Minutes

Audit and Risk Committee Meeting to be held at 9.00 AM on Wednesday 27 April 2022 in the Bennett Room, Pleasant Creek Historic Precinct.

1 Present

Mr Peter Knights (Chair)
Mr Tony Roberts (via phone)
Ms Lynn Jensz
Cr Murray Emerson
Cr Kevin Erwin (left meeting 10.30am)

Ms Liana Thompson, Chief Executive Officer
Mr Vaughan Williams, Director Corporate and Community Services
Mr Graham Haylock, Manager Financial Services
Ms Stretch Smith, Manager Business Transformation
Mr Phil Delahunty, RSD Audit (via phone)
Ms Blessing Mendoza, RSD Audit (via phone)

2 Apologies

No apologies were received

3 Disclosures of a Conflict of Interest at a Council Auspiced Meeting

Nil

4 Confirmation of Minutes from the Previous Meeting

Confirmation of draft minutes from the Northern Grampians Shire Council Audit and Risk Committee meeting held, Wednesday, 2 February 2022.

Moved: Cr Murray Emerson
Seconded: Cr Kevin Erwin
Carried

5 Matters Arising from the Minutes

Nil

6 General Business

6.1 Audit and Risk Committee Reappointment - Ms Lynn Jensz

Discussion regarding the reappointment of Ms Lynn Jensz to the Audit and Risk Committee.

Outcome

The committee discussed the reappointment of Ms Lynn Jensz to the Audit and Risk Committee and recommended that Ms Jensz be reappointed to the Committee for a new three-year term.

Resolution

That Ms Lynn Jensz be reappointed to the Audit and Risk Committee for a three-year term ending 30 April 2025.

Moved: Mr Tony Roberts
Seconded: Cr Murray Emerson
Carried

6.2 Biannual Report

Audit Committee Chair to table the Biannual Report. **(Attachment)**

Outcome
Mr Peter Knights tabled the Biannual Report.

Resolution
That the Biannual Report be received and endorsed for tabling at the next Council Meeting.

Moved: Ms Lynn Jensz
Seconded: Mr Tony Roberts
Carried

6.3 Victorian Protective Data Security Standards (VPDSS)

Ms Stretch Smith to provide an update on the Victorian Protective Data Security Standards. **(Attachment)**

Outcome
Ms Stretch Smith provided an update on the VPDSS including the project plan and policies including the acceptable use policy, privacy policy, information security management framework and information security performance indicators.

Ms Smith also gave a presentation of cyber security and the associated challenges.

Resolution
That the Victorian Protective Data Security Standards update be received and noted.

Moved: Cr Murray Emerson
Seconded: Cr Kevin Erwin
Carried

7 Risk Management

7.1 Risk Committee Update

Mr Vaughan Williams to provide a Risk Committee Meeting update.

Outcome

Mr Williams provided an update from the last Risk Committee Meeting. Topics included: policies and procedures, risk management policy, and the review of operating risks to identify 3 items for review in the next 12 months (procurement, cyber security/penetration testing, and EPA legislation compliance).

Resolution

That the Risk Committee update be received and noted.

Moved: Ms Lynn Jensz
Seconded: Mr Tony Roberts
Carried

7.2 Risk Management Plan

Item deferred to next meeting.

8 Financial Reporting and VAGO Audit

8.1 Audit Strategy

Mr Phil Delahunty from RSD Audit to present the Audit Strategy for the 2021/22 financial year.

Outcome

Mr Phil Delahunty and Ms Blessing Mendoza from RSD Audit presented the Audit Strategy for the 2021/22 financial year. Items discussed included: notes regarding COVID-19 impact, the challenges for the audit following a reduction in the number of VAGO audit providers for the sector, valuation of infrastructure, property, plant and equipment. and the accounting treatment of grants.

Resolution

That the Audit Strategy update be received and noted.

Moved: Ms Lynn Jensz
Seconded: Mr Tony Roberts
Carried

8.2 Quarterly Finance Report

Mr Graham Haylock to present the Finance Report for the period ending 31 December 2021.

Outcome

Mr Haylock provided a summary of the key highlights from the Quarterly Finance Report.

Recommendation

That the Finance Report be received and noted.

Moved: Mr Tony Roberts
Seconded: Cr Murray Emerson
Carried

9 Next Meeting

Next Meeting is scheduled 22 June 2022.

10 Close

The meeting closed at 11.00am.

Northern Grampians Shire Council

AUDIT COMMITTEE BIANNUAL REPORT
for the 6 months to 31 December 2021

1. Attendance and Meetings

The Northern Grampians Shire Council Audit Committee has met twice this financial year to date by way of online teams meetings. Whilst adequate, at times this format is less than ideal for enabling fuller communication and discussion. This is obviously a direct result of the Covid restrictions and having attendees join the meeting online from time to time for either expediency and practicality, is now established as appropriate protocol, we will look forward to in person meetings where possible for, I would suggest, most of our meetings going forward.

2. Activity

The VAGO appointed external auditors RSD Chartered Accountants from Bendigo continued their engagement and completed the full year Audit Report and Final Management letter, reviewed in our first meeting in September. The lack of internal audit activity was flagged as a concern by RSD. From that reporting to our meeting a resolution was passed for management to prepare an external review into Councils' Risk Management Framework as a basis for developing the internal audit function.

Consultants Crowe prepared the review with nine recommendations for Council to use in finalising the RMF and integration of associated systems, which was presented at the February meeting.

The former Annual Audit Activity Calendar and Risk Register has been transitioned gradually to the digital system by the Council leadership team to enable a much improved and pertinent risk reporting function. We understand it is largely from this CAMMS system reporting the internal audit and strategic review functions will be managed including the input from this committee. Whilst this has taken longer than ideal, we would expect to see initiated action from this systems based approach this year, if compliance with the implied requirement to have a formal internal audit program cannot be met as yet by the CAMMS system then an interim arrangement should be made before balance date June 30.

The industry move to systems and reliance on digital data increasingly places this organisation into risk exposures from either malicious or inadvertent data breaches or failures. The noted need of an updated disaster management plan for ICT as noted in this quarter's audit plan from RSD, highlights to continued need for resources to this area, and gives us an ideal target for internal audit and strategic review for the current year with further items for the 2022 /2023 year's program to be determined on review of reporting from CAMMs and feedback from the Risk Committee.

We have received and reviewed interim Financial Statements at our February meeting and found them well presented and explained. Thank you to the Governance, Compliance and Finance team and to my fellow members of the committee for their contribution.

Peter Knights FCPA
Chair
Northern Grampians Shire Council Audit Committee

April 22nd. 2022

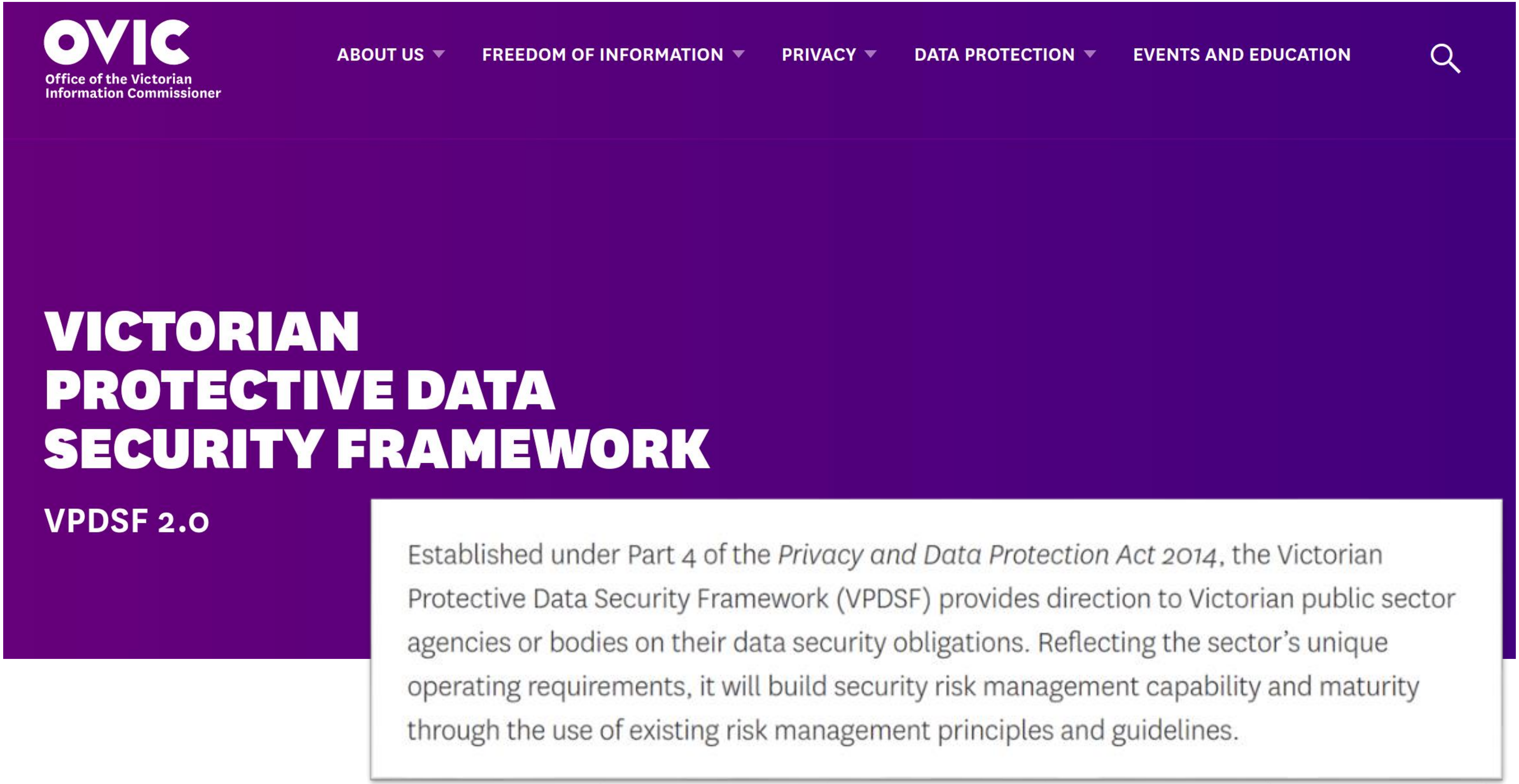
Office of the Victorian Information Commissioner

INFORMATION SECURITY

Victorian Protective Data Security Standards

Version V2.0

Implementation Guidance V2.1



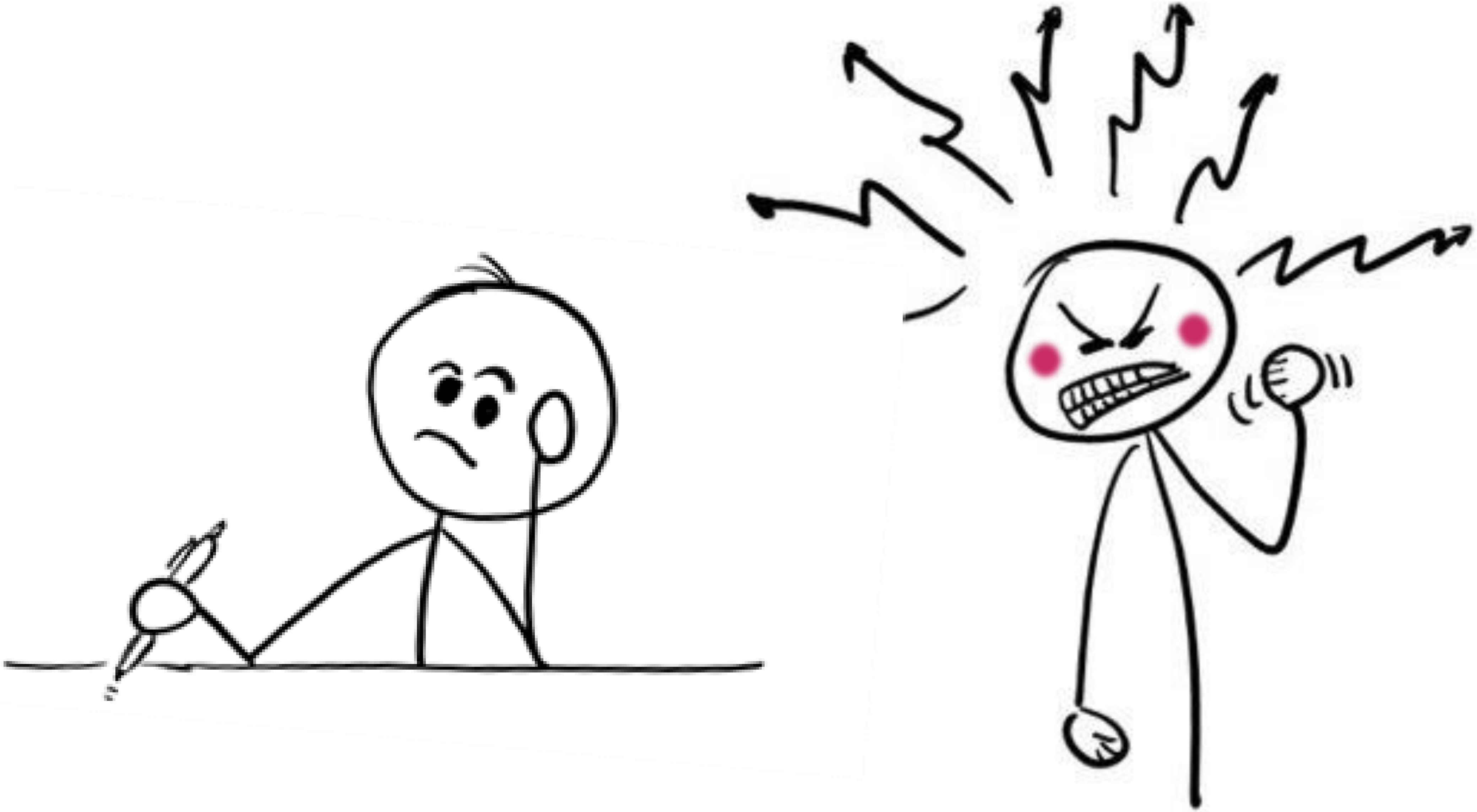
VICTORIAN PROTECTIVE DATA SECURITY FRAMEWORK

VPDSF 2.0

Established under Part 4 of the *Privacy and Data Protection Act 2014*, the Victorian Protective Data Security Framework (VPDSF) provides direction to Victorian public sector agencies or bodies on their data security obligations. Reflecting the sector's unique operating requirements, it will build security risk management capability and maturity through the use of existing risk management principles and guidelines.

VPDSF Objectives

- manage information throughout its lifecycle
- manage information across all the security areas
- manage security risks to information confidentiality, integrity, and availability
- manage external parties with access to information
- share information with other organisations with confidence
- minimise security incidents

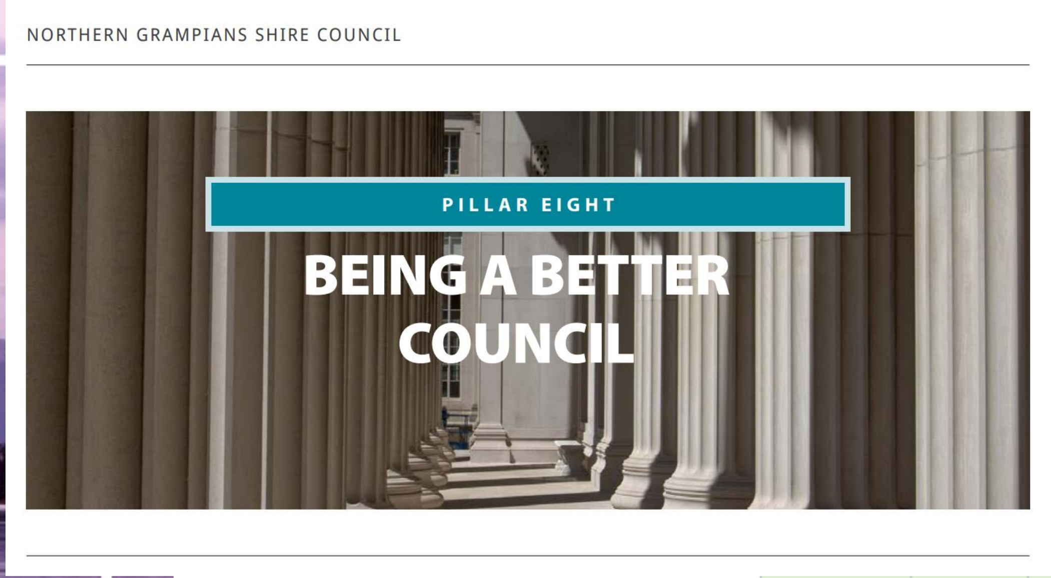


COUNCIL PLAN

2021-2025

NORTHERN Grampians SHIRE COUNCIL

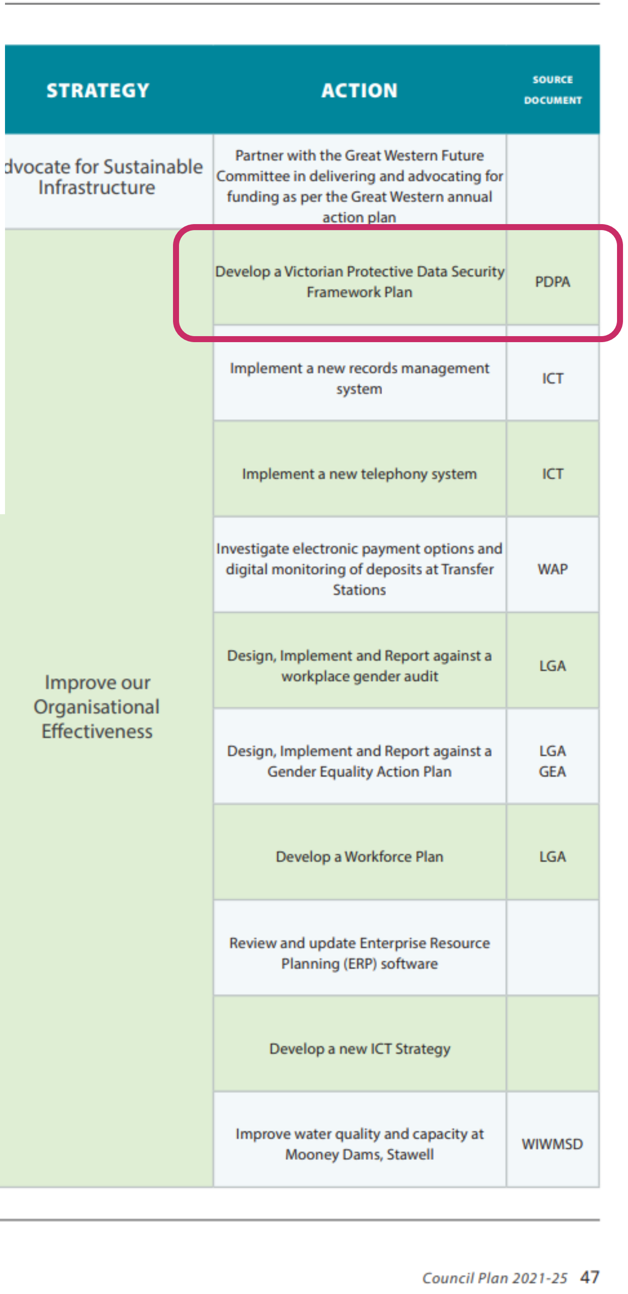
Our COMMUNITY together



NORTHERN GRAMPIANS SHIRE COUNCIL

PILLAR EIGHT

BEING A BETTER COUNCIL



		STRATEGY	ACTION	SOURCE DOCUMENT
		dvocate for Sustainable Infrastructure	Partner with the Great Western Future Committee in delivering and advocating for funding as per the Great Western annual action plan	
Improve Organisational Effectiveness	Being a Better Council	Improve our Organisational Effectiveness	Develop a Victorian Protective Data Security Framework Plan	PDPA
			Implement a new records management system	ICT
			Implement a new telephony system	ICT
			Investigate electronic payment options and digital monitoring of deposits at Transfer Stations	WAP
			Design, Implement and Report against a workplace gender audit	LGA
			Design, Implement and Report against a Gender Equality Action Plan	LGA GEA
			Develop a Workforce Plan	LGA
			Review and update Enterprise Resource Planning (ERP) software	
			Develop a new ICT Strategy	
			Improve water quality and capacity at Mooney Dams, Stawell	WIWMSD

Office of the Victorian Information Commissioner

INFORMATION SECURITY

Victorian Protective Data Security Standards

Version V2.0

Implementation Guidance V2.1

Freedom of Information | Privacy | Data Protection

- covering 5 areas
- 12 standards
- each standard has elements

The Standards cover five areas:

governance

- executive sponsorship of and investment in security management, utilising a risk-based approach, security policies and procedures, training, business continuity and disaster recovery, security incident management, external party engagement and oversight;

information security

- protection of information across the information life cycle from when it is created to when it is disposed or destroyed;

personnel security

- engagement and ongoing management to ensure the continued eligibility and suitability of people accessing public sector information;

ICT security

- secure communications and technology systems processing or storing information; and

physical security

- secure physical environment including facilities, equipment and services and the application of physical security measures to protect information.

No.	Standard
1	Information Security Management Framework
2	Information Security Value
3	Information Security Risk Management
4	Information Access
5	Information Security Obligations
6	Information Security Incident Management
7	Information Security Aspects of Business Continuity and Disaster Recovery
8	Third Party Arrangements
9	Information Security Reporting to OVIC
10	Personnel Security
11	Information Communications Technology (ICT) Security
12	Physical Security

Ref #	Element
E1.010	The organisation documents a contextualised information security management framework (e.g., strategy, policies, procedures) covering all security areas.
E1.020	The organisation's information security management framework contains and references all legislative and regulatory drivers.
E1.030	The organisation's information security management framework aligns with its risk management framework.
E1.040	Executive management defines information security functions, roles, responsibilities, competencies and authorities.
E1.050	Executive management nominates an information security lead and notifies OVIC of any changes to this point of contact.
E1.060	Executive management owns, endorses and sponsors the organisation's ongoing information security program(s) including the implementation plan.
E1.070	The organisation identifies information security performance indicators and monitors information security obligations against these.
E1.080	Executive management commits to providing sufficient resources to support the organisation's ongoing information security program(s).
E1.090	The organisation sufficiently communicates its information security management framework and ensures it is accessible.
E1.100	The organisation documents its internal control library that addresses its information security risks.
E1.110	The organisation monitors, reviews, validates and updates the information security management framework.

Office of the Victorian Information Commissioner

INFORMATION SECURITY

Victorian Protective Data Security Standards

Version V2.0

Implementation Guidance V2.1

Freedom of Information | Privacy | Data Protection

Annual attestation – CEO support

Biennial attestation on progress/plans vs each element:

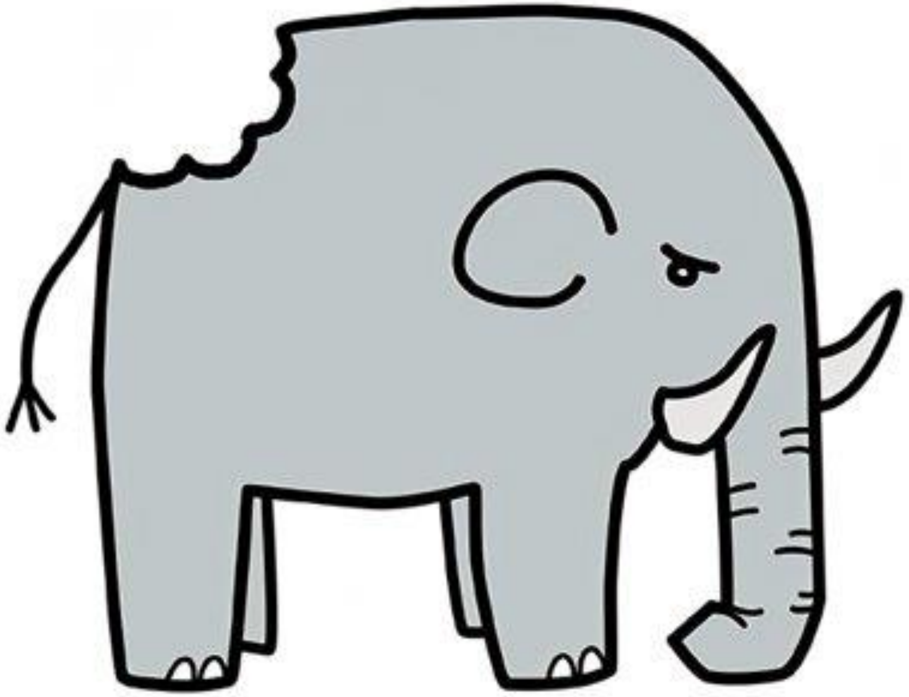
- what we've done
- what we're going to do
- when we're going to do it

> develop our annual plan

Ref #	Element
E1.010	The organisation documents a contextualised information security management framework (e.g., strategy, policies, procedures) covering all security areas.
E1.020	The organisation’s information security management framework contains and references all legislative and regulatory drivers.
E1.030	The organisation’s information security management framework aligns with its risk management framework.
E1.040	Executive management defines information security functions, roles, responsibilities, competencies and authorities.
E1.050	Executive management nominates an information security lead and notifies OVIC of any changes to this point of contact.
E1.060	Executive management owns, endorses and sponsors the organisation’s ongoing information security program(s) including the implementation plan. ✓ ✘
E1.070	The organisation identifies information security performance indicators and monitors information security obligations against these.
E1.080	Executive management commits to providing sufficient resources to support the organisation’s ongoing information security program(s).
E1.090	The organisation sufficiently communicates its information security management framework and ensures it is accessible.
E1.100	The organisation documents its internal control library that addresses its information security risks.
E1.110	The organisation monitors, reviews, validates and updates the information security management framework.

HOW DO YOU EAT AN ELEPHANT?

ONE BITE AT A TIME!



Task		Due Date
Review ICT Acceptable Use Policy	✓	31/12/2021
Review Privacy Policy	✓	31/12/2021
Finalise Information Security Management Framework	✓	31/12/2021
Identify and set appropriate security performance indicators and monitor and report against them	✓	31/12/2021
Complete annual KPI report and present to ELT and Risk Committee	WIP	30/6/2022
Populate the IAR - High Priority Systems	WIP	30/6/2022
Develop and implement annual review process of IAR records by record 'owner'	Not started	30/6/2022
Review Records Management Policy (Procedure to be reviewed in the next annual VPDSS action plan)	Not started	30/6/2022
Finalise and formalise Business Systems and User Access Management Procedure		**30/6/2022**
Develop a system administration and user management monitoring system	✓	30/6/2022
Develop an annual system to review administration and user management monitoring system	Not started	30/6/2022
Finalise and formalise Business Systems and User Access Management Procedure	WIP	30/6/2022
Develop a formal internal training/communications framework		**30/6/2022**
Review and update Data Privacy and Security Training Framework and associated training documents and put through formal approval process	✓	30/6/2022
Develop an information security induction session (review LDH content and update)	✓	30/6/2022
Develop an annual refresher session to be completed by all staff via LDH	WIP	30/6/2022
Complete annual data privacy and security training record	WIP	30/6/2022
Develop a Cyber Response Plan	✓	30/6/2022
Review ICT Business Continuity Plan	WIP	30/6/2022
Develop ICT Disaster Recovery Plan	WIP	30/6/2022
Third party contractors arrangements		**30/6/2022**
Develop an Information Security Management Procedure for third party arrangements and put through formal approval process	WIP	30/6/2022
Develop contractor register for contracted employees and 3rd party providers, with associated agreement and regular monitoring process.	WIP	30/6/2022
Review contractor engagement/induction process/paperwork	WIP	30/6/2022
Develop a software procurement and implementation framework		**30/6/2022**
Develop a software selection procedure	WIP	30/6/2022
Develop a software implementation procedure	WIP	30/6/2022
Develop a SaaS pre-engagement checklist	WIP	30/6/2022

What we've done ...

ICT Acceptable Use Policy

November, 2013

Privacy Policy

January 2022

Information Security Management Framework

December 2021

Information Security Pe

Indicators

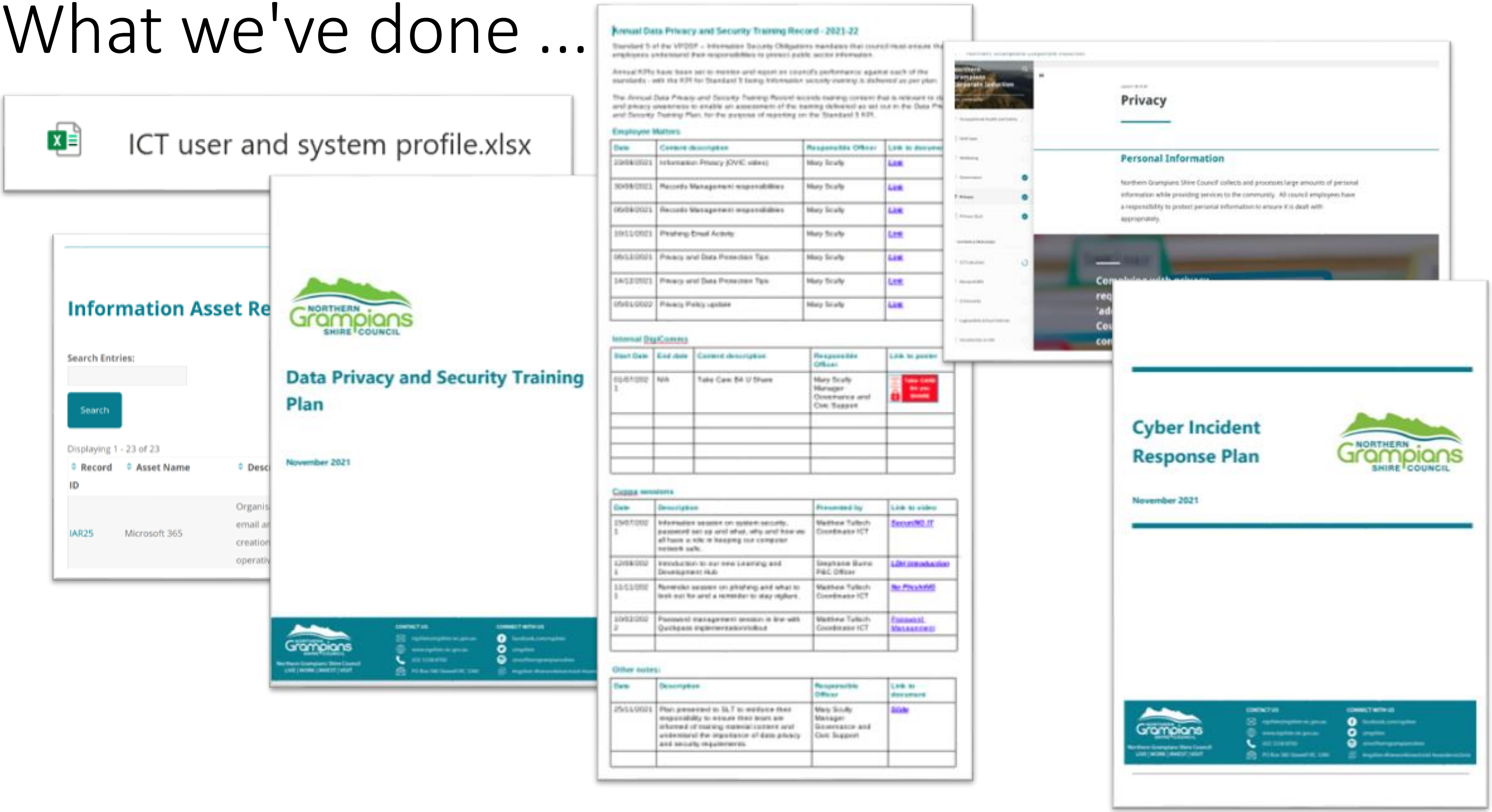
November 2021

Information Security Performance Indicators

Annual Report – MONTH, YYYY

NORTHERN
Grampians
SHIRE COUNCIL
CONTACT US
CONNECT WITH US
Northern Grampians Shire Council
LIVE | WORK | INVEST | VISIT

What we've done ...



ICT user and system profile.xlsx

Information Asset Re

Search Entries:

Search

Displaying 1 - 23 of 23

Record ID	Asset Name	Desc
IAR25	Microsoft 365	Organis email ar creation operativ

NORTHERN Grampians SHIRE COUNCIL

Data Privacy and Security Training Plan

November 2021

Annual Data Privacy and Security Training Record - 2021-22

Standard 5 of the VPDSF – Information Security Obligations mandates that council must ensure that employees understand their responsibilities to protect public sector information.

Annual KPIs have been set to monitor and report on council's performance against each of the standards - with the KPI for Standard 5 being Information security training is delivered as per plan.

The Annual Data Privacy and Security Training Record records training content that is relevant to data and privacy awareness to enable an assessment of the training delivered as set out in the Data Privacy and Security Training Plan, for the purpose of reporting on the Standard 5 KPI.

Employee Matters

Date	Content description	Responsible Officer	Link to docume
23/08/2021	Information Privacy (OVIC video)	Mary Scully	Link
30/08/2021	Records Management responsibilities	Mary Scully	Link
06/09/2021	Records Management responsibilities	Mary Scully	Link
10/11/2021	Phishing Email Activity	Mary Scully	Link
06/12/2021	Privacy and Data Protection Tips	Mary Scully	Link
14/12/2021	Privacy and Data Protection Tips	Mary Scully	Link
05/01/2022	Privacy Policy update	Mary Scully	Link

Internal DigiComms

Start Date	End date	Content description	Responsible Officer	Link to poster
01/07/2021	N/A	Take Care B4 U Share	Mary Scully Manager Governance and Civic Support	Take Care for you [illegible]

Cuppa sessions

Date	Description	Presented by	Link to video
15/07/2021	Information session on system security, password set up and what, why and how we all have a role in keeping our computer network safe.	Matthew Tulloch Coordinator ICT	SecureMD IT
12/08/2021	Introduction to our new Learning and Development Hub	Stephanie Burns P&C Officer	LDH introduction
11/11/2021	Reminder session on phishing and what to look out for and a reminder to stay vigilant.	Matthew Tulloch Coordinator ICT	No PhishING
10/02/2022	Password management session in line with Quickpass implementation/rollout	Matthew Tulloch Coordinator ICT	Password Management

Other notes:

Date	Description	Responsible Officer	Link to document
25/11/2021	Plan presented to SLT to reinforce their responsibility to ensure their team are informed of training material content and understand the importance of data privacy and security requirements.	Mary Scully Manager Governance and Civic Support	Slide

Northern Grampians Corporate Induction

Privacy

Personal Information

Northern Grampians Shire Council collects and processes large amounts of personal information while providing services to the community. All council employees have a responsibility to protect personal information to ensure it is dealt with appropriately.

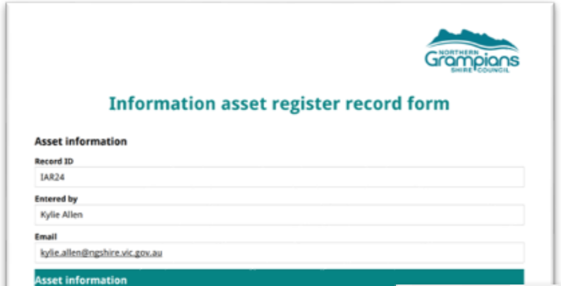
Complying with privacy req 'ad Cou con

Cyber Incident Response Plan

NORTHERN Grampians SHIRE COUNCIL

November 2021

What we're doing …



NORTHERN Grampians SHIRE COUNCIL

Information asset register record form

Asset information

Record ID
IAR24

Entered by
Kylie Allen

Email
kylie.allen@ngshire.vic.gov.au

Asset information

Asset name
What is the system, dataset or collection of information?
SirsiDynix

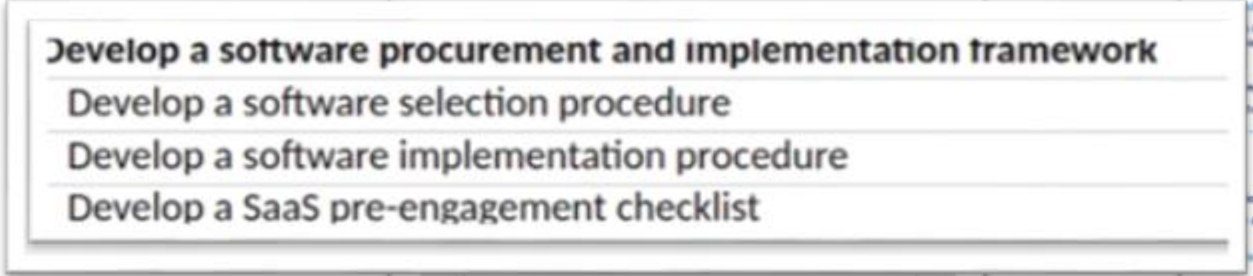
Description
What is the purpose of the information asset and what type of information is contained in it? What are t

Library Management System software including catalogue library assets, member conta
management, issuing & returning items, accessing collections from external Sirsi conso

Business Systems and User Access Management Procedure

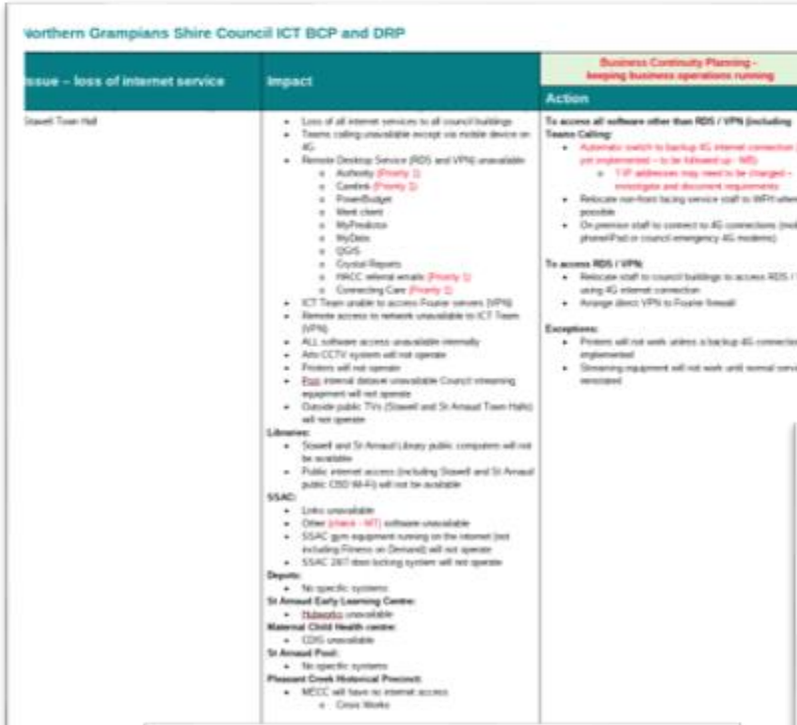
NORTHERN Grampians SHIRE COUNCIL

July 2020



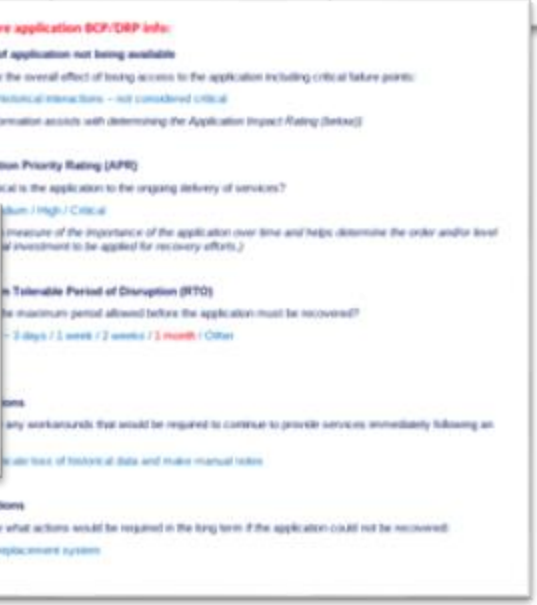
Develop a software procurement and implementation framework

- Develop a software selection procedure
- Develop a software implementation procedure
- Develop a SaaS pre-engagement checklist



Northern Grampians Shire Council ICT BCP and DRP

Issue – loss of internet service	Impact	Business Continuity Planning - keeping business operations running	Disaster Recovery Planning - restoring normal business operations
		Action	Action
Stawell Town Hall	- Loss of all internet services to all council buildings - Teams calling unavailable except via mobile device on 4G - Remote Desktop Service (RDS) and VPN unavailable - Authority (Priority 1) - Cardinal (Priority 1) - PowerBudget - Merit client - MyPredictor - MyData - QGIS - Crystal Reports - HACC referral emails (Priority 1) - Connecting Care (Priority 1) - ICT Team unable to access Fourier servers (VPN) - Remote access to network unavailable to ICT Team (VPN) - ALL software access unavailable internally - Avigilon CCTV system will not operate - Printers will not operate - Foxtel internal dataset unavailable Council streaming equipment will not operate - Outside public TVs (Stawell and St Arnaud Town Halls) will not operate **Libraries:** - Stawell and St Arnaud Library public computers will not be available - Public internet access (including Stawell and St Arnaud public CBD Wi-Fi) will not be available **SSAC:** - Links unavailable - Other (check - MT) software unavailable - SSAC gym equipment running on the internet (not including Fitness on Demand) will not operate - SSAC 24/7 door locking system will not operate **Depots:** - No specific systems **St Arnaud Early Learning Centre:** - Hubworks unavailable **Maternal Child Health centre:** - CDIS unavailable **St Arnaud Pool:** - No specific systems **Pleasant Creek Historical Precinct:** - MECC will have no internet access - Cross Works	**To access all software other than RDS / VPN (including Teams Calling:** - Automatic switch to backup 4G internet connection (not yet implemented – to be followed up - MB) - 1 IP addresses may need to be changed - investigate and document requirements - Relocate non-front facing service staff to WFH wherever possible - On premise staff to connect to 4G connections (mobile phone/iPad or council emergency 4G modems) **To access RDS / VPN:** - Relocate staff to council buildings to access RDS / VPN using 4G internet connection - Arrange direct VPN to Fourier firewall **Exceptions:** - Printers will not work unless a backup 4G connection is implemented - Streaming equipment will not work until normal service reinstated	**Option 1:** Reinstate service **Option 2:** In the case of inability of provider to reinstate service source replacement provider. Refer to most recent RFQ for specification, review and source replacement



Software application BCP/DRP info:

Impact of application not being available

Describe the overall effect of losing access to the application including critical failure points:

Loss of historical interactions – not considered critical

(This information assists with determining the Application Impact Rating (below))

Application Priority Rating (APR)

How critical is the application to the ongoing delivery of services?

[illegible] dium / High / Critical

[illegible] measure of the importance of the application over time and helps determine the order and/or level [illegible] al investment to be applied for recovery efforts.)

[illegible] n Tolerable Period of Disruption (RTO)

[illegible] he maximum period allowed before the application must be recovered?

[illegible] – 3 days / 1 week / 2 weeks / 1 month / Other

[illegible] ons

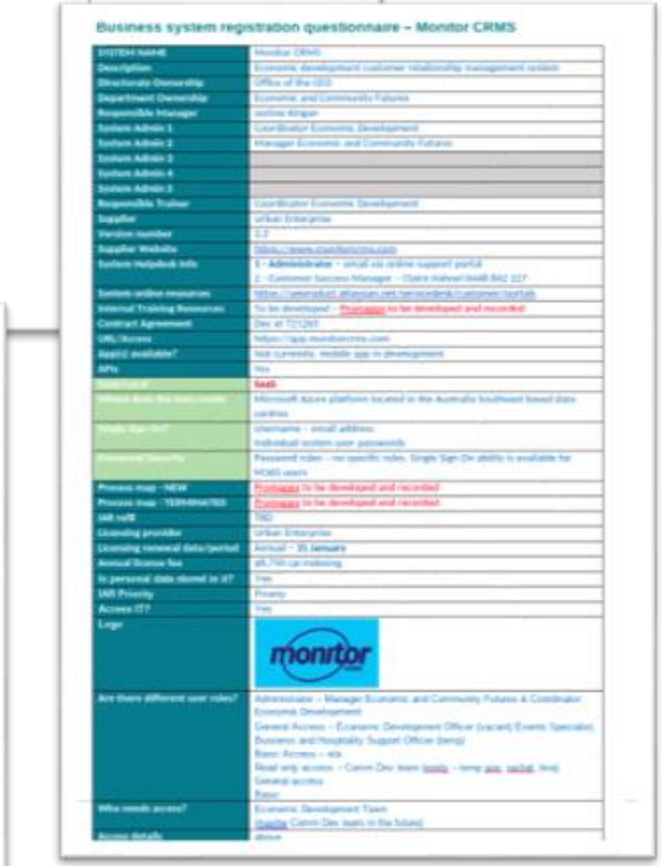
[illegible] any workarounds that would be required to continue to provide services immediately following an [illegible]

[illegible] ate loss of historical data and make manual notes

DRP actions

Describe what actions would be required in the long term if the application could not be recovered:

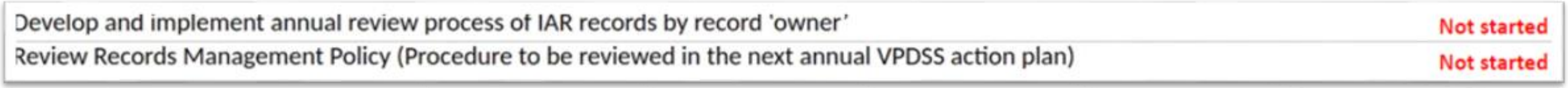
Source replacement system



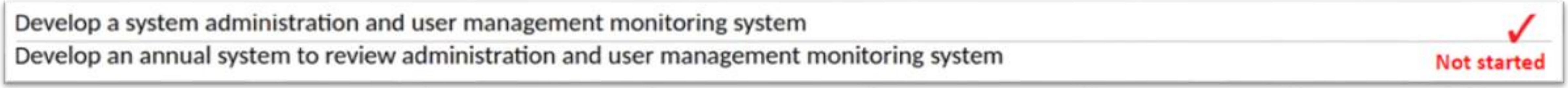
Business system registration questionnaire – Monitor CRMS

SYSTEM NAME	Monitor CRMS
Description	Economic development customer relationship management system
Directorate Ownership	Office of the CEO
Department Ownership	Economic and Community Futures
Responsible Manager	[illegible]
System Admin 1	Coordinator Economic Development
System Admin 2	Manager Economic and Community Futures
System Admin 3	
System Admin 4	
System Admin 5	
Responsible Trainer	Coordinator Economic Development
Supplier	Urban Enterprise
Version number	2.2
Supplier Website	https://www.monitorcrms.com
System Helpdesk info	1 - **Administrator** – email via online support portal 2 - Customer Success Manager – [illegible]
System online resources	https://[illegible].atlassian.net/servicedesk/customer/portal/[illegible]
Internal Training Resources	To be developed - Promapp to be developed and recorded
Contract Agreement	Dec at T21/[illegible]
URL/Access	https://app.monitorcrms.com
App(s) available?	Not currently, mobile app in development
APIs	Yes
[illegible]	SaaS
[illegible]	Microsoft Azure platform located in the Australia Southeast based data centres
[illegible]	Username – email address Individual system user passwords
[illegible]	Password rules – no specific rules. Single Sign On ability is available for M365 users
Process map - NEW	Promapp to be developed and recorded
Process map - TERMINATED	Promapp to be developed and recorded
IAR ref#	TBD
Licensing provider	Urban Enterprise
Licensing renewal date/period	Annual – 31 January
Annual license fee	$[illegible]
Is personal data stored in it?	Yes
IAR Priority	Priority
Access IT?	Yes
Logo	monitor
Are there different user roles?	Administrator – Manager Economic and Community Futures & Coordinator Economic Development General Access – Economic Development Officer (vacant) Events Specialist Business and Hospitality Support Officer (temp) Basic Access – n/a Read only access – Comm Dev team ([illegible] – temp [illegible], [illegible], [illegible]) General access Basic
Who needs access?	Economic Development Team (maybe Comm Dev team in the future)
Access details	above

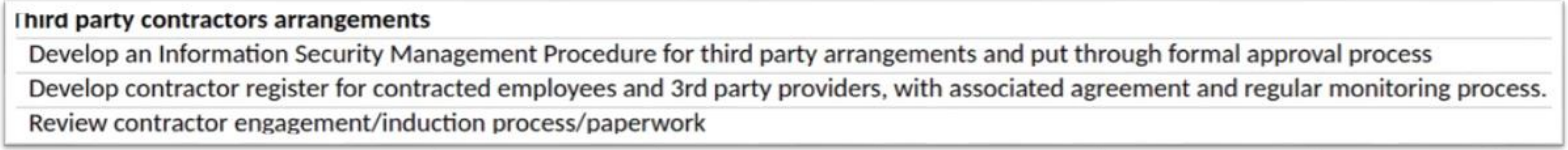
What we're going to do ...



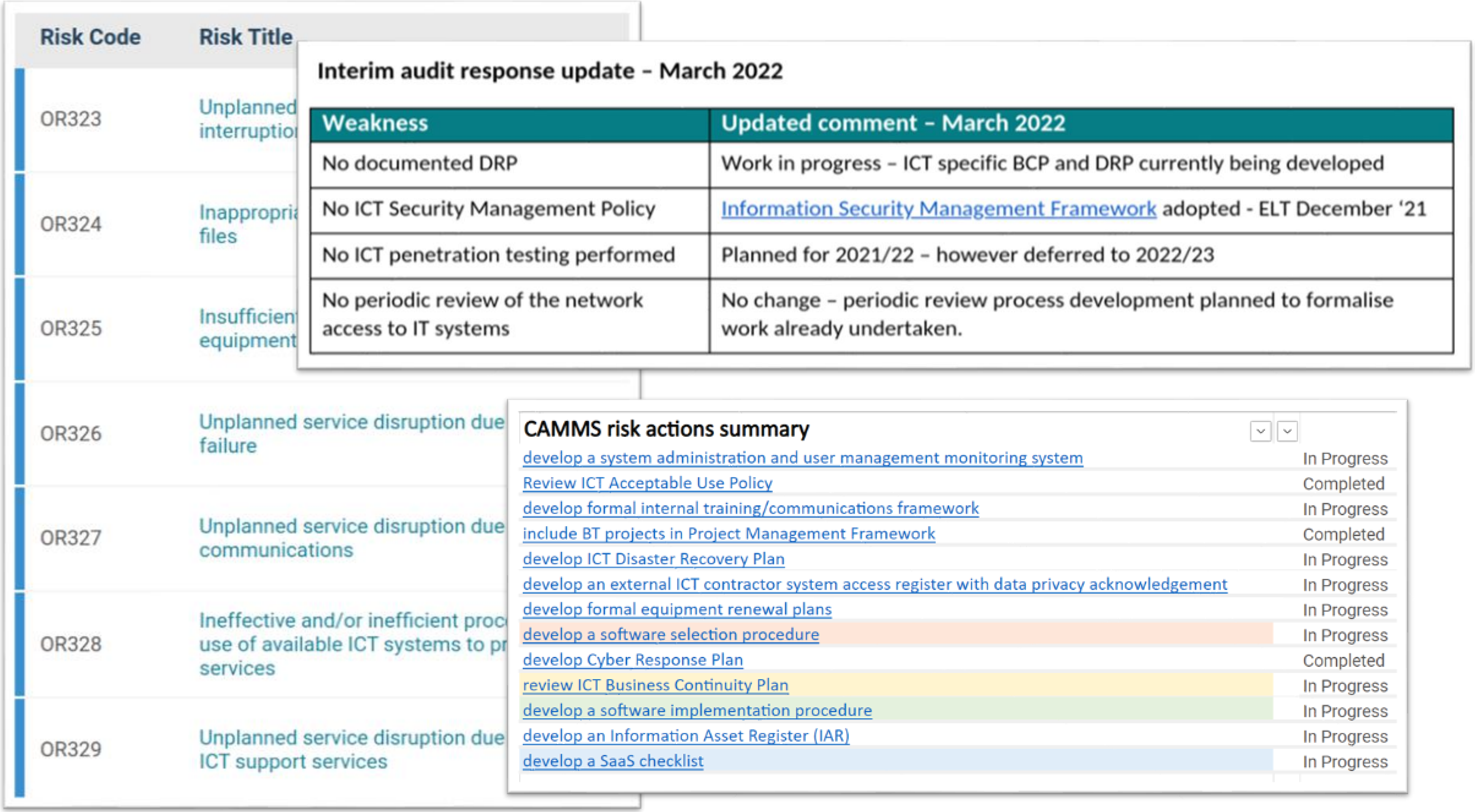
Develop and implement annual review process of IAR records by record 'owner'	Not started
Review Records Management Policy (Procedure to be reviewed in the next annual VPDSS action plan)	Not started



Develop a system administration and user management monitoring system	✓
Develop an annual system to review administration and user management monitoring system	Not started



Third party contractors arrangements
Develop an Information Security Management Procedure for third party arrangements and put through formal approval process
Develop contractor register for contracted employees and 3rd party providers, with associated agreement and regular monitoring process.
Review contractor engagement/induction process/paperwork



Risk Code	Risk Title
OR323	Unplanned interruptio
OR324	Inappropri files
OR325	Insufficien equipment
OR326	Unplanned service disruption due failure
OR327	Unplanned service disruption due communications
OR328	Ineffective and/or inefficient proc use of available ICT systems to pr services
OR329	Unplanned service disruption due ICT support services

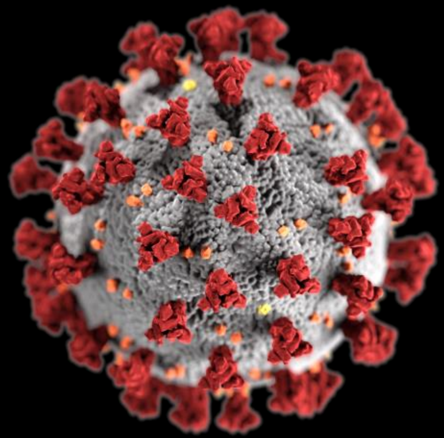
Interim audit response update – March 2022

Weakness	Updated comment – March 2022
No documented DRP	Work in progress – ICT specific BCP and DRP currently being developed
No ICT Security Management Policy	Information Security Management Framework adopted - ELT December '21
No ICT penetration testing performed	Planned for 2021/22 – however deferred to 2022/23
No periodic review of the network access to IT systems	No change – periodic review process development planned to formalise work already undertaken.

CAMMS risk actions summary

develop a system administration and user management monitoring system	In Progress
Review ICT Acceptable Use Policy	Completed
develop formal internal training/communications framework	In Progress
include BT projects in Project Management Framework	Completed
develop ICT Disaster Recovery Plan	In Progress
develop an external ICT contractor system access register with data privacy acknowledgement	In Progress
develop formal equipment renewal plans	In Progress
develop a software selection procedure	In Progress
develop Cyber Response Plan	Completed
review ICT Business Continuity Plan	In Progress
develop a software implementation procedure	In Progress
develop an Information Asset Register (IAR)	In Progress
develop a SaaS checklist	In Progress

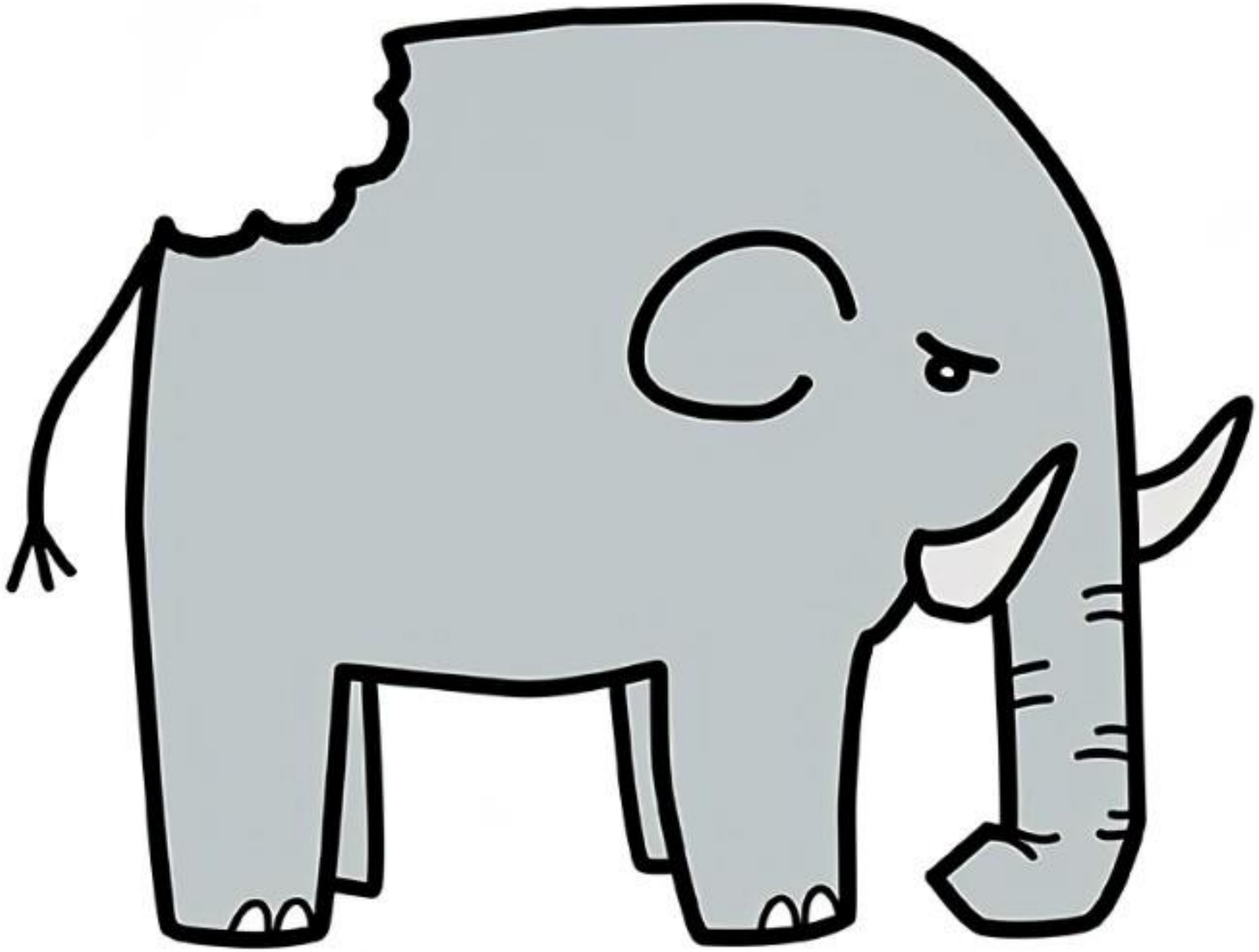
Cyber Security is the new black!



'the application of technologies, processes and controls to protect systems, networks, programs, devices and data from cyber attacks'

HOW DO YOU EAT AN ELEPHANT?

ONE BITE AT A TIME!



Victorian Government Office 365 Security Guidance

Microsoft Secure Score

ACSC Essential Eight Maturity Model

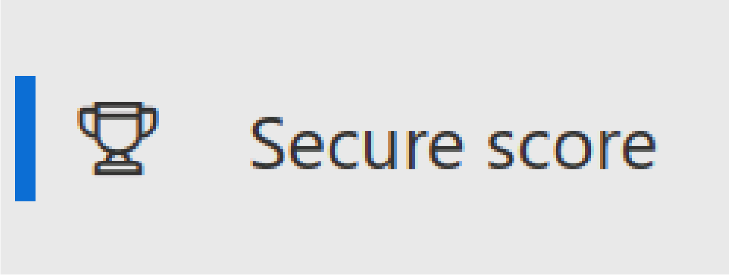
Zero Trust Security Model

Victorian Government
Office 365
Security Guidance
DRAFT

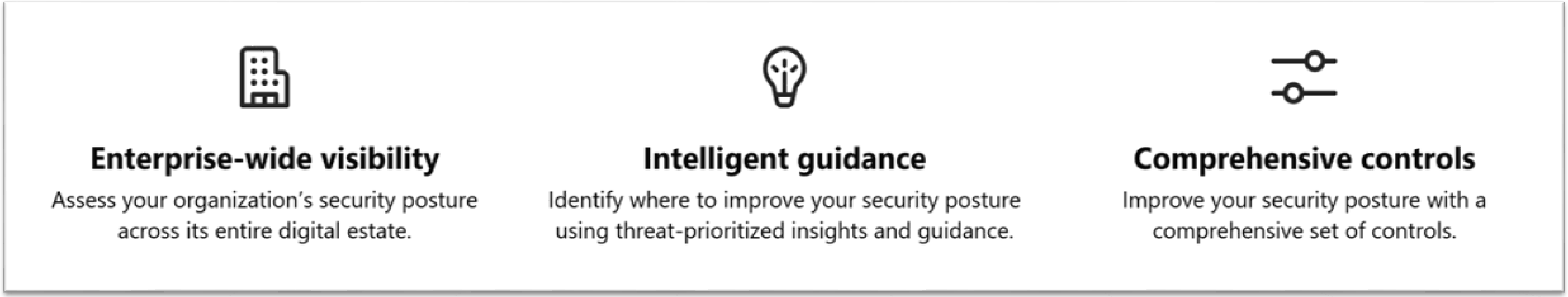
VICTORIA State Government | Premier and Cabinet

- **recently released**
- **reviewing requirements and developing a plan**
- **Microsoft secure score >70**

Microsoft Secure Score



visibility, insights, and guidance to maximize council's security and take advantage of Microsoft 365



Enterprise-wide visibility

Assess your organization's security posture across its entire digital estate.

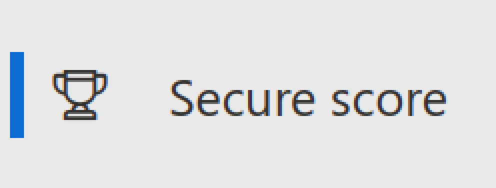
Intelligent guidance

Identify where to improve your security posture using threat-prioritized insights and guidance.

Comprehensive controls

Improve your security posture with a comprehensive set of controls.

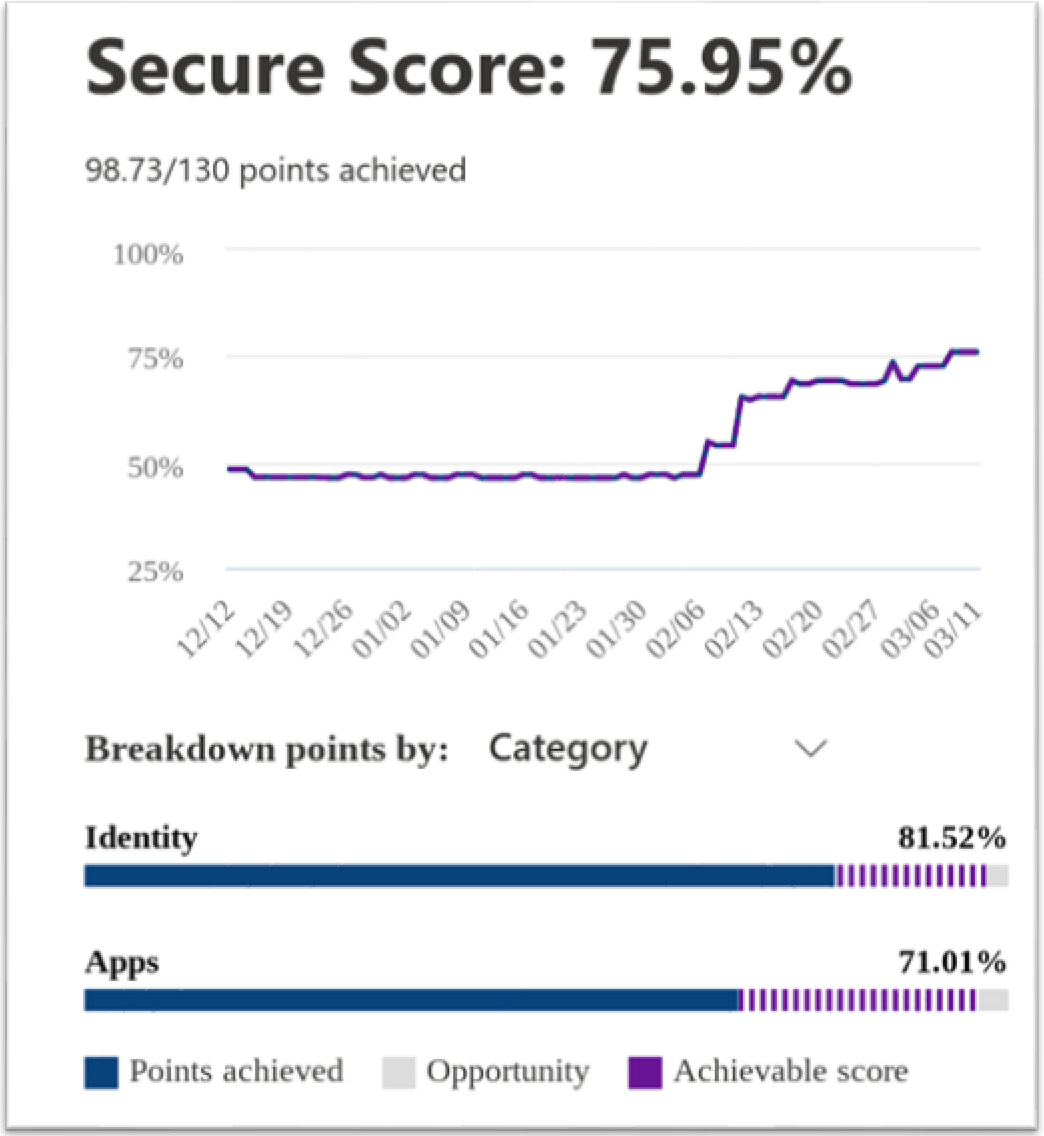
- a measurement of an organisation's security posture
- improve security posture by providing, visibility, guidance, and control
- following recommendations can protect the organisation from threats



Secure score

47% when we started

- 33 tasks
- 22 completed
- 3 outstanding risks accepted
- 8 still to action



Secure Score: 75.95%

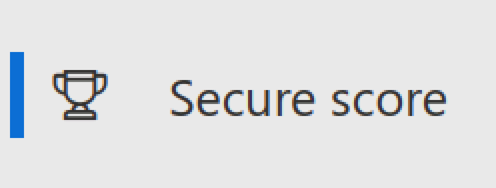
98.73/130 points achieved

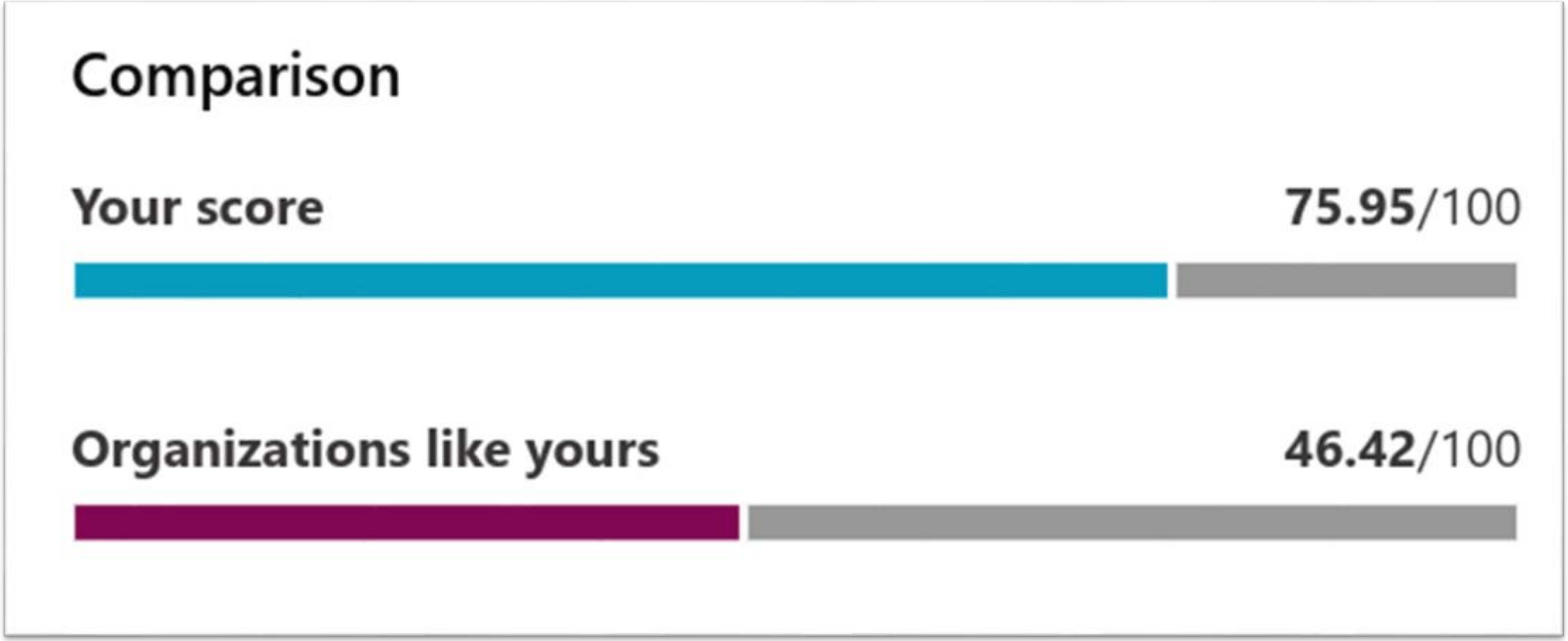
Breakdown points by: Category

Identity 81.52%

Apps 71.01%

🟦 Points achieved ⬜ Opportunity 🟪 Achievable score




Comparison

Your score 75.95/100

Organizations like yours 46.42/100

Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Essential Eight

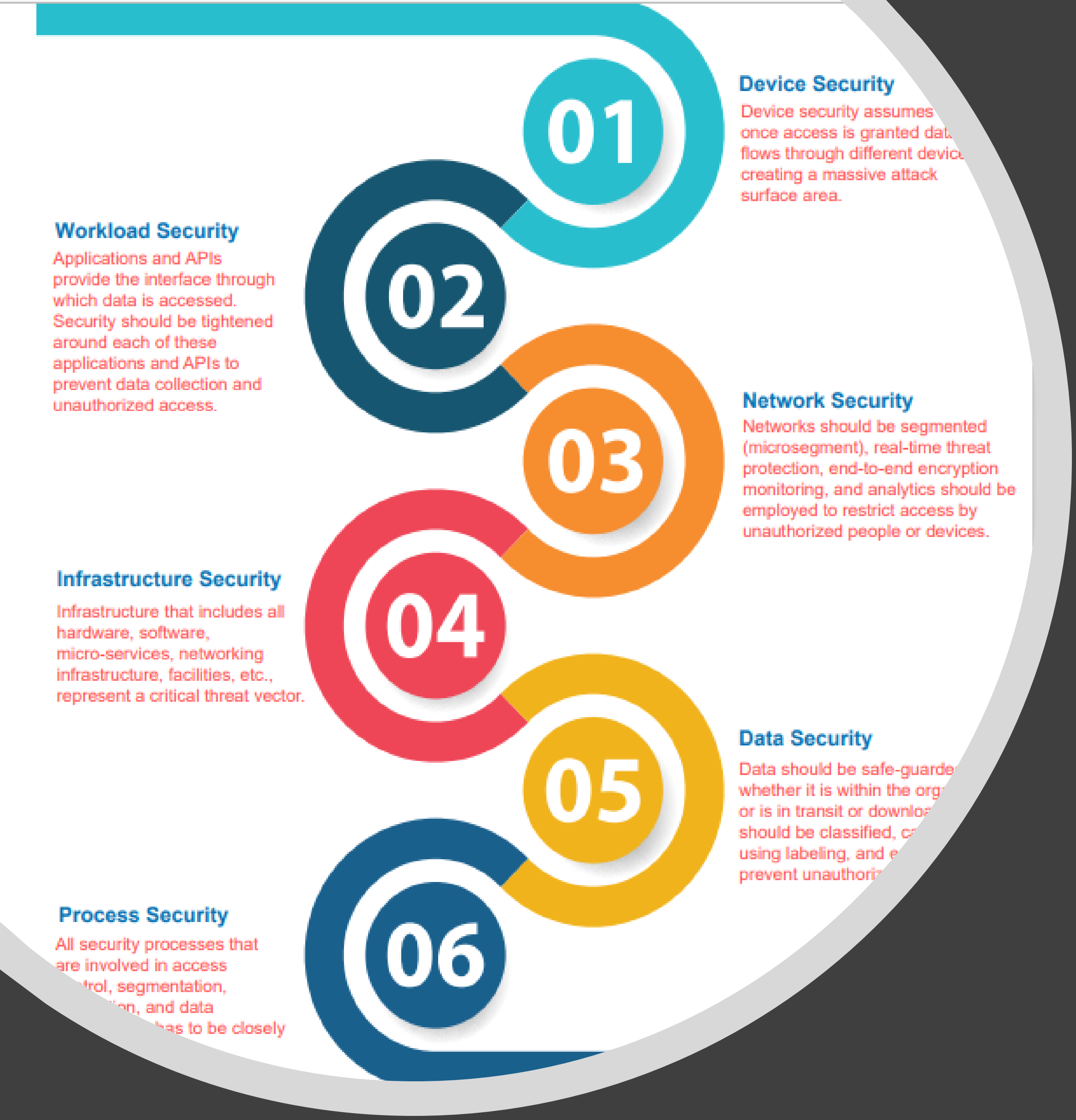
Essential Eight

The **Essential Eight** are designed to protect Microsoft Windows-based internet-connected networks.

- **application control**
- **patch applications**
- **configure Microsoft Office macro settings**
- **user application hardening**
- **restrict administrative privileges**
- **patch operating systems**
- **multi-factor authentication**
- **regular backups**

Maturity levels 0 – 3

- review baseline strategies
- assess council's maturity level against
  - our current security practices
  - VPDSS work undertaken
  - Microsoft Secure Score actions
- develop a plan
- implement identified improvements
- 2022/23 external audit against Essential Eight



Device Security

Device security assumes once access is granted dat flows through different device creating a massive attack surface area.

Workload Security

Applications and APIs provide the interface through which data is accessed. Security should be tightened around each of these applications and APIs to prevent data collection and unauthorized access.

Network Security

Networks should be segmented (microsegment), real-time threat protection, end-to-end encryption monitoring, and analytics should be employed to restrict access by unauthorized people or devices.

Infrastructure Security

Infrastructure that includes all hardware, software, micro-services, networking infrastructure, facilities, etc., represent a critical threat vector.

Data Security

Data should be safe-guarde whether it is within the org or is in transit or downloa should be classified, c using labeling, and e prevent unauthori

Process Security

All security processes that are involved in access trol, segmentation, tion, and data has to be closely

The zero-trust security model

"never trust, always verify"

particularly where significant use of cloud services is in place

BOOM!