (third-party data breaches).
  - Domain names and hostnames attributed (domain visibility).
  - IP addresses attributed (IP visibility).
  - DNS zone file validation and dangling hostname detection (DNS hygiene).

CHIPs regularly expands the cyber hygiene metrics to provide additional visibility of cyber hygiene.

How CHIPs data is used

Detailed CHIPs reports are distributed quarterly directly to organisations that have provided CHIPs with contact details.

For government organisations, CHIPs data is available to the relevant state or territory or portfolio cyber lead.

CHIPs data is used to inform cyber security related intelligence assessments. CHIPs data is shared internally with ASD teams responsible for the protection of Australian systems.

Anonymised CHIPs data is used in various external reports by ASD including:

- Reporting to federal parliament on the performance of federal government portfolios and organisations.
- ASD Annual Threat Briefing.

Similar data will also be provided to state and territory parliaments upon request.

Critical Vulnerabilities

Software vulnerabilities in internet-facing systems provide malicious actors with an easy opportunity to establish a staging point from which to further explore and attack an organisation's networks. During the last four years ASD has observed a major increase in the use of internet-facing software vulnerabilities to compromise networks.

The Critical Vulnerabilities hygiene indicator gives organisations visibility of serious 'Copy-Paste' vulnerabilities that CHIPs is able to detect.

Detection for critical vulnerabilities is added on a vulnerability-by-vulnerability basis. To be included a vulnerability must be:

- Serious and likely to allow the compromise of the system if left unpatched (such as, through Remote Code Execution, or leaking of critical information which will allow compromise).
- Detectable with a high degree of confidence.
- Related to a technology known to, or likely to be used by, government or critical infrastructure.
- In active use by, or expected to be used by, malicious actors.

Not all serious vulnerabilities can be detected with high-confidence. In some cases, CHIPs can only determine that a system 'may be vulnerable'. For these cases, CHIPs reports the potential vulnerability in the critical vulnerabilities CSV file. CHIPs is aware these findings may contain false positives, but on balance, provides this information for visibility so that your organisation can make its own determination on whether the system is vulnerable.

The CHIPs critical vulnerability scanning capability is not exhaustive and should not be seen as a replacement for organisations operating their own vulnerability scanning capability.

ASD recommends that organisations review reported items carefully. However, false positives are always possible. If an organisation believes a reported, high-confidence, critical vulnerability is a false positive please notify the CHIPs team so scanners can be adjusted to improve accuracy.

Detected vulnerabilities

At 01 February 2025 CHIPs may detect, with high confidence:

- Apache Httpd: (CVE-2021-41773, CVE-2021-42013)
- Apache Ofbiz: (CVE-2020-9496, CVE-2023-51467)
- Apache Solr: (CVE-2019-0193)
- Apache Tomcat: (CVE-2020-1938)
- Atlassian Confluence: (CVE-2019-3396, CVE-2019-3398, CVE-2021-26084, CVE-2022-26134,CVE-2023-22515, CVE-2023-22527)
- Atlassian Crowd: (CVE-2019-11580)
- Centreon: (CVE-2020-10945)
- Citrix Netscaler/ADC: (CVE-2019-19781, CVE-2022-27510, CVE-2022-27518, CVE-2023-3519)
- ConnectWise Screenconnect: (CVE-2024-1709, CVE-2024-1708)
- Crush FTP: (CVE-2024-4040)
- Cutenews: (CVE-2019-11447)

- DotNetNuke: (CVE-2018-15811, CVE-2017-9822, CVE-2018-15812, CVE-2018-18325, CVE-2018-18326)
- Drupal: (CVE-2020-28948, CVE-2018-7600)
- Exim SMTP: (CVE-2023-42114, CVE-2023-42115, CVE-2023-42116, CVE-2023-42117, CVE-2023-42118)
- Fortigate: (CVE-2018-13383, CVE-2020-19283, CVE-2022-39952, CVE-2022-40684, CVE-2023-27997, CVE-2024-21762, CVE-2024-23113)
- Fortimail: (CVE-2020-9294)
- GeoServer: (CVE-2024-36401)
- Global Protect: (CVE-2024-3400)
- Ivanti Connect Secure (All versions considered critically vulnerable)
- Jenkins: (CVE-2024-23897, CVE-2024-23898, CVE-2018-1999002)
- Jetbrains TeamCity (CVE-2024-23917)
- ManageEngine ADSelfService Plus: (CVE-2021-40539, CVE-2022-47966)
- Microsoft Exchange: (CVE-2005-0560, CVE-2020-0688, CVE-2020-17144, CVE-2021-26857 CVE-2021-26412,CVE-2021-27078, CVE-2021-26854, CVE-2021-26855, CVE-2021-27065, CVE-2021-26858, CVE-2021-28480, CVE-2021-28481, CVE-2021-28482, CVE-2021-28483, CVE-2021-34473, CVE-2021-34523, CVE-2021-33766, CVE-2021-31195, CVE-2021-31198, CVE-2021-31207, CVE-2021-31209, CVE-2021-31196, CVE-2021-31206, CVE-2021-33768, CVE-2021-34470, CVE-2022-41040, CVE-2022-41082, CVE 2023-32031, Exchange 2013 is considered critically vulnerable and unpatchable due to being out of support)
- Microsoft Sharepoint: (CVE-2019-0604, CVE-2019-0594, CVE-2010-3964, CVE-2023-29357)
- MobileIron/EPMM: (CVE-2021-44228, CVE-2020-15505, CVE-2023-35078)
- Oracle Weblogic: (CVE-2020-14644)
- OpenAM: (CVE-2021-35464)
- Pulse Connect: (CVE-2019-11510, CVE-2021-22893)
- Sitecore: (CVE-2021-42237, CVE-2023-35813)
- Sonatype: (CVE-2020-10199, CVE-2020-10204)
- Sonicwall: (CVE-2021-20038)
- Sophos Firewall: (CVE-2020-12271, CVE-2022-1040)
- Telerik: (CVE-2019-18935, CVE-2017-11317, CVE-2017-11357)
- Wordpress Plugins:
    - Elementor: (CVE-2023-48777)
    - Backup Migration: (CVE-2023-6553, CVE-2023-6971, CVE-2023-6972, CVE-2023-7002)
    - Layer Slider: (CVE-2024-2879)
    - Hash Form: (CVE-2024-5084)
    - LiteSpeed Cache: (CVE-2024-44000, CVE-2024-28000)
- VMware Horizon: (CVE-2021-44228, CVE-2021-45046)

In the critical vulnerabilities CSV file CHIPs will also report these lower confidence findings if detected (i.e. may be vulnerable):

- Telerik 2017 and later (CVE-2019-18935, CVE-2019-3398 and CVE-2017-11357)
- Cisco Adaptive Security Appliance (ASA): (CVE 2024-20353)

For lower confidence detections, it is not possible for CHIPs to positively determine if systems are vulnerable without attempting to exploit. Organisations should review these findings and determine their own risk and patch levels against these known vulnerabilities.

Detection capabilities will continue to be expanded in future reports.

Relevant ISM Controls: 1691, 1694.

Service Visibility

Open ports on internet exposed devices add to the overall attack surface of systems. While some ports need to be open to provide services across the internet, many do not.

Adversaries can quickly and easily obtain information on open services using open source intelligence aggregators without needing to scan your network. ASD experience shows few organisations detect this scanning activity, even when noisy and attributed.

Organisations should regularly review internet exposed services to confirm they are necessary to provide its services and are being risk managed with all reasonable and practical mitigations, including:

- Timely patching of all internet exposed services.
- Terminating internet exposed services in segregated parts of the network, such as a DMZ.
- Only opening services designed and tested for exposure to the public internet.
- Logging and monitoring access to these services.
- Regularly conducting vulnerability assessments against internet exposed services.

Note: Publishing services on non-standard ports does not provide suitable protection as this tends to highlight services that would be of interest to an adversary.

The service visibility data is based on data from open source intelligence aggregators, specifically Shodan and Censys. This data can be dated (up to a month old) and may contain false positives. It is recommended that before any action or decision is taken on the basis of this report, organisations conduct their own review of their open services in the context of their operational requirements and plan any remediation activity accordingly.

Relevant ISM Controls: 0631, 0628.

Administration Consoles

Administration consoles allow privileged users to adjust the configuration and operation of systems. Leaving administration consoles exposed to the internet increases the risk of systems being compromised. Privileged access is often a key goal of an adversary. They can use privileged access to:

- Propagate malware to multiple workstations and servers.
- Add new user accounts, including privileged accounts.
- Bypass security controls for applications, databases and file servers.
- Implement configuration changes to make future access easier.

Admin consoles should only be accessible from an internal network or via other secure paths to reduce the chance of systems being compromised due to software faults, brute force, credential re-use, and other adversary techniques.

Detected consoles

At 01 February 2025 CHIPs may detect:

- Aruba admin consoles
- Specific Cisco management interfaces
- Coldfusion admin consoles
- cPanel admin consoles
- Cyberhound admin consoles
- CrushFTP admin consoles
- Django admin consoles
- Exchange admin centre login pages
- Specific F5 Big IP products admin consoles
- FortiGate admin consoles
- FortiMail admin consoles
- FortiManager admin consoles
- FGFM protocol on TCP 541 or 542
- GoAnywhere admin consoles
- Jenkins admin consoles
- Juniper J-Web interfaces
- KairosDB consoles
- Metabase admin consoles
- OpenVPN admin consoles
- Palo Alto management interface
- pfSense consoles

- PGAdmin consoles
- PHPMyAdmin consoles
- Pritunl admin consoles
- PRTG network management consoles
- Pulse admin consoles
- SAP admin consoles
- Sitecore admin consoles
- SNMP protocol on UDP 161
- Sonicwall admin consoles
- Splunk admin consoles
- Synology admin consoles
- UniFi admin consoles
- Weblogic admin login pages
- Specific VMWare products admin consoles

Detection capabilities will continue to be added and updated in future reports.

Advice on configuring privileged access management for admin consoles is detailed in ASD publication Secure Administration.

Relevant ISM Reference: Protect Principles P3 and P4.

Multi-factor Authentication

Services that grant authorised access to internal resources over the internet, which only require username and password authentication, are susceptible to a broad range of attacks including, password spraying, credential stuffing, brute force attacks, credential reuse and more.

Multi-factor authentication (MFA) is a mitigation strategy that requires users to provide more than one factor of authentication, beyond their username and password, before being granted access. MFA requires at least two factors from the following:

- Something only the user knows e.g. password, passphrase or PIN.
- Something the user has e.g. client certificate, physical token, etc.
- Something the user is e.g. biometrics, fingerprints, iris scans, etc.

MFA detection assists organisations by identifying high value services, such as remote/virtual desktops, virtual private networks (VPN), and corporate email interfaces that are exposed to the internet but do not appear to be protected by MFA.

Confidence in MFA detection is subject to the services being scanned and the MFA methodologies being utilised by the service. Due to the various unique methods of implementing MFA, CHIPs scanning covers a limited number of common services and MFA providers.

Providing certainty in MFA detection would require attempting authentication which is not within CHIPs' scope. Results are therefore not definitive and an organisation should make their own assessment on whether their authentication methods meet the minimum requirements for MFA and their individual risk appetite.

Current services being scanned for MFA include the following:

- Citrix Remote Desktop
- Cisco ASA Anyconnect VPN
- F5 BIG-IP Edge Client
- FortiClient
- Outlook Web Access
- Palo Alto Networks GlobalProtect VPN
- Windows Server Web Access
- Any login pages utilising DUO MFA (CISA Alert AA22-074A).

Current MFA platforms and methodologies within CHIPs detection capabilities:

- Citrix enabled MFA
- F5 enabled MFA
- Cisco ASA enabled MFA
- FortiToken
- Auth0
- Okta
- RSA SecurID
- SAML/Single Sign On (SSO)
- Microsoft 365

The tests used to determine if MFA is adequate is based on the recommended and required criteria for multi-factor authentication used by ASD in Protect Yourself: Multi-Factor Authentication.

Due to limitations in capabilities, orange scoring is attributed to a host when it is not possible to determine if the authentication measures in place meet MFA requirements or not enough information was able to be gathered by the scanner to attribute whether or not the page has MFA.

Detection capabilities will be expanded to more authentication services and MFA platforms in future reports.

Relevant ISM controls: 0974, 1173, 1401, 1504, 1505, 1559, 1679, 1680, 1681, 1682, 1683, 1684.

Dormant Websites

Websites are highly visible and accessible. Organisations should ensure that websites are maintained and kept up to date, by:

- Supporting and patching operating system and application software.
- Using appropriate and hardened configurations.
- Keeping content current and up to date.
- Handling unexpected requests gracefully.

Recommendations for managing websites including patching and configuration hardening are outlined in the ISM (see Guidelines for System Management and Guidelines for Software Development).

Relevant ISM Controls: 0304, 1501, 1409, 1239, 1240.

Email Security

Adversaries commonly conduct attacks using spoofed email. Email spoofing can be used to gain the trust of a target and increase the likelihood of a successful cyber intrusion.

Organisations can reduce the effectiveness of spoofing, and protect their brands, by implementing Sender Policy Framework (SPF), Domain-based Message Authentication, Reporting and Conformance (DMARC), and Domain Keys Identified Mail (DKIM) records in their Domain Name System (DNS) configuration.

SPF is an email verification system designed to detect spoofed emails. DMARC allows organisations to specify policies for the handling of spoofed email, including how others can notify the organisation of spoofing attempts. DKIM allows organisations to digitally sign email providing recipients with high-assurance that the email is genuine.

SPF and DMARC records are highly visible indicators of cyber hygiene. The public can query a DNS server and see whether an organisation has SPF and/or DMARC records in place.

Advice on utilising SPF and DMARC is detailed in the ASD publication How to Combat Fake Emails.

Relevant ISM Controls: 0574, 1183, 1540.

Website Encryption

HTTPS (Hypertext Transfer Protocol Secure) and TLS (Transport Layer Security) are protocols that provide encryption and authentication to assure users of the World Wide Web that they are connecting to the website they intended to, and that their interactions are not able to be viewed or modified while in transit.

All public-facing websites should use HTTPS to protect their users' confidentiality.

HTTP Strict Transport Security (HSTS) is a web security policy mechanism that helps protect users from person-in-the-middle attacks. It allows web servers to tell HTTPS compatible web browsers that they should only interact with the web server over HTTPS connections. Compliant web browsers will also change any insecure links to secure links (e.g. http://cyber.gov.au becomes https://cyber.gov.au).

HTTPS and TLS configurations are highly visible indicators of cyber hygiene. The public can query web servers using a variety of tools and websites, which will assess whether the security is being operated in line with the government's or other contemporary standards.

CHIPs has expanded the acceptable TLS cipher suites to improve alignment with Content Distribution Networks' (CDNs) most stringent TLS configurations. These ciphers use 'Cipher Block Chaining' - a method that is no longer considered completely safe, but for which attacks remain theoretical. These ciphers will be removed if practical weaknesses are identified, or when CDNs make stronger alternatives possible.

Advice on utilising HTTPS and TLS for websites, and recommended ciphers are detailed in the ASD publication Implementing Certificates, TLS, HTTPS and Opportunistic TLS.

Relevant ISM Controls: 1552, 1139, 1553, 1453, 1369, 1370, 1372, 1448, 1374, 1375, 0476, 0471, 0994, 0472, 1629, 0473, 1630, 1446, 0474, 0475, 0476, 0477, 0479, 0480, 0481, 0998.

Email Encryption

Opportunistic TLS (IETF RFC 3207) is a mechanism that enables mail servers to use encryption to protect email messages in transit. All mail servers should support and offer Opportunistic TLS.

Opportunistic Encryption is highly susceptible to person-in-the-middle downgrade attacks. Domain owners should use Mail Transport Agent - Strict Transport Security (MTA-STS) to reduce the opportunity for downgrade attacks against their mail servers.

Similar to websites, TLS encryption on mail servers needs to be configured with an appropriate certificate and set of cryptographic protocols and cipher suites.

CHIPs data indicates that encryption settings on email servers are frequently overlooked. Additionally, mail servers are not as regularly updated as web browsers and other end user software that uses TLS. Consequently, many email servers only support older and less secure version of TLS and ciphers.

To offer the strongest security possible, mail servers should offer the latest and strongest cryptography possible, but should also accept lower standards of cryptography to allow encrypted mail delivery with older servers.

Advice on the selection of TLS protocols, configuration options, cipher suites and MTA-STS can be found in the ASD publication Implementing Certificates, TLS, HTTPS and Opportunistic TLS.

All mail servers should implement MTA Strict Transport Security (MTA-STS) using the enforce mode.

MTA-STS will allow the mail server provider to declare their ability to use TLS.

Where enforce mode is implemented, this will specify that sending MTAs should refuse to deliver messages to hosts that do not offer TLS with trusted server certificates.

The recommendation to use Opportunistic TLS and MTA-STS is contained in the ISM Guidelines for Email.

Relevant ISM Controls: 0572, 1589 and TLS related controls from above.

API Detection

Application Programming Interfaces (APIs) allows a calling process to exchange information automatically with a server component. APIs can be used by a client process for record access (Create Read Update Delete - CRUD) and controlling infrastructure.

Security issues with APIs can be particularly serious as a poorly secured API will allow attackers to rapidly and conveniently access records and systems they are not supposed to. Further, because humans rarely see APIs, security issues with them are often overlooked.

Security issues related to APIs include issues such as poor authentication, poor handling of authentication credentials, poor validation of security tokens, inadequate access control - particularly Insecure Direct Object Reference (IDOR) and other programming logic faults.

API security issues are often the result of incorrect assumptions about where business rules are enforced in multi-tier systems. They can be challenging for people familiar with the system to spot but easy for malicious actors familiar with these kinds of logic errors to identify.

It is important for organisations to know what APIs it exposes to the internet and carefully review those APIs to ensure they have appropriate security.

API detection provides organisations with an understanding of their internet-exposed APIs. This report is non-exhaustive and relies on CHIPs endpoint discovery process.

ASD recommends organisations:

- Review and ensure that all internet-exposed APIs are supposed to be.
- Carefully review the security of APIs that are exposed on the internet.

Route Security

Adversaries routinely attempt to reroute traffic to create interception opportunities or effect denial of service attacks. One frequently used technique is fake route announcements which advertise routes to IP address space that is owned by someone else.

Resource Public Key Infrastructure (RPKI) uses public key cryptography to authenticate routing data on the internet. This allows telecommunications carriers and cloud service providers to verify routing data they receive, transmit and process in order to determine routing calculations for internet traffic. By publishing RPKI data, an organisation may reduce Border Gateway Protocol-related (BGP) cyber threats, such as some types of denial-of-service attacks, accidental or deliberate rerouting of internet traffic, and opportunities for the undermining of IP address-based reputational services.

RPKI Route Origin Authorization (ROA) associates IP networks (usually referred to as prefixes) with Autonomous System Numbers (ASN). This allows routers receiving BGP announcements to confirm that an IP prefix is being announced by an ASN authorised to announce it.

Without RPKI, internet routers normally implicitly trust routes shared with them by ASNs they peer with.

Internet routing is a specialised area. Depending on your arrangements you may need to discuss these results with your internet service provider, or an internet routing specialist.

Further information on:

- BGP route hijacks: Protecting the Integrity of Internet Routing: Border Gateway Protocol (BGP) Route Origin Validation.
- RPKI: APNIC - What is RPKI?
- ROA: APNIC - Routing.
- Securing BGP with RPKI: Securing BGP.

Relevant ISM Controls: ISM-1783.

DNS Hygiene

DNS is a fundamental protocol on the internet and provides the ability to translate domain names and hostnames to specific service endpoints such as IP addresses. These IP addresses then allow transfer of information over the internet. Sometimes described as the "phone book for the internet", DNS is instrumental to the operation of the internet, and has also become crucial to internet security.

DNS misconfiguration, and failing to take advantage of contemporary security features in DNS, creates opportunities for adversaries to obtain malicious advantage by pretending to be legitimate organisations that other systems and users may trust. This trust is then abused for purposes such as credential scraping, watering hole attacks, interception of confidential information and other malicious activity. And while encryption with authentication, such as TLS, can mitigate some of these risks, in other cases DNS proves to be a lynchpin that holds the entire trust model together.

The DNS Hygiene capability provides organisations with information on many different DNS configuration issues, ranging in severity from serious to information only.

Detected issues include:

- **Dangling hostnames** – dangling hostnames allow adversaries to host content claiming to be a legitimate organisation, often complete with a valid TLS certificate. Dangling hostnames are a security risk and should be removed from DNS if no longer required.
- **Dangling storage** - dangling storage (AWS S3 and Azure Blob Storage) allow adversaries to serve data on your websites. They claim ownership of unique identifiers on cloud storage platforms that existing links still use, but are no longer owned.
- **Dangling name servers** (NS) – also known as broken NS delegations, dangling name servers may allow an adversary to take control of the delegated domain and then create records for hosts within the domain, including creating valid TLS certificates. Dangling name server records are a significant security risk and should either be removed or re-pointed at a name server the organisation controls and has configured to manage that domain.
- **Domain loading loops** – DNS records can redirect a visitor to a different domain. If these redirects loop back on itself, the domain will be in a broken state.
- **Incorrect record use** – MX, NS, or CNAME records should point to another domain name. If an IP address is placed in the record this will cause unexpected behaviour.
- **Private addresses** – DNS records which resolve to private, non-internet routable IP address space provide adversaries with an opportunity to understand internal networks, and can

also indicate to operators of split-zone DNS (where internal and external networks are served different results) that internal results may be leaking externally.

- **CNAME misuse** – CNAME records allow domains to redirect to another domain. Issues can occur where these redirect chains are too long, there are branching pathways, or CNAME records are used on top-level domains.
- **Statement of Authority (SOA) error** – SOA records stores important information about a domain or zone. Checks are made to validate the SOA record, and that exactly one is present where expected.
- **DNSSEC** – DNSSEC is a protocol designed to improve the overall security of DNS requests and replies using cryptography. Although adoption has been slow in Australia, .gov.au domains have, for some time now, been able to make use of DNSSEC to reduce the opportunity for adversaries to interfere with or manipulate DNS replies.

Organisations may wish to consider the use of split-horizon DNS, or other configurations, if they need to resolve public domain names to non-routable addresses.

Additional advice for domain owners

Additional advice DNS server operators

HOT CHIPs

HOT (High-priority Operational Tasking) CHIPs notifications are targeted information sent to customers we believe may be affected or impacted by critical vulnerabilities.

HOT CHIPs typically focuses on the latest and most concerning vulnerabilities, such as 0-days. These notifications prioritise timeliness and are sent as the vulnerabilities are discovered and/or released. This means that notifications will not always distinguish between systems that are still vulnerable, and systems which have already been patched.

Open source aggregates such as Shodan are used to detect at-risk assets and notify organisations as soon as possible. Where necessary custom scans are also conducted against systems suspected to be affected.

While responses to HOT CHIPs notifications are appreciated, they are not expected.

A full list of all the HOT CHIPS reports sent to your organisation in the previous quarter is shown in the HOT CHIPs CSV, with summarised information presented in the reports.

Third-party data breaches

Third-party data breaches refers to situations where a third-party's system is compromised by cyber criminals, and information from that system is either traded privately by cyber criminals or publicly disclosed. Depending on the information disclosed this can have adverse impacts on the confidentiality of organisations' and users' information.

Third-party data breaches can also lead to specific cyber security risks to other systems and the potential to allow malicious parties to leverage, blackmail and/or coerce users.

In partnership with Have I Been Pwned CHIPs provides government domain owners with visibility of information in data breaches.

As these breaches occur with third-party systems there is limited steps domain owners can take. ASD's publication, 'Minimising the impact of third party data breaches' provides guidance. Contact the CHIPs team if you require a copy.

Domain visibility

The domain visibility report provides organisations with an understanding of their internet-facing domain and hostname footprint. Separate tables are provided for domains and hostnames. Subdomains are included within the hostname count.

The report is non-exhaustive and relies on CHIPs domain enumeration capabilities or information you provided to us. More details on the domain enumeration process are noted in the Methodology section.

Note: CHIPs sometimes refers to domains and hostnames as domains even though the terms have slightly different meanings.

The reason for publishing domains on the internet can vary. Domains may be published to:

- Support public interactions (websites and email servers);
- Enable internal and background communications processes (server to server, corporate VPNs, etc); or
- Meet accepted network hygiene practices (e.g. publishing A records to align with reverse lookup names for public routable IP address space assigned to an organisation).

ASD recommends organisations:

- Be aware of all the domains and hostnames they publish, and the reasons for publishing them.
- Ensure they complete any cyber hygiene required for domains and hostnames.
- Regularly review publicly published domains and hostnames and remove any which are no longer required.
- Investigate the use of any publicly published domains and hostnames where the business reason is not known.

- Review the security of associated systems (those pointed to by the domain records) where those systems are not visible to the organisation's monitoring systems.

IP Visibility

The IP visibility report provides organisations with an understanding of their IPv4 address space. The report is non-exhaustive and relies on the CHIPs IP address discovery capabilities and organisation self-reporting. More details on the IP address discovery process are noted in the Methodology section.

ASD recommends organisations:

- Be aware of their public-facing IP address space.
- Complete any cyber hygiene required for IP address space, such as maintaining appropriate DNS reverse lookup zones.
- Ensure they are aware of all internet-facing systems that are deployed on their address space.
- Take measures to protect the integrity of their IP address space, such as using RPKI (Resource Public Key Infrastructure) to protect BGP route announcements.

20. Appendix - Methodology

CHIPs data, assessment and presentation principles

CHIPs is committed to providing accurate information in a format that provides insight and facilitates comparison of performance over time. However, as CHIPs evolves the way data is measured and presented will change.

The most accurate information available at the time

New techniques for measuring hygiene will become available as development of CHIPs continues. CHIPs may expand measurement capability in existing areas. This may lead to a change in previous assessment. For example, CHIPs may implement new capability to measure edge cases that could not previously be measured. Systems owners may find their assessment is affected positively or negatively by such changes.

Assessment against contemporary standards

As cyber standards evolve and change, so will the policy that CHIPs uses to perform assessments. When CHIPs needs to make changes in assessment policy to maintain alignment with the ISM, these changes will be notified in the prior report.

Before and after comparisons

When CHIPs gives before and after comparisons:

- The same assessment policy will be used against the before and after data sets. Where this is not possible, such as a new measurement capability (see above), CHIPs will note that data sets have not had a consistent assessment policy applied.
- The "before" value may be corrected to account for:
  - Data errors identified in the previous report.
  - Domains or hostnames that have been deleted and/or re-attributed to other organisations.

Collapsing indicators when appropriate

To maintain the brevity of reports, CHIPs may roll up data points that relate to similar topics. These changes will be notified in the prior report.

How data is presented

Within the main CHIPs report, data presentation is designed to provide key insight to executive officers, emphasising issues and areas that require investigation. As the cyber threat landscape changes, the areas emphasised may also change. CHIPs may also change how information is presented if a more effective means to provide insight is identified.

Critical Vulnerabilities

CHIPs uses a custom vulnerability scanner to detect critical vulnerabilities. Scan targets are identified through domain enumeration, IP address enumeration and open source port discovery.

The Critical Vulnerabilities metric reports the total number of systems identified as having a critical vulnerability.

The larger graph at the top is an 'Aged Issues' report that shows the reporting period during which vulnerabilities were first identified. When CHIPs detects that a vulnerability has been remediated it is removed from the graph.

For comparison purposes, an average of all similar organisations is shown, scaled relative to the number of hosts present in the organisation.

The smaller table at the bottom is the 'Changes' report and summarises vulnerabilities resolved, and new vulnerabilities detected, since the previous report.

Critical Vulnerabilities legend

Colours

Organisation	The graph shown in this colour shows the count of systems with detected critical vulnerabilities on organisation' systems for the relevant reporting period.
Organisation Comparison	The graph shown in this colour shows the average count of systems with critical vulnerabilities across similar government/critical infrastructure organisations and then scaled to the number of domains in your organisation.

Reporting periods

Current	The numbers in this section represent the total outstanding critical vulnerabilities that **have not** been patched or mitigated.
New	The numbers in this section represent critical vulnerabilities first identified during the most recent scan of CHIPs (as per the report date).
3 Months	The numbers in this section represent critical vulnerabilities identified in the last scan of CHIPs that **have not** been patched or mitigated.
6+ Months	The numbers in this section represent critical vulnerabilities identified **six months or more** in the past that **have not** been patched or mitigated.

Classification

Systems are classified as Vulnerable or Potentially Vulnerable.

Note - the CHIPs scanner's assessment of all systems identified as Vulnerable or Potentially Vulnerable, is found in the relevant CSV file. Only 'Vulnerable' systems are reported in this document.

Unlikely Vulnerable	CHIPs has detected software which is unlikely to be vulnerable but existing CVEs exist in older versions.
Potentially Vulnerable	CHIPs has detected software which is potentially vulnerable but is unable to determine it is vulnerable without attempting to compromise the system.
Vulnerable	CHIPs has detected software which almost certainly has a critical vulnerability.
Unknown	CHIPs has detected software which has significant existing vulnerabilities, but we cannot determine accurately whether vulnerable or not.

Service Visibility

Service Visibility data is obtained by comparing information from the CHIPs domain and IP address database against open port and service data from open source aggregators.

Open services (also known as ports) are assessed according to the Service Visibility assessment legend.

Service Visibility assessment legend

Green	Services that are typically exposed to the internet, and are necessary for communications over the internet. This includes services such as Domain Name Service (DNS), HTTP (Hyper Text Transfer Protocol), Email (Simple Mail Transfer Protocol) and others.
Orange	Services that may present an elevated risk when exposed to the internet. Services may be included in this list for reasons including not typically being able to support multi-factor authentication, being opened on a non-standard port or being services that rarely need to be exposed to the broader internet. Services that CHIPs has not yet categorised are also included in this list to bring them to the organisation's attention.
Red	Services that, under most circumstances, should not be exposed to the internet. This includes services such as databases, administrative and system configuration interfaces, deprecated and insecure protocols etc.

Service Visibility metrics are complicated by the relationship between hosts and services. A single host (or domain) can have many services open.

The first page of the Service Visibility assessment shows information related to service visibility on a per-host basis. This data provides business owners with a sense of how many of their internet-facing hosts are exposing risky services to the internet.

Each host is assessed at the level of the lowest scoring open service detected on that host. For example, if a host offers two green and one orange services to the internet, the overall assessment for the host is orange.

The first figure on the first page ('Hosts with service visibility issues over recent quarters') shows the total number of orange and red hosts (based on the methodology above) in the current and two previous reporting periods. This graphic allows owners to track the number of hosts that are exposing potentially dangerous services to the internet over time.

The two changes tables at the bottom of the first page of service visibility track improvements in host scores.

For a host to be remediated all service visibility issues on that host need to be remediated.

For example, if a host offers one green and two orange services, and one orange service is filtered from the internet the host will still be rated as orange. When the second orange port is closed the host will be rated green, will be shown as "Resolved/Mitigated" in the orange issues change table and will also no longer appear in the 'Hosts with Service Visibility issues over recent quarters' graphic.

If a host offers a red, green and orange service, and the red service is closed, it will transition to an orange host. This would appear as Resolved/Mitigated in the red changes table, but show up as a new orange issue in the changes table, and also move from red to orange in the 'Hosts with Service Visibility issues over recent quarters' graphic.

Page 2 of Service Visibility provides a breakdown on a per service basis into six broad subtypes.

This data provides business owners with a sense of the types of potentially risky services that are being exposed to the internet.

Hosts can have many services open, so there may be little correlation between the numbers on the first page and second page of the Service Visibility section.

The Service Visibility CSV file contains data on all open services on all hosts in the organisation, including hosts without domains reachable by IP addresses. The CSV dataset is much more detailed and should be used by technical staff to identify and remediate issues.

Administration Consoles

CHIPs scans for management, configuration and administration consoles. These include exposed consoles and login pages to those consoles exposed to the internet. Scan targets are identified through domain enumeration, IP address enumeration and open source port discovery.

The admin consoles metric reports the total number of systems identified as having a management, configuration and/or administration console.

The larger graph at the top is an 'Aged Issues' report that shows the reporting period during which consoles were first identified. When CHIPs detects that the issue has been remediated it is removed from the report.

For comparison purposes, an average of all similar organisations is shown, scaled relative to the number of hosts present in your organisation.

The smaller table at the bottom is the 'Changes' report and summarises vulnerabilities resolved, and new vulnerabilities detected, since the previous report.

Administration Consoles assessment legend

Colours

Organisation	The graph shown in this colour shows the count of systems with detected admin consoles on organisation systems for the relevant reporting period.
Similar Organisations Scaled Average	The graph shown in this colour shows the average count of systems with admin consoles across similar organisations and then scaled to the number of domains in your organisation.

Reporting periods

Current	The numbers in this section represent the total outstanding admin consoles that are currently detectable.
New	The numbers in this section represent admin consoles first identified during the most recent scan of CHIPs (as per the report date).
3 Months	The numbers in this section represent admin consoles identified in the last scan of CHIPs that are still detectable.
6+ Months	The numbers in this section represent admin consoles identified **six months or more** in the past that are still detectable.

Classification

Detected systems are classified as Administration Console Found.

Administration Console Found	CHIPs has detected software which almost certainly has an administration console running.

Multi-Factor Authentication

This metric reports on instances where services that are commonly used for internal access, such as Virtual Desktop Infrastructure (VDI), Virtual Private Networks (VPN) and corporate email interfaces do not appear to be offering multi-factor authentication (MFA).

Each domain, hostname, and IP is scanned on common ports and paths for the associated service. If the service is found, CHIPs fingerprinting techniques are utilised alongside analysis of common MFA paths for that service to determine whether a known form of MFA is implemented.

Multi-Factor Authentication risk assessment legend

Colours

Organisation	The graph shown in this colour shows the count of systems with detected admin consoles on organisation systems for the relevant reporting period.
Similar Organisations Scaled Average	The graph shown in this colour shows the average count of systems without MFA across similar organisations and then scaled to the number of domains in your organisation.

Reporting periods

Current	The numbers in this section represent the total outstanding admin consoles that are currently detectable.
New	The numbers in this section represent products identified without MFA during the most recent scan of CHIPs (as per the report date).
3 Months	The numbers in this section products identified without MFA in the last scan of CHIPs that are still detectable.
6+ Months	The numbers in this section products identified without MFA **six months or more** in the past that are still detectable.

Classification

Detected systems are classified as MFA Enabled, Potentially No MFA, or No MFA.

MFA Enabled	Service login page identified and scanner detects multi-factor authentication enabled or no service of interest was located by the scanner.
Potentially No MFA	Service login page identified and the scanner was unable to determine whether the page utilised multi-factor authentication or whether it met the requirements for multi-factor authentication. E.g. Utilising a "Second Password" field, is unclear if it meets the requirements of MFA. Refer to: Implementing-MFA for more details.
No MFA	Service login page identified and the scanner was unable to detect any multi-factor authentication on the login page.

Note on false negatives: There is always a possibility that some multi-factor authentication may be missed. This can be due to the difficulty in fingerprinting some multi-step MFA and the limited MFA types/providers we are scanning for. Please notify the CHIPs team if you identify false negatives so we can modify our methodologies for future reports.

Dormant Websites

This metric reports the total number of websites identified as being dormant. Endpoints are identified through domain enumeration and IP address enumeration. Open source intelligence aggregators are used to identify HTTP/HTTPS services running on non-standard ports (See Port Discovery below). Live endpoints are scanned on a list of standard ports and non-standard ports.

The large graph at the top is as an 'Aged Issues' report that shows the reporting period during which issues were first identified. When CHIPs detects that an issue has been remediated it is removed from the report.

The smaller table at the bottom is the 'Changes' report and summarises issues resolved, and new issues detected, since the previous report.

Dormant websites also identifies the number of websites that are detected as potentially having issues. These issues are only reported in the CSV file.

Dormant Websites assessment legend

Colours

Organisation	The graph shown in this colour shows the count of systems classified as Dormant on organsations' systems for the relevant reporting period.

Similar Organisations Scaled Average	The graph shown in this colour shows the average count of systems classified as Dormant across similar organisations and then scaled to the number of domains in your organisation.

Reporting periods

Current	The numbers in this section represent the total outstanding dormant websites that **have not** been made active again.
New	The numbers in this section represent dormant websites first identified during the most recent scan of CHIPs (as per the report date).
3 Months	The numbers in this section represent dormant websites identified in the last scan of CHIPs that **have not** been made active again.
6+ Months	The numbers in this section represent dormant websites identified **six months or more** in the past, that **have not** been made active again.

Classification

Websites are classified as Dormant, Potentially Dormant or Active according to the following criteria.

Note - the CHIPs scanner's assessment of all websites, Dormant, Potentially Dormant or Active, is found in the relevant CSV file. Only 'Dormant' websites are reported in this document.

No detected issues	According to existing indicators the website appears to be current and up to date.
Potential issues detected	The website content hasn't been updated for more than 4 years OR the server is running software which may be out of date OR the server does not offer a valid certificate for TLS OR does not support at least TLS1.2.
Dormant website	The website is running out of support software OR is running a default configuration page OR responds to requests with a server side error code (5xx series, excluding a 502 or 503 response) OR returns an invalid response code to an HTTP or HTTPS request.

Email Security

This metric reports the ratio of domains and hostnames covered by valid SPF/DMARC records to the total number of domains and hostnames attributed to an organisation.

Email Security assessment legend

Explicit Protection	The domain/hostname has a valid DMARC record, or has a valid DMARC record on its base domain, with an effective policy of 'reject' or 'quarantine' AND the domain/hostname is explicitly protected with a 'hard fail' SPF record.
Implicit Protection	The domain/hostname has a valid DMARC record, or has a valid DMARC record on its base domain, with an effective policy of 'reject' or 'quarantine'.
Configuration Error	There is some error in configuration of the DMARC and/or SPF record such that the record is not RFC compliant.
No Effective Protection	The domain/hostname is not protected with a DMARC or SPF record OR the DMARC record is set to a policy of 'none' OR the SPF record is not set to 'hard fail'.

Website Encryption

Websites are included in this metric if a response is received on port 80 or 443 when the assessment takes place.

The criteria for categorising websites are based on the current requirements for TLS and HTTPS in the ASD's Information Security Manual (ISM).

Please note where your hostnames point at third-party hosted services, you will receive a score based on our assessment of that service. Third-party services form part of your attack surface, but it is your decision which risks are acceptable. For example autodiscover Microsoft hostnames are often used, and score red in this metric.

Websites are scored for HTTPS and TLS according to the following criteria:

Website Encryption assessment legend

Strong HTTPS and HSTS preloaded	Strong HTTPS (as below) AND the domain has been submitted to the HSTS Preload list (hstspreload.org) and the HSTS configuration is preloaded into the browser.
Strong HTTPS Configuration and HSTS used	The website sends a HSTS header when accessed AND HTTPS is enabled AND no weak or insecure cipher suites are used AND users are redirected to an HTTPS connection AND the oldest supported version of TLS is 1.2 or higher AND client-initiated TLS renegotiation is disabled.
Weak HTTPS Configuration and HSTS used	The website sends a HSTS header when accessed, but HTTPS is neither configured securely enough for an overall green score, or poorly enough for an overall red score (For example, TLS 1.2 with weak ciphers) OR client-initiated TLS renegotiation is supported.
No HTTPS, No HSTS or	The website does not send a HSTS header when accessed OR HTTPS is not enabled OR insecure ciphers suites are used OR users are not strictly redirected to a HTTPS

Insecure Configuration	connection OR the oldest supported version of TLS is 1.1 or lower OR compression is not disabled OR the names on the certificate (CN or SAN) do not match the hostname requested (servers scanned on IP only are excluded).

Email encryption

This metric reports the ratio of mail-enabled domain/hostname (where an MX record points to an email servers) and assesses them according to the following table. Where a domain/hostname has multiple associated mail servers the lowest assessed score of those mail servers is used.

Opportunistic TLS assessment legend

Secure Opportunistic TLS and MTA-STS	The domain/hostname's email server(s) support Opportunistic TLS at a Green level (as below) and a valid MTA-STS policy enforcing encryption is published.
Secure Opportunistic TLS	The mail server supports Opportunistic TLS (STARTTLS) AND supports at least TLS 1.2 (but may also allow TLS 1.1 and TLS 1.0 for backwards compatibility) AND has a valid certificate AND offers at least one strong cipher AND offers no insecure ciphers.
Weak Opportunistic TLS	Not blue, green or red. For example, TLS 1.2 with insecure ciphers, or TLS 1.1, or supports client initiated re-negotiation.
No or insecure Opportunistic TLS	The mail server does not support Opportunistic TLS (STARTTLS) OR supports any version of SSL OR supports TLS compression

API Detection

CHIPs uses a custom API detection scanner to detect exposed APIs. Scan targets are identified through domain enumeration, IP address enumeration, open source port discovery, open source web crawl datasets such as Common Crawl, and robots.txt files. Information of common API deployment patterns is also used to create scan targets.

The API detection summary metric reports the total number of API endpoints detected.

CHIPs is not suggesting these APIs have vulnerabilities or should be disabled. Please consider each in context and requirements. We encourage minimising attack surface where possible.

API detection legend

Green	Not an API endpoint

Grey	Potential API endpoint

Route Security

This metric measures if there are valid ROA certificates for IPv4 addresses attributed to your organisation. Route Security checks both IP addressed pointed to by your hostnames/domains, and assigned IP addresses.

CHIPs checks ROA configuration by determining if the IP address's prefix (the network part of the internet address) is contained within a valid ROA. If an ROA is present, CHIPs attempts to determine if any unauthorised ASNs are announcing the prefix.

Each hostname or IP address associated with the organisation is individually counted and presented as a data point the chart.

Route Security assessment legend

Valid	The IP address prefix is contained in a valid ROA and assigned to an ASN and is not invalid for any other reason.
Invalid	The ROA record is invalid (bad signature/expired certificate etc), or there is no matching ASN for the prefix, the prefix announcement is more specific than the matching valid ROA allows or there is evidence that an unauthorised ASN is announcing the prefix.
Not found	There are no ROA containing the prefix.

DNS Hygiene

This metric reports the number of domains and hostnames affected by each of the particular types of DNS Hygiene issues. The methodology used to assess each different issue is below.

Note: CHIPs sometimes refers to hostnames and domains as "domains" although they are slightly different things. In most cases the distinction is not meaningful. However, as DNS specific issues are reported the distinction becomes important, and so in this section you will see reference to domains and hostnames as separate things.

Issue Methodology

Dangling hostnames	A dangling hostname exists if the query for a hostname returns a CNAME record which points to an A record at specific service providers and the corresponding A record does not exist. **Note:** This list of service providers is currently: Azure, AWS Apps and Elastic Bean Stalk. This list will be extended as particular service providers are confirmed as being vulnerable to dangling hostnames. Dangling

	storage exists if the query for a hostname returns a CNAME record which points to an AWS S3 or Azure Blob Storage platform, and a not found error code is returned.
Dangling name servers	A dangling name server exists where a query for a hostname returns an NS record (indicating the hostname is actually a subdomain), but the NS servers nominated do not resolve the domain delegated to them. This metric only ever applies to domains.
Loading loops	Loading loops exist where a query to the hostname or domain returns a CNAME record, that leads to another CNAME that either then, or through a chain, loops back on itself.
Incorrect record use	MX, NS, and CNAME records should return another domain or hostname when queried. Then an A record query is made to the new domain/hostname for the resolved address. MX, NS, or CNAME records should never contain an IP address directly.
Private addresses	A private address exists where an A record exists and responds with a non-internet routable IP address (as defined in RFC1918) including a loopback address (127.0.0.0/8). To prevent spurious, low value and harmless results hostnames with the prefix of localhost are excluded.
CNAME misuse	CNAME records can redirect multiple times in a 'chain'. If these chains become too long it makes initial resolution of the domain/hostname take longer. If there are multiple CNAME records, a resolver can only follow one. A CNAME cannot be placed at the root domain level, because the root domain is the DNS Start of Authority (SOA) which must point to an IP address.
Statement of Authority errors	SOA records should be present on root domains to contain information about the DNS zone. You can have SOA records on child zones but there still must be a parent zone with exactly one SOA record.
DNSSEC	Any domains, as identified through name server delegation are queried for DNSSEC information which is assessed in accordance with the RFC. The DNSSEC configuration of domains can be: • "DNSSEC implemented - zone apex is signed and validated and chain of trust is valid" – indicating the domain and delegated name server(s) has a validated DNSSEC configuration and is signed by the parent zone through a DS record. • "DNSSEC partially implemented - zone apex is signed and validated but chain of trust is not valid " – indicating the domain and delegated name server(s) has a validated DNSSEC configuration but is not signed by the parent zone through a DS record. • "DNSSEC partially implemented - zone apex is not signed or validated but chain of trust is valid" – indicating the domain and delegated name server(s)

	does not have a valid DNSSEC configuration but is signed by the parent zone through a DS record. • "DNSSEC not implemented for the zone apex" – indicating the domain and delegated name server(s) has no DNSSEC configuration that CHIPs could detect.

Third-party data breaches

CHIPs relies on data provided by Have I Been Pwned (HIBP) for notification of third party data breaches. HIBP provides CHIPs with notifications when it detects **government** email addresses appearing in breach data.

Have I Been Pwned data is parsed and broken down by data-breach and provided to organisations through the CHIPs report. The number of email accounts exposed in each data breach is summarised in this report. The exact exposed email account and related data breach is detailed in the CSV.

Where the breach source is noted as 'sensitive' ASD will withhold the usernames/email address due to the potential sensitivity of the breach. If the organisation's cyber security staff need more details on the breach to manage risk they should contact the CHIPs team (asd.chips@defence.gov.au).

Changes in open issues since last quarter

This box summarises the change in the status of open issues since last quarter for each hygiene indicator.

The data points are as follows:

Issues date	Shows issues open at that date according to CHIPs.
New (existing hosts)	Issues detected on hosts, where CHIPs already knew about the host prior to the latest scan. These may be new issues (such as a new critical vulnerability), or an issue that CHIPs could not previously detect (such as upgraded scanner capability), or a change in the system state (the system did not previously have a hygiene issue, but it does now).
New	Issues detected on hosts where those hosts were unknown to CHIPs prior to this quarter.
Resolved/ Mitigated	Hosts where issues have been mitigated, but the host/service is still live.
Removed	

	Issues where the host did not respond to the scanner, and thus the issue is no longer present. The host or service may have been decomissioned, but these can also be temporary effects that may return.
Others	(If present) - an adjustment to make issues at start and end of period align. Others represent edge cases in counting that CHIPs has not entirely allowed for. In general these are small relative to overall numbers.

Box plots

Box plots (also known as 'box and whisker' plots) are provided to allow organisations to compare their performance to peers.

A box plot provides five statistical data points:

1. Lowest value (the left hand end of the left whisker).
2. 25% percentile (the left hand end of the box).
3. Median (the orange line).
4. 75% percentile (the right hand end of the box).
5. Maximum value (the right hand end of the right whisker).

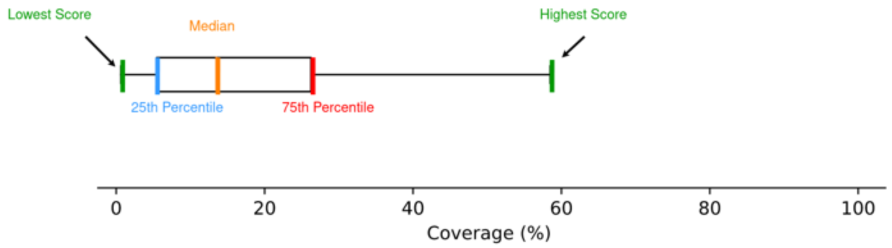


Figure 20.1 Box plot interpretation

Four separate plots are provided with data from small, medium, large and all organisations. The 'all' category includes organisations listed in other classes as well as organisations for which no size data is known.

These four separate plots allow organisations to compare themselves against the group of peers they feel is most representative to their size.

Organisations that have 0% coverage are excluded from the plot.

Your organisation's performance is shown as a red line drawn across all plots allowing comparison to all sized organisations.

CSV Files

CHIPs provides additional information in "comma separated value" (CSV) files attached to this report.

These CSV files provide the details required for technical staff to understand the specific issues and weaknesses being identified.

Each hygiene metric has an associated CSV file.

Each CSV file contains a legend at the top which explains the columns contained in the file.

CHIPs does change the columns in these files from time to time as new information and capabilities are added. These changes are described in the csv_changelog.txt file.

Domain liveness check

CHIPs regularly checks domains and hostnames to ensure they continue to resolve. They are considered active if they answer a DNS query.

Domains or hostnames that resolve to non-public IP address space (as per IETF RFC5735), including networks such as private IP address space, and the loopback address are identified in the domain visibility CSV for visibility, but will not be scanned.

Domain attribution

Linkage between domains and organisations is primarily based on WHOIS registrant information and information provided to us. Various other uses support our techniques.

CHIPs asks organisations to continue to advise of any incorrectly attributed domains or hostnames.

IP enumeration

CHIPs sources IP addresses by:

- Reconciling forward lookups against known netblocks and ASN information.
- Through organisations reporting their own address spaces.
- Through open source network information aggregators.

A complete listing of all IPs is in the attached IP Visibility CSV file.

IP visibility

The IP visibility report shows the number of IP addresses attributed against the organisation at the date of scanning.

Live IPv4 addresses is established through an open source aggregator.

IP attribution

Linkage between IP addresses is via ASN, other discovery techniques and self reporting. Manual correction is used when incorrect attribution is identified.

Any inaccuracies notified to the ASD at least ten business days before the scan have been corrected in the data presented here. Changes advised within ten business days of the scan will be reflected in the next report cycle.

ASD asks organisations to continue to advise of any incorrectly attributed IP addresses or ranges.

Port, server and service enumeration

CHIPs predominantly uses open source intelligence aggregators, such as Shodan and Censys, to identify live servers, open services and ports of endpoint associated IP addresses. CHIPs may also conduct direct port scanning depending on circumstances.

How to detect CHIPs scanning

The following methods are implemented by CHIPs to enable analyst teams to identify our scanning. Please be aware, these methods can be copied by any actor.

- HTTP requests are accompanied by a header. X-ACSC-Scan: "CHIPs scan (contact asd.assist@defence.gov.au for further information)".
- STARTTLS and generic TCP connections are opened with the byte string "CHIPs".
- Reverse IP lookups (PTR records) will resolve to "p<1-8>.chips.cyber.gov.au" during the scan.
- Remember you should verify reverse lookups by checking the forward lookup of the domain name. Make sure it points to the same IP address. The IP network owner sets the reverse lookup, the domain owners sets the forward lookup.

We rotate IP addresses and request user-agents. These will not reliably identify a CHIPs scan.

Authority

CHIPs scans are conducted at the direction of the Australian Government and ASD is authorised to perform them under Australian Law, specifically Section 7 of the Intelligence Services Act 2001.

Any customers with questions or concerns about CHIPs' authority and activities should contact ASD at asd.assist@defence.gov.au.

21. Further Information

The Australian Government Information Security Manual (ISM) assists organisations in using their risk management framework to protect their information and systems from cyber threats.

ASD provides further guidance on:

- SPF, DKIM and DMARC in How to Combat Fake Emails.
- TLS, HTTPS and HSTS in Implementing Certificates, TLS, HTTPS and Opportunistic TLS.

For additional assistance contact CHIPs at:

Cyber Hygiene Improvent Programs
Cyber Uplift Branch, Cyber Security Resilience Division
Australian Signals Directorate
☎: +61 2 62 430 435 : asd.chips@defence.gov.au

22. Traffic Light Protocol

The following table lists the classification levels used in the traffic light protocol (TLP) and describes the restrictions on access and use for each classification level.

TLP classification	Restrictions on access and use
TLP:RED	**Access to and use by your ASD security contact officer(s) only. You must ensure that your ASD security contact officer(s) does not disseminate or discuss the information with any other person, and you shall ensure that you have appropriate systems in place to ensure that the information cannot be accessed or used by any person other than your ASD security contact officer(s).**
TLP:AMBER+STRICT	Restricted for internal access and use only. You shall only make TLP:AMBER+STRICT publications available to your employees on a 'need to know basis'. In some instances, you may be provided with TLP:AMBER+STRICT publications which are marked to allow you to also disclose them to your contractors or agents on a need-to-know basis—strictly for internal purposes and only to assist in the protection of your ICT systems.
TLP:AMBER	Restricted internal and external use only. You shall only make AMBER publications available to your employees, contractors, Managed Service Providers (MSPs), or to your clients on a 'need to know basis'. You may disclose TLP:AMBER publications to your contractors or agents strictly for internal purposes and only to assist in the protection of your ICT systems.
TLP:GREEN	Restricted to closed groups and subject to confidentiality. You may share GREEN publications with external organisations, information exchanges, or individuals in the network security, information assurance or critical infrastructure community that agree to maintain the confidentiality of the information in the publication. You may not publish or post on the web or otherwise release it in circumstances where confidentiality may not be maintained.
TLP:CLEAR	Not restricted. CLEAR publications are not confidential. They contain information that is for public, unrestricted dissemination, publication, web-posting or broadcast. You may publish the information, subject to copyright and any restrictions or rights noted in the information.