Government Services

Victorian Government IT Asset Management Guidance

Digital Victoria

Cyber Security Branch

Version 1.5 Issued February 2023

Content

Document	
Name	WoVG IT Asset Management Guidance
Reference	VG-CISO Guidance V1.5 – IT Asset Management
Approved	David Cullen Victorian Government Chief Information Security Officer Cyber Security Branch, Digital Victoria
Issued	Xavier Brouwer Victorian Government Lead Security Architect Cyber Security Branch, Digital Victoria
Authority	Victorian Government Cyber Security Strategy 2021/2022 *1.1 Develop an IT asset management guideline in line with Asset Management Accountability Framework (AMAF) and Victorian Protective Data Security Framework (VPDSF) requirements.*
Contact for updates	vicgov.ciso@dpc.vic.gov.au
Registration	Version 1.5, D21/150630

Context

Purpose

To effectively manage IT and Cybersecurity risk, it is essential for organisations to continuously maintain visibility of their IT infrastructure and applications and manage the full asset lifecycle from planning, through acquisition and operation, to disposal. This document provides recommended best practices for Victorian government entities to adopt in this regard.

Audience

This guidance is targeted at department and agency:

- CIO's (Chief Information Officers)
- CISO's (Chief Information Security Officers)
- Cyber Security Practitioners
- IT Asset Owners/Custodians
- Application Managers/Product Managers
- IT Asset Management Steering Committees/Governance Board Members
- IT Asset Managers
- IT Infrastructure/Operations Managers and Team Leads
- Enterprise Architects

and assumes a basic knowledge of IT operational processes.

Resources

The following resources are associated with this guidance. Please contact the Cyber Security Branch at vicgov.ciso@dpc.vic.gov.au to access the following resources:

Title	Description
AMAF 41 Processes – IT Asset Class Considerations	Excel Spreadsheet - Commentary on how the asset generic AMAF processes can be interpreted in an IT asset context.
WoVG IT Asset Management Data Dictionaries	Excel Spreadsheet - Recommended standardised fields that can be used to capture Application and Infrastructure data in a CMDB

WOVG IT Asset Management Cybersecurity KPIs	Excel Spreadsheet - A list of example KPIs that can be applied to IT asset management to ensure the maintenance of good cybersecurity.

Benefits

Cybersecurity

Good IT asset management contributes directly to better cybersecurity in an organisation. Regularly performing IT asset management processes such as updating asset registers, replacing assets before end of life, patching systems, monitoring systems, and securely disposing of storage results in a significantly improved organisational security posture.

Cyber security issues that can occur when IT assets are not well managed include:

- Data being **stolen** from unpatched IT assets or lost IT assets
- Unmaintained IT assets being encrypted by **ransomware**
- Unused assets being repurposed as **internal attack platforms**
- Malicious actors making unmaintained assets **unavailable** for normal business use
- Unmaintained assets become unavailable due to **lack of maintenance**
- Lack of **basic** (e.g. Essential 8) operating system cybersecurity controls leading to avoidable breaches
- An inability to map often **urgent threat intelligence** to specific IT assets
- An inability to **prioritise** IT asset maintenance activities and budget based on risk
- Unknown risk visibility and **risk exposure** of the IT asset fleet, including asset **end-of-life**
- An inability to detect **rogue**, malicious and unsanctioned IT assets
- **Insecure disposal** of IT assets resulting in data leakage
- Difficulties **attracting and retaining staff** to perform important but sometimes mundane/repetitive IT asset maintenance activities
- Higher **cyber insurance (re)insurance premiums** due to an inability to demonstrate good asset management and basic cybersecurity hygiene
- An inability to assess the adverse impact of aging IT assets on cyber risk and business productivity, resulting in **suboptimal planning** for timely disposal and replacement

Financial Benefits

In addition to these cybersecurity-related problems, poor IT asset management can also result in **financial inefficiency**, for example:

- Duplicate contracts, over licensing and overprovisioning of IT assets within an organisation
- Lack of all-of-government contracts/efficiency of scale, due to lack of IT asset visibility
- Unused assets creating unnecessary ongoing costs and non-strategic budget spend
- Inefficient cost optimisation/asset utilisation
- Service continuity/supportability issues

Note that financial benefits are not directly addressed by this guidance. Improving IT asset management for cybersecurity reasons lays the groundwork for an organisation to realise financial benefits more easily through additional improvement activities.

Regulatory Requirements

The following regulatory requirements apply to IT asset management for many Victorian Government departments and agencies:

Asset Management Accountability Framework 2016 (DTF)

- 41 Mandatory Requirements
- Optional Guidance
- Self-assessment every three years

Victorian Protective Data Security Standard v2.0 (OVIC)

- "The organisation manages all ICT assets (e.g. on-site, and off-site) throughout their lifecycle" [E11.020]

Scope

Agency Scope

This guidance applies to all Victorian Public Service departments and agencies, including the Health, Water, Education, Justice and Local Government sectors. Note that even though some agencies are not covered by the Financial Management Act mandating AMAF, or be required to comply with VPDSS or Essential 8, they may still wish to follow this guidance as a collection of best practices.

In Scope IT Assets

The following IT assets are in scope of this guidance:

- Servers (virtual and physical)
- Applications (client-side, on prem/data centre and cloud-hosted)
- Database systems and Middleware
- Network appliances (Wi-Fi access points, firewalls, switches, routers, bridges, gateways, modems, repeaters, hubs etc)
- PCs (laptops and desktops)
- Mobile devices/Smartphones/Tablets/SIM cards issued by department/agency
- Business critical IP phones and phone lines, cloud phone systems
- Networked Multifunction Devices/Printers/Scanners/Faxes
- Security Certificates
- Cloud applications (SaaS)
- Cloud platforms (PaaS)
- Cloud infrastructure (IaaS)
- Outsourced/Third Party Hosted/Managed Services IT assets (delegated IT asset management responsibility)
- IoT/embedded systems/electronic medical devices (if relevant to the organisation)

Out of Scope IT Assets

The following are out of scope of this guidance:

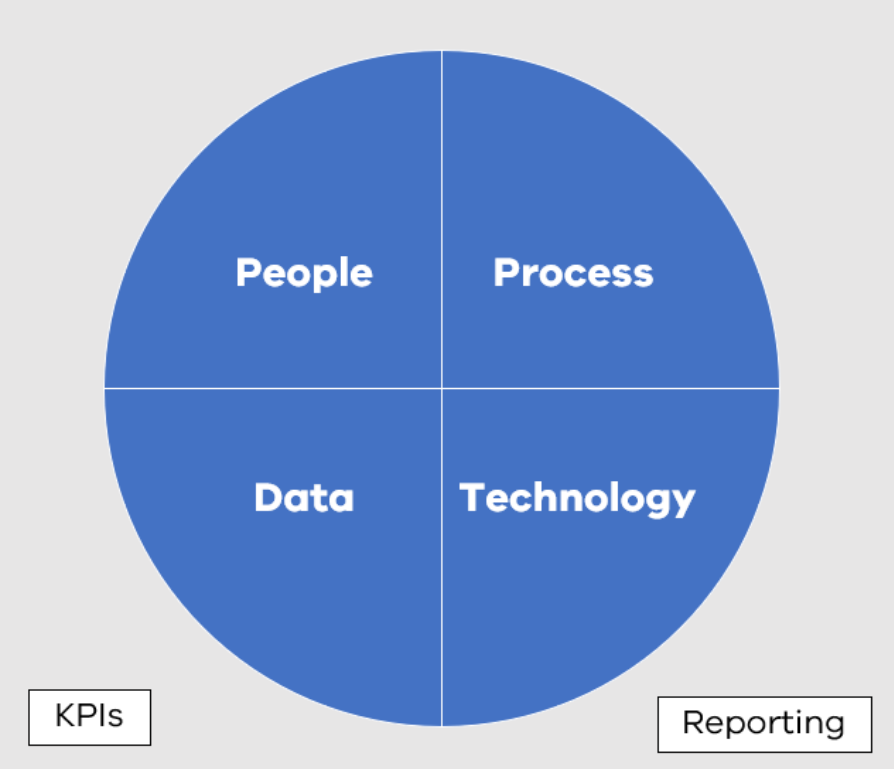
- Keyboards and pointing devices (e.g. mice)
- Monitors
- Data Centres
- Information/Data Assets (this is covered by OVIC's VPDSS Framework)
- Data retention and archiving
- IT Contracts
- IT Financial Management (including depreciation)
- Linking IT assets to Business Processes
- Linking IT assets to Business or public services

Framework

The aim of this guidance is to help departments and agencies across all sectors (including health, water, education and local government) improve their IT asset management. In addition to ensuring that the cybersecurity issues are addressed, a standard way of approaching IT asset management across the Victorian Government makes the following easier:

- Choosing and implementing an IT asset management approach in a department/agency
- Performing Machinery of Government changes
- Providing pre-configured (including multi-tenant) ITAM technology solutions
- Establishing value-for-money WoVG Deeds of Standing Offer
- Facilitating the movement of IT asset management and IT operations staff within and across departments and agencies
- Sharing asset management people, process and training resources
- Achieving consolidated and streamlined reporting across government
- Performing maturity assessments and benchmarking across government
- Identifying comparative risks across government

To improve IT asset management in an organisation, four areas need to be addressed: **People**, **Process**, **Data** and **Technology.**



People

One of the main issues impeding good IT asset management is the difficulty attracting and retaining staff to perform important but often repetitive IT asset management processes. Another major hurdle is that IT asset management responsibilities are usually distributed across multiple IT and even business teams, even if an organisation has a dedicated and centralised IT Asset Manager role.

Some of the actions an organisation can take to address these people-related issues include:

1. Establishing or leveraging an existing **Steering Committee / Governance Board** chaired by the CIO (or equivalent) and including the managers of staff who have IT asset management responsibilities across the organisation. This can be dedicated to IT asset management or leverage an existing committee/board e.g. for IT, IT Operations, Asset Management (all classes) or Enterprise Architecture.
2. **Allocate the responsibility** for each IT asset management process against staff (and any external providers). Typical roles involved in IT asset management include: Enterprise Architect, Asset Owners/Custodians, End User Administration Team Lead, Windows Administration Team Lead, Unix/Linux Administration Team Lead, Network Administration Team Lead, Database Administration Team Lead, Cloud Platform Administration Leads, and Application Support Leads.
3. Embed IT asset management KPIs into the **Performance Plans** of the relevant staff in your organisation
4. Embed IT asset management KPIs into the **contracts** of relevant external suppliers (with levers to ensure these KPIs are achieved and maintained)
5. If finding and retaining staff to fulfill IT asset management roles is an issue, consider **hiring Victorians from diverse backgrounds**. There are several programs encouraging more people from diverse backgrounds into entry-level cybersecurity and IT roles.
6. Educate **Risk and Audit committees** on the need to consider auditing IT asset management

Some examples of **entry level** IT asset management jobs include:

- Infrastructure asset identification (e.g. maintaining CMDB data, chasing up missing data)
- Infrastructure scanning (identifying missing assets and patch levels)
- Malware monitoring & remediation (on PCs)
- Maintaining client-side application packages
- Phone and PC provisioning
- Infrastructure performance monitoring against SLAs
- Monthly KPI reporting
- Yearly reconciliation (e.g. CMDB vs HR system reconciliation for end user devices)
- Certificate management
- Secure asset disposal
- Identity lifecycle management user access reviews

Some examples of **more advanced** IT asset management/career progression jobs could include:

- Infrastructure patching (servers)
- Backup management and restore testing
- Windows server administration
- Unix server administration
- Network administration
- Office365, Azure, AWS and Google Cloud Platform administration
- Application support/administration
- Cybersecurity analysis (including Security Operations Centre eyes-on-glass)

Process

This process is written to comply with requirements in the Asset Management Framework (AMAF) overseen by the Victorian Department of Treasury and Finance.

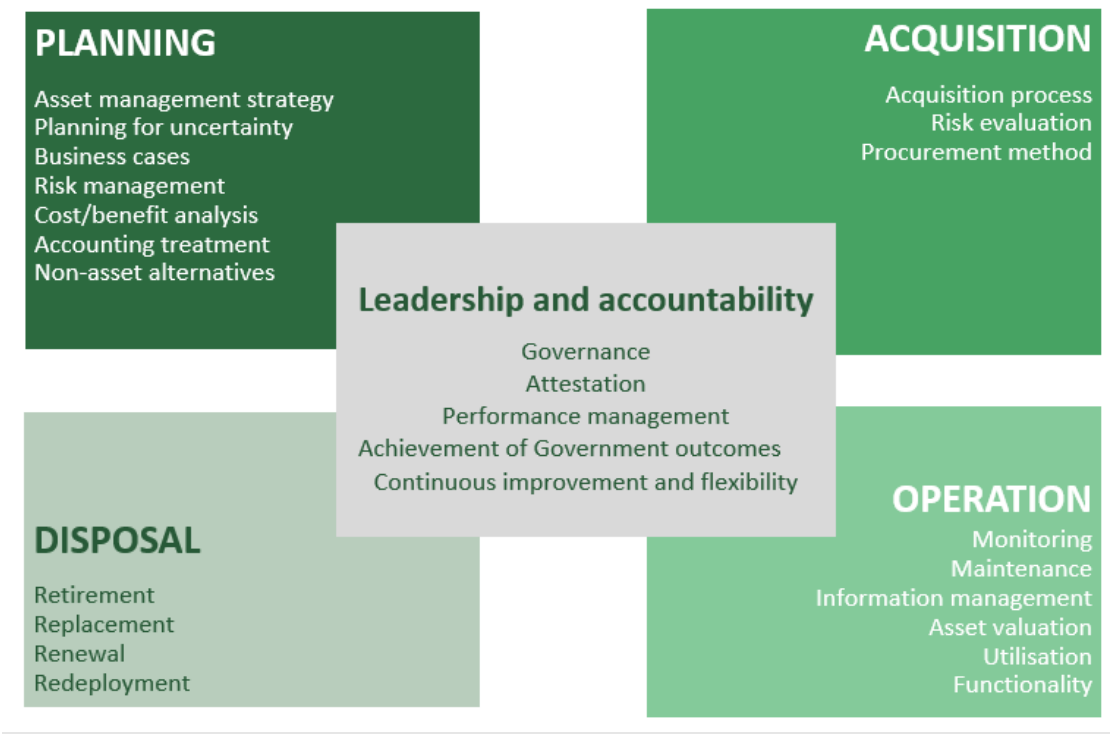
AMAF is a framework used to measure the maturity of government asset management across all asset classes (IT, buildings, vehicles etc). Although this is a generic asset framework, it can be applied in the context of the IT asset class (when interpreted through an ITIL lens).

Please contact the Cyber Security Branch at vicgov.ciso@dpc.vic.gov.au to access the **AMAF 41 Processes – IT Asset Class Considerations** resource for a suggested interpretation.

Other frameworks were considered such as COBIT, IT-CMF and ISO 19770, however AMAF is recommended for the following reasons:

- The **41 process areas** of AMAF allow IT asset management to be measured at a manageable and useful level of detail (not too high level nor too low level)
- Many Victorian Government organisations are **already measuring** the maturity of their overall asset management, and in some instances their IT asset management, using AMAF
- AMAF is a **mandatory framework** (underpinned by the Financial Management Act) for many Victorian Government departments and agencies

AMAF describes the following end-to-end **asset lifecycle**:



AMAF also provides a self-assessment **Compliance Tool** with which the 41 process areas can be allocated one of the following maturity levels:

- Innocence (level 0)
- Awareness (level 1)
- Developing (level 2)
- Competence (level 3)
- Optimising (level 4)

This tool can be used to measure the maturity of the IT asset class (as well as other asset classes).

Some organisations will also be assessing some of their IT asset management processes against VPDSS requirements which uses a similar 5 tier system (the tiers being: Informal, Basic, Core, Managed, Optimising).

It is recommended that all Victorian Government departments and agencies achieve and maintain a minimum level of **Competence** (level 3) for all 41 AMAF processes in the domain of IT asset management.

It is recommended that the level of **Optimising** (level 4) should be achieved and maintained for the following specific IT assets:

- IT assets that process or hold **Protected** or above data, or have one or more OVIC Integrity or Availability Business Impact rating of **3 (Major)** or above
- IT assets containing **Personal Information** (as per Privacy and/or Health Acts)
- **Internet-facing** IT assets (including webservers, network perimeter devices, SaaS, PaaS and IaaS)

AMAF requires a generic asset self-assessment against these 41 process areas every **three years**, however it you have an active IT asset management uplift project or BAU (business as usual) activity in progress, it is recommended redoing the self-assessment every 6-12 months to measure and demonstrate progress. Note that the first time an AMAF maturity assessment for the IT asset class is undertaken may take more time and effort than subsequent assessments.

Data

It is important that department and agency IT Asset Registers hold **complete and correct** data. Missing asset entries can lead to IT assets being overlooked and subsequently unpatched and unmonitored, which can lead to cybersecurity incidents. Missing asset fields can lead to difficulties prioritising assets based on risk and allocating ownership and responsibility.

This guidance defines a minimum standard of asset fields that can be captured for both **Application** as well as **Infrastructure** assets. Note that OVIC's VPDSS provides a minimum standard around **Information (Data)** assets. This VPDSS Information (Data) Asset Register spreadsheet can be imported into and maintained in your CMDB or Enterprise Architecture system in order to link Information (Data) assets to Application assets more easily.

Please contact the Cyber Security Branch at vicgov.ciso@dpc.vic.gov.au to access the resource **WoVG IT Asset Management Data Dictionaries** for a detailed breakdown of the recommended Application and Infrastructure fields.

Business Impact Levels

Two main **business impact** rating systems are used across Victorian Government departments and agencies to indicate Confidentiality, Integrity and Availability consequence (one from OVIC and one used in the Health Sector).

If an agency does not yet use a Business Impact system, or wishes to standardise on one, OVIC's system is recommended.

The following table describes the OVIC Business Impact Levels:

Confidentiality (PROTECTED MARKING)	Integrity	Availability
5 – Exceptional (TOP SECRET)	5 - Exceptional	5 - Exceptional
4 – Serious (SECRET)	4 - Serious	4 - Serious
3 – Major (PROTECTED)	3 - Major	3 - Major
2 – Limited (OFFICIAL:SENSITIVE)	2 - Limited	2 - Limited
1 – Minor (OFFICIAL)	1 - Minor	1 - Minor
0 – n.a. (UNOFFICIAL) = no business impact	0 - n.a. = no impact	0 - n.a. = no impact

In some circumstances the **aggregation** of a data set or multiple data sets may raise the consequence from a Business Impact Level to the next higher one. The combined data itself doesn't get reclassified at the higher level but the business impact pertaining to the combined datasets, and the cybersecurity controls required to protect against these risks, may be heightened (e.g. a shift from a BIL of 2 to a BIL of 3 for a large aggregation of OFFICIAL:SENSITIVE data).

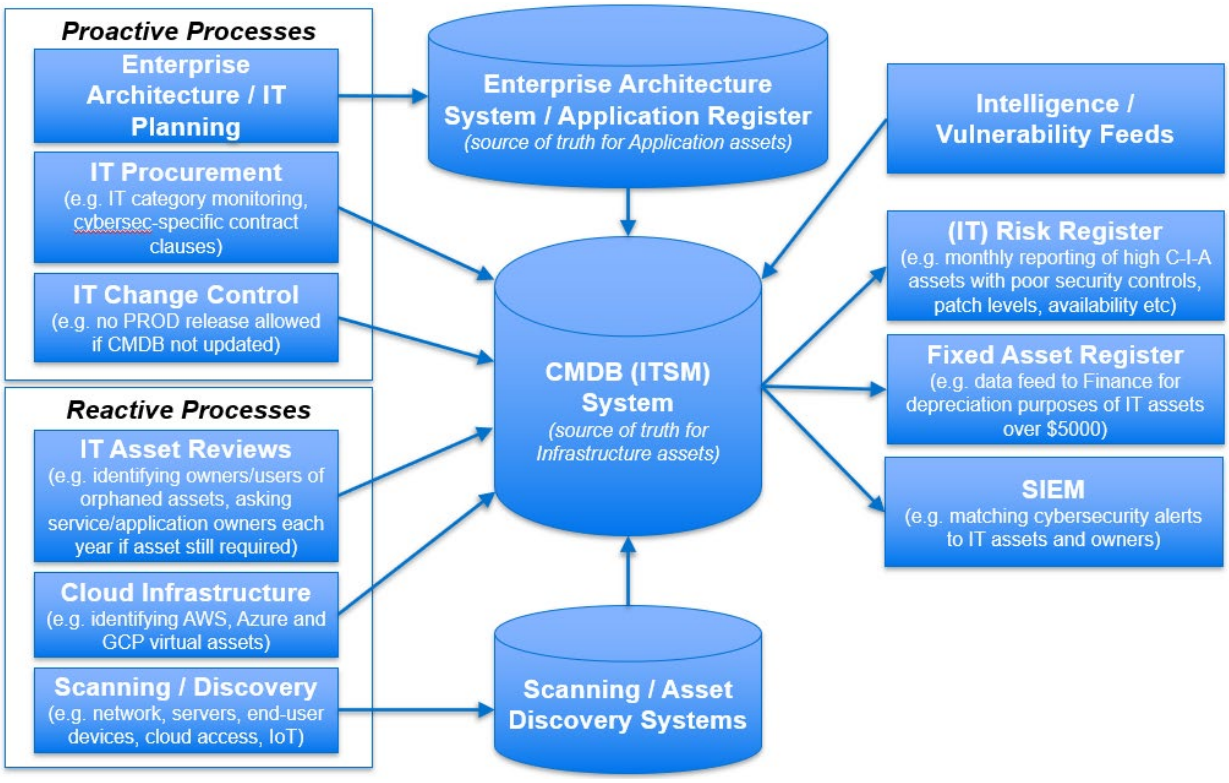
The health sector in Victoria currently uses ISO 31000: 2018 (VGRMF) / VPHS 2019 Consequence Ratings, a five level system with the following options: Catastrophic, Major, Moderate, Minor, Insignificant/Negligible.

Technology

The use of a Configuration Management Database (CMDB) is recommended for all organisations with more than 200 end users, as this has the following benefits:

- All IT asset data can be stored in one place (source of truth)
- Automated and semi-automated IT operational and IT asset management processes can be built around the IT asset data
- Data can be imported into and exported out of this database to other systems

Here is an example of a technology ecosystem for IT asset management:



Some organisations may wish to have their own CMDB, others may wish to share. In the context of a shared CMDB, each IT asset can be tagged with the department/agency that owns it, so access to the data can be restricted to just the owning department/agency.

The deployment of Standard Operating Environments across an organisation can also aid in managing assets and gathering information on assets in a standardised way.

Key Performance Indicators

The use of Key Performance Indicators by Victorian Government departments and agencies is highly recommended. Their use is critical in order to ensure that IT asset management is being performed to a level that can maintain good cyber security. This guidance categorises KPIs into the following areas:

- IT Asset Identification
- IT Asset Vulnerability Identification
- IT Asset Lifecycle Management
- IT Asset Monitoring
- IT Asset Security Patching
- IT Asset Basic Security Controls
- IT Asset Disposal

Please contact the Cyber Security Branch at vicgov.ciso@dpc.vic.gov.au to access the resource **WoVG IT Asset Management Cybersecurity KPIs** for a comprehensive list of cybersecurity related KPIs.

This list of KPIs includes a suggestion as to which **role** ("Example Responsible Party") in your organisation is responsible for each KPI. Note that the naming of these roles may be different, and that multiple roles may be fulfilled by the same person. If a role has been outsourced to a third party, the relevant KPIs against that role should be included in the **contract** with the third party (it is recommended that penalty clauses with recoup opportunities be included to ensure that the third party strives to meet the KPIs on an ongoing basis). If a role is fulfilled by a Victorian Public Servant, the KPI should be written into their **Performance Plan**.

Note that there are different suggested **Target Asset Coverage KPIs,** and **Minimum Process Frequencies** for IT assets being managed at "AMAF level 3 Competence" and "AMAF level 4 Optimising" levels of maturity.

The initial focus of implementing KPIs should be **visibility** i.e. an agency can start by measuring processes against the KPIs to see where they are at currently, and to identify missing processes and insufficient resourcing.

The recommended target KPIs may be adjusted by the WoVG IT Asset Management Working Group over time, if there is consensus that they are too high or too low, or where compensatory controls are in place. These recommended target KPIs are **currently not mandatory**. The final decision as to which target KPIs are applicable to an agency, and how high they should be, should rest with the agency's management and Audit and Risk Committee, and be based on risk.

Reporting

Ongoing reporting of IT asset management maturity and KPIs has the following benefits:

- Ensuring IT asset management processes continue to be run effectively on an **ongoing basis**, as it is very easy for them to degrade if they are not being managed and monitored
- Ensuring **process improvements** continue to be made until AMAF maturity and KPI targets have been reached
- Providing evidence of maturity to the VMIA and other cyber insurance providers to help achieve **reduced cybersecurity premiums**
- Enabling a smooth inclusion of the IT asset class into DTF's overall multi-asset class AMAF **assessment** and **attestation obligations**

Report Type	Reason	Target	Measurement	Suggested Reporting Frequency
AMAF Maturity Assessment – IT Asset Class *(Can feed up into dept/agency all asset class AMAF assessment)*	To understand **how mature** a dept/agency's IT asset management processes are at a medium level of detail (41 process areas)	All (100%) 41 processes at Competence (level 3) Relevant processes for relevant higher-risk IT assets at Optimising (level 4)	% of the 41 processes at Competence (level 3) % of the relevant 41 processes for relevant higher-risk assets at Optimising (level 4)	Every financial year for internal dept/agency IT Asset governance board and maturity improvement planning, Digital Victoria Cyber Security Unit visibility, and VMIA insurance re-pricing purposes Every three years as part of overall (all asset classes) AMAF assessment
IT Asset Management Process Frequency KPI Report	To understand **how often** IT asset management processes are run (for more than 100 discrete KPIs)	All (100%) relevant KPI processes run at Competence (level 3) frequency Relevant KPI processes for relevant higher-risk	% of the >100 KPI processes running at the target Competence (level 3) frequency % of the relevant KPI processes for relevant higher-risk assets	Every financial year for internal dept/agency operational monitoring and maturity improvement planning, Digital

		IT assets run at Optimising (level 4) frequency	running at the target Optimising (level 4) frequency	Victoria Cyber Security Unit visibility, and VMIA insurance re-pricing
IT Asset Management <u>Asset Coverage</u> KPI Score Report	To understand **how many** IT assets are being managed (more than 100 discrete KPIs)	All (100%) relevant Coverage KPIs meeting the target Competence (level 3) Coverage for relevant higher-risk IT assets meeting Optimising (level 4) KPIs	Average % of all the > 100 Coverage KPIs meeting the target Competence (level 3) KPIs Average % of the Coverage KPI for relevant higher-risk assets meeting the target Optimising (level 4) frequency	Every quarter for internal dept/agency operational monitoring Every financial year for Digital Victoria Cyber Security Unit visibility, and VMIA insurance re-pricing

Implementation

The following is a suggested (pro forma) IT asset management uplift plan that can be modified and re-arranged based on an individual department/agency's priorities and maturity. Note that each phase may take anywhere from a month for a smaller agency to up to say six months for a department/agency with a large asset fleet.

PHASE	People	Process	Data	Technology
Phase 1	Assemble ITAM **steering committee/governance board** (managers of relevant IT staff, risk and assurance, finance and procurement representatives) and allocate a senior ITAM sponsor (e.g. CIO/CTO) Hire an **accountable IT Asset Manager** or an ITAM Project Manager to manage the uplift process either through a project or BAU program of work Identity **staff roles** and shortages **Allocate processes** and KPIs to relevant staff **Train** relevant ITAM staff on AMAF and this guidance	Perform a **baseline maturity assessment** using AMAF (41 areas) Implement an **IT Change Control** CMDB update hook (e.g. no PROD release until the CMDB is updated) Implement an Enterprise Architecture **forward planning** process (minimum 12 months ahead)	Configure CMDB to the **WoVG standard fields** for Applications and Infrastructure Identify IT asset data shortcomings (priority is the data accuracy of BIL 3+ systems)	Start using a **modern CMDB** (ITSM) system (if not already) Implement **discovery/scanning tools** **Decommission** unused public websites/Domain Names **Decommission** unused and unsupported servers

PHASE	People	Process	Data	Technology
Phase 2		Do **baseline KPI assessment** against WoVG ITAM KPIs Achieve minimum WoVG KPIs for all **Essential 8**-related KPIs to Level 3 ("Competence") Implement **IT Procurement visibility** governance hooks (esp. to capture cloud and shadow assets)	Uplift **Application** data coverage and quality (including SaaS and shadow systems) Define **mappings** between IT assets Meet **End User Administration** minimum KPIs across all areas	Integrate ongoing **scanning data feeds** into CMDB Commence regular and automated **reporting** Identity **IaaS** platform accounts/tenants/subscriptions (e.g. AWS, Azure, GCP) inc. owners **Decommission** unused IaaS and SaaS services
Phase 3	**Reinforce the need** for ITAM responsibilities and improvements across the business through socialisation, awareness and reporting	Achieve **Security Patching** KPIs to Level 3 ("Competence") Achieve **Asset Disposal** KPIs to Level 3 ("Competence")	Uplift **Infrastructure** data coverage and quality	Implement ongoing **product Vulnerability** data import feeds Implement outgoing feed process to inject IT asset risks into IT and/or organisational **Risk Registers**

PHASE	People	Process	Data	Technology
Phase 4	Train relevant ITAM staff on SQL/ITSM reporting/advanced data analysis/**advanced ITSM/CMDB** configuration **Reinforce the need** for ITAM responsibilities and improvements across the business through socialisation, awareness and reporting	Implement **Application re-attestation** processes Achieve **lifecycle management** KPIs to Level 3 ("Competence") Achieve **Monitoring** KPIs to Level 3 ("Competence") **Repeat AMAF maturity assessment** to show improvements since uplift commencement	Achieve minimum (to Level 3 "Competence") WoVG ITAM KPIs for **Identification**, including Internet of Things/Operational Technology assets if relevant	Implement ongoing automated feed of IT asset reference data into **SIEM** system Expand reporting
Phase 5	Consider **cycling staff** around ITAM processes/jobs to avoid disengagement	Expand Enterprise Architecture/**forward planning** to a minimum of 3 years in advance Identify which assets need to be managed at a maturity of **Level 4 (Optimising)**	Enterprise architecture/ planning /technology investment decisions now based on the CMDB data as the **source of the truth**	Implement ongoing feed to inject one of **AWS, GCP or Azure** asset data into CMDB
Phase 6	**Reinforce the need** for ITAM responsibilities and improvements across the business through socialisation, awareness and reporting	Commence uplifting the ITAM processes supporting **more critical assets** to Level 4 "Optimising"	Identify **asset de-duplication** and **standardisation** opportunities based on business capabilities	Implement ongoing feed to inject one of **AWS, GCP or Azure** asset data into CMDB

PHASE	People	Process	Data	Technology
Phase 7	Ensure that ITAM processes and data are embedded into the organisation and maintained on an **ongoing basis**	**Achieve AMAF Level 4 "Optimising"** across all 41 areas and WoVG ITAM KPIs for the more critical assets		Implement ongoing feed from CMDB into the **Fixed Asset Register** for financial depreciation purposes

References

Reference	Description
ACSC	Australian Cyber Security Centre https://www.cyber.gov.au/
AMAF	Asset Management Accountability Framework https://www.dtf.vic.gov.au/infrastructure-investment/asset-management-accountability-framework
AWS	Amazon Web Services https://aws.amazon.com
Azure	Microsoft Azure https://azure.microsoft.com
BAU	Business As Usual
BIL(s)	Business Impact Level(s) for Confidentiality, Integrity and Availability, as per OVIC's VPDSS (https://ovic.vic.gov.au/data-protection/standards/)
CIA / C-I-A	Confidentiality, Integrity and Availability
CIO	Chief Information Officer
CMDB	Configuration Management Database
COBIT	Control Objectives for Information and Related Technologies https://www.isaca.org/resources/cobit
DJSIR	Department of Jobs, Skills, Industry and Regions https://djsir.vic.gov.au/digital-jobs
DTF	Victorian Department of Treasury and Finance
DV CSB	Digital Victoria's Cyber Security Branch https://www.vic.gov.au/cyber-security-victorian-government
GCP	Google Cloud Platform https://cloud.google.com
IaaS	Infrastructure as a Service

Reference	Description
ITAM	Information Technology Asset Management (IT Asset Management)
IT-CMF	IT Capability Maturity Framework https://ivi.ie/it-capability-maturity-framework/
ITIL	Information Technology Infrastructure Library https://www.axelos.com/certifications/itil-service-management
ITSM	Information Technology Service Management
ISO	International Organization for Standardization https://www.iso.org/home.html
KPI	Key Performance Indicator
OVIC	Office of the Victorian Information Commissioner https://ovic.vic.gov.au/
PaaS	Platform as a Service
PDP	Performance & Development Plan
SaaS	Software as a Service
SIEM	Security Information and Event Management
SLA	Service Level Agreement
Victoria's Cyber Strategy 2021	https://www.vic.gov.au/victorias-cyber-strategy-2021
VMIA	Victorian Managed Insurance Authority https://www.vmia.vic.gov.au/
VPDSS	Victorian Protective Data Security Standards https://ovic.vic.gov.au/data-protection/standards/
WOVG	Whole of Victorian Government