A guideline for managing risk from technology obsolescence

Technology Reform Priority

VICTORIA State Government | Premier and Cabinet

Document Control

Approval

This document was approved by CIO leaders at the September 2019 governance forum.

Applies to	All VPS departments and agencies	**Authority**	CIO Leadership Group
Period	2019 - 2022	**Advised by**	Digital Strategy and Transformation, Department of Premier & Cabinet
Issue Date	20/09/2019	**Document ID**	TECH-GUIDE-01
Review Date	01/07/2022	**Version**	3.0

Version history

Version	Date	Author	Description
1.0	21 June 2019	D. Cate Principal Advisor Enterprise Solutions	Document establishment in collaboration with the Assistant Chief Information & Security Officer.
1.1	24 June 2019	D. Cate Principal Advisor Enterprise Solutions	Updates post initial review
1.2	28 June 2019	D. Cate Principal Advisor Enterprise Solutions	Feedback from Cyber team, VMIA and readability updates. Final draft version for syndication.
1.3	8 July 2019	D. Cate Principal Advisor Enterprise Solutions	Feedback VMIA and readability updates.
1.4	9 July 2019	D. Cate Principal Advisor Enterprise Solutions	Feedback from the Acting Director of IT Strategy & Policy.
1.5	10 July 2019	D. Cate Principal Advisor Enterprise Solutions	Feedback from VMIA and Acting Director of Strategy & Policy.
1.6	23 July 2019	D. Cate Principal Advisor Enterprise Solutions	Feedback from VMIA and alignment review with DHHS Applications Register presented to the CIO Leaders forum 16 July 2019
1.7	25 July 2019	D. Cate Principal Advisor Enterprise Solutions	Review from Acting Director IT Strategy & Policy. Review by ESB communications team
1.8	5 August 2019	J. Green Senior Project Officer Enterprise Solutions	Minor amendments to structure and headlines.
1.9	19 August 2019	B. Baudoin Acting Director IT Strategy and Policy Enterprise Solutions	Review and updates

2.0	20 August 2019	D. Cate Principal Advisor Enterprise Solutions	Updates post review and style guide changes
2.1	5 September 2019	D. Cate Principal Advisor Enterprise Solutions	Updates post review from the Family Violence Technology Architecture Group
3.0	24 September 2019	D. Cate Principal Advisor Enterprise Solutions	Updates post the September 2019 CIO Leaders Group. Reviewed against the Victorian Government Asset Management Framework and Implementation Guide.

Contents

Introduction

Overview

This guide assists public sector organisations to identify, record and manage the lifecycle of their significant information technology systems then subsequently use these insights from their application's attributes to reduce the risk from systems/software obsolescence that can potentially pose a threat to service delivery continuity.

The guideline has been designed to promote a robust management practice to enhance enterprise-wide Information Technology (IT) business planning. IT planning forms part of each organisation's broader security considerations which aims to address threats and reduce the serious incidents that occur because of technology obsolescence.

This guide compliments existing Victorian Public Sector (VPS) standards and guidelines which Victorian Public Sector organisations must comply with.

Specifically, the Enterprise Solution's guide supports the Victorian Government's 2016 Asset Management Accountability Framework and the 2017 Asset Management Accountability Framework Implementation Guidance which sets out the policies, strategies, records management and risk management practices.

Public sector organisations are encouraged to perform an annual audit that records and assesses their IT applications. To implement an IT application repository, Enterprise Solutions recommends that this practice guide is leveraged to fast-track an audit.

This guideline sets out an approach to establish and maintain an IT application repository for the purposes of managing technology obsolescence.

Public Sector organisations are encouraged to design their specific implementations with standardisation in mind to promote data-sharing and cross-agency practices.

The benefits of standardisation will:

- support a technology evaluation of a machinery of government change
- effective management of WOVG cyber incident risks
- support technology service providers' IT service management functions
- aid the effective evaluation of medium to long term technology planning.

This obsolescence guide has been developed in consultation with Victorian Managed Insurance Authority (VMIA), the Victorian Government's insurer and risk adviser.

The guideline suggests a minimum of data to be captured and is intended for Victorian Public Sector use. Victorian Public Sector organisations should make an individual assessment of their requirements for managing their technology obsolescence, rather than solely relying on the advice within this document.

Rationale

The guide also acknowledges that an increasing number of cyber incidents are occurring, and IT obsolescence is a contributing factor.

Implementation will support executive management teams to adopt a risk-based approach to decision making thereby assisting them with:

- the management of increasing technology complexity
- the advancement of business cases for platform renewal investments
- the establishment of programmes[1] of work that address risk and remediation
- the management of ongoing arrangements with service providers software/hardware vendors.

Many Public Sector organisations have already taken appropriate steps to address technology obsolescence. However, the VPS can work better together and promote leading practices, tools, and methods.

The following technology-based registers already currently exist to record:

- information assets, an organisation's information asset register (IAR)
- public sector owned technology fixed assets e.g. depreciable assets
- configuration management databases (CMDB).

This guideline extends beyond these registers to capture technology planning insights about essential IT applications[2] and their associated relationships with the overall intent to improve an organisation's management of service delivery continuity.

An organisation's CMDB and IAR will provide input to an IT application's lifecycle and risk assessment.

Forrester have profiled the suite of Enterprise Architecture tools at March 2019[3]. These tools enable better technology planning across the whole technology ecosystem. However, some organisations may choose to custom build their own. For example, Department of Health and

[1] WOVG or agency specific

[2] See Appendix A – A conceptual Meta Model of an application repository.

[3] The Forrester Wave™: Enterprise Architecture Management Suites, Q1 2019, The 12 Providers That Matter Most and How They Stack Up

Human Services (DHHS) has developed their owned tools on existing platforms using SharePoint and PowerBuilder[4].

The advice in this guideline is designed to be continually updated to reflect leading practice in IT portfolio planning. It is informed through research of proven models deployed interstate and overseas, and through experience gained from testing and prototyping.

Commencement date

The commencement of this guideline begins from 1 October 2019.

[4] Please contact DHHS to gain further details

Derivation, Scope & Definition.

Derivation

This document has been derived from the Victorian Government IT Strategy 2016-2020 and the Victorian Government Cyber Security Strategy 2016-2020.

The document aligns with the Victorian Government's 2016 Asset Management Accountability Framework and the 2017 Asset Management Accountability Framework Implementation Guidance.

Scope

This document applies to whole-of-government (WOVG) departments and agencies.

The IT applications register excludes:

- information assets, however linkages can be appended if feasible
- end-user hardware does not form part of the IT applications register as it is separately recorded and managed as a depreciable fixed asset within financial management systems.

Audience

The audience for this document is senior executives of whole-of-government (WOVG) departments and agencies.

Glossary

The glossary of terms and abbreviations used in this document are defined in Appendix D.

Related documents, tools and references

Related documents and references have been notated in footnotes and the glossary.

Guideline usage

This guideline shares public sector leading practices and offers a standardised approach. Enterprise Solutions Branch will coordinate future updates based on the feedback from users.

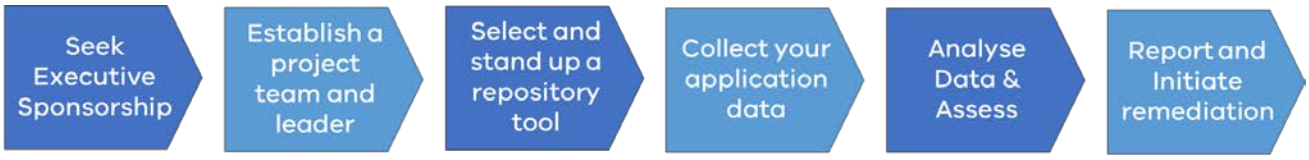
This repository will:

- identify systems that are becoming obsolete
- build an application record then rate the application or supporting technology to assess lifecycle planning
- assist IT professionals determine impacts on dependent applications and technologies when planning or undertaking change.

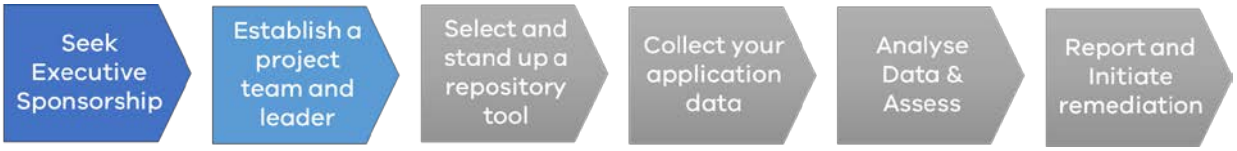
This guideline will support organisations to:

1. create an application inventory where the applications that support service delivery or operations are classified in a standard manner
2. assess and evaluate application records as part of an annual planning cycle
3. uncover insights that inform an IT roadmap, project scope or funding request to reduce IT obsolescence risk.

The following high-level process illustrates the six key steps to drive the audit outcome.



Sponsorship & the audit team



Undertaking an audit takes time. So, seek executive sponsorship to prioritise the establishment of a responsible team to implement and update the IT application repository.

A sponsor should be a senior executive as there is a significant investment to create the initial repository followed by ongoing review and maintenance.

Most organisations are much better at introducing new technologies than retiring them. The cost of running unsupported technology can be high. Costs of IT outages and data breaches can run into the millions of dollars.

At the end-of-life of technology becomes harder to manage IT managers may experience:

- integration issues
- limited functionality, low service levels
- lack of available skills in market
- limited support from vendors.

These factors form the justification to support a case for a sponsor to approve a project team to undertake the annual audit.

If there is an existing tool, or a register, it may be used to create the application repository, however if this is not present, a data collection spreadsheet has been included within this guideline to assist in building a register. See Appendix B.

Roles and responsibilities

A senior technology manager or architect is the best-skilled person to lead the project's audit team. An optimal project team would comprise of the resources outlined in figure 1.

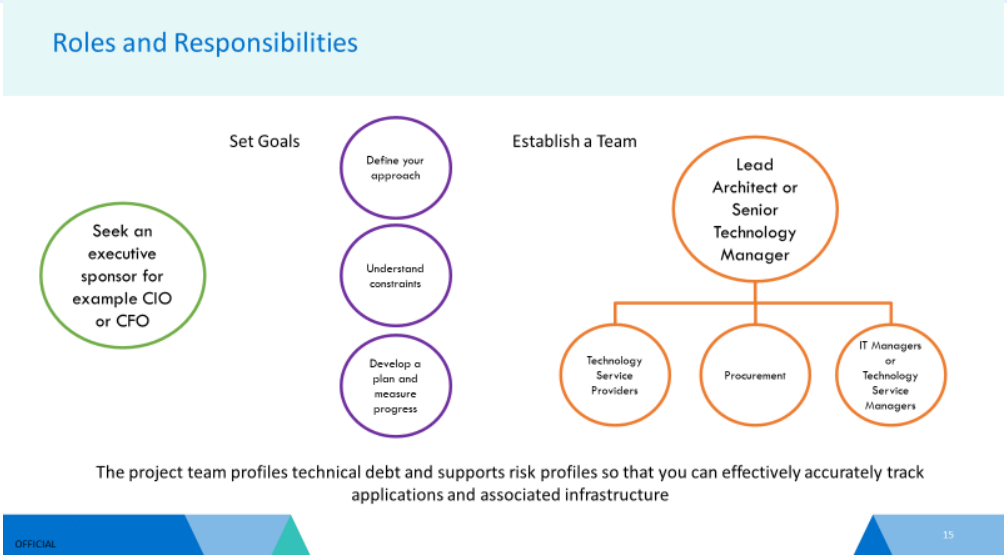


Figure 1: Sponsor, Goals and team composition

Ongoing maintenance of the repository

Post the initial audit, the project team will need to transition the ongoing maintenance of the repository to a responsible position within their organisation. This role will administer, update and make changes to the repository and be accountable for reporting.

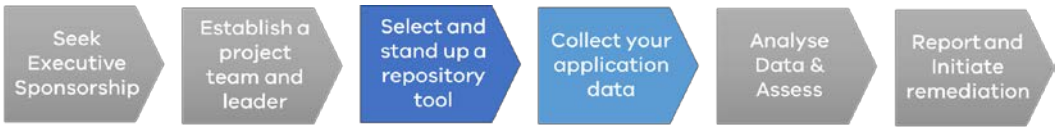
Specific responsibilities include:

- maintenance of ongoing updates of the register on an annual basis
- control access to the repository[5]
- risk reporting, actions and escalations
- modification and upgrading of the register to improve visibility and usability across an organisation
- representing an organisation as part of a WOVG practice community.
- input into any future proposed WOVG contracts for IT Portfolio Planning tools[6].

[5] Maintain the confidentiality, integrity and availability of the repository.

[6] Where Public Sector organisations have an appetite to enter into aggregated WOVG purchasing contract

Data collection



The data for applications and their technology components will exist in multiple sources. There will be numerous versions of the truth.

Enterprise Solutions recommends running several audit surveys to create an initial view of an application repository. Some examples include the following:

- surveys of existing service providers[7]
- extracting entitlements and contract obligations from internal procurement areas
- exploring electronic records management system for previous enterprise architecture artefacts or projects that have implemented new systems
- surveys of end users[8]
- assessing new projects that are implementing new applications.

When collecting an application's data, where possible define the relationship of an application to its supporting technology components, then capture the owner or custodian of the application — for example, this could be the named owner of software licences.

At minimum collect the data catalogued in the following sections. If needed a decision to collect more can be made. Ensure that all applications have been catalogued uniquely. See the glossary for definitions and values that are assigned to the record attributes.

The application's primary data fields

The following data is required for an application's source record:

- Name or alias.
- Description.
- Application status.
- Application location.
- Application hosting profile.
- Confidentiality rating.

[7] Service providers may have a CMDB and or an asset management register

[8] End users may have Business Managed IT (BMIT) see the glossary for the definition.

- Integrity rating.
- Protective markings.
- Availability rating.
- Disaster recovery rating.
- User profile.
- Application developer or operations provider (Dev Ops provider).
- Department or portfolio entity owner.
- Primary functional business user.

The application's technology profile data

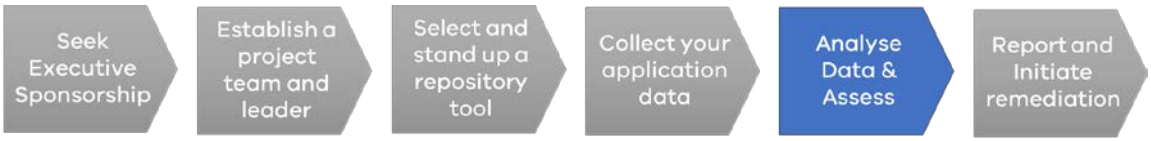
Matching the supporting technology components for each application is a challenging task. The technology profile relates to the infrastructure components that support the application. Note that infrastructure components can support multiple applications. So, there may be many applications operating on a single server.

Work closely with infrastructure services provider or infrastructure architects to populate a minimum set of data that will provide insights about the organisation's technology obsolescence position.

The following data is required for application records:

- Hardware profile.
- Hosting entity.
- Database profile.
- Operating system profile.
- Other key dependent technology components.

Assessment



Ensure that there are no duplicate records, no critical gaps, and the application's information is accurate. Classify each application record, to assign a business services zone, and perform a risk assessment for obsolescence and determine the application's lifecycle rating.

Assigning business services or functional zones

Business services zones are part of an enterprise framework used as a leading practice for IT planning.

Classifying each of the applications into business services zones and sub zones will provide the following benefits:

- the creation of collective insights and an overview of the technology landscape for the whole of enterprise
- the enablement of more straightforward communications
- the enablement of decision support for managing change
- the enablement of investment and planning for product rationalisation
- profiling of technology investments and costs.

Enterprise Solutions has developed a beta release of the business services zone framework (WOVG BZF)[9] for common cross-agency zones.

The initial framework is a useful starting point that adopts a hybrid approach synthesizing other public sector adaptations. It is anticipated that the WOVG BZF will continue to evolve with cross-agency input. The zones represent a cluster of logical business and technology services.

The WOVG BZF does not deep dive into agency-specific zones, as each will have individual needs. The government portfolio services zone layer in the framework, is a collective placeholder for agency specific applications. For example, the government portfolio services primary domain would record a student management system for the Department of Education and Training, a hospital monitoring system for the DHHS or a law enforcement assistance program for Victoria Police.

[9] See Appendix C

The following application's assessment data is required to append to records:

- The primary business zone.
- The sub business zone.

Assess and assign a technology risk rating

A technology risk exists when one or more of an application's supporting components is at the end of its life. When assessing the end of life status, the vendor, version and release number of the hardware and/or software must be known. Vendors periodically publish public statements about their products end of support. Contact vendors to understand the current and unsupported version of their products. Updates can be searched for online.

Servers, databases and operating systems can have different obsolescence cycles. Microsoft, Sparc[10], Windows[11], Oracle[12] and Sun Solaris[13] are examples of technology components.

The following risk data is required to append to an application record:

- Technology risk rating.

Assess and assign an application lifecycle rating

Applications are to be assessed in terms of their product lifecycles.

To undertake this assessment, use specific evaluation criteria on two dimensions: business value and technical quality. Based on this assessment, an application falls into one of the following quadrants illustrated in figure 2:

[10] https://en.wikipedia.org/wiki/Sun_Ultra_series

[11] https://en.wikipedia.org/wiki/List_of_Microsoft_Windows_versions and https://straightpathsql.com/archives/2017/01/sql-server-version-numbers/

[12] https://en.wikipedia.org/wiki/Oracle_Database#Releases_and_versions

[13] https://en.wikipedia.org/wiki/Solaris_(operating_system)

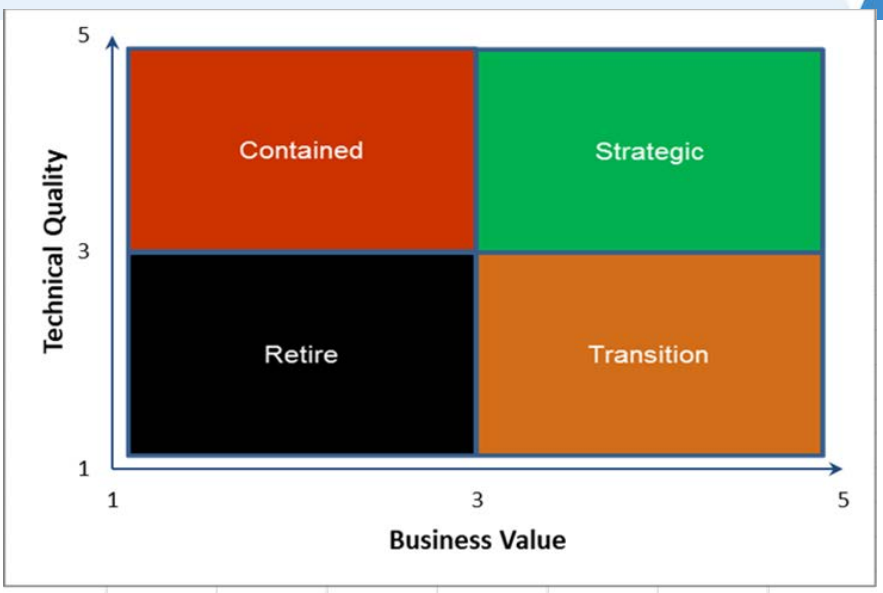


Figure 2 The application lifecycle rating states

An application lifecycle assessment tool is provided in Appendix B[14] which can be leveraged to assist in classifying applications.

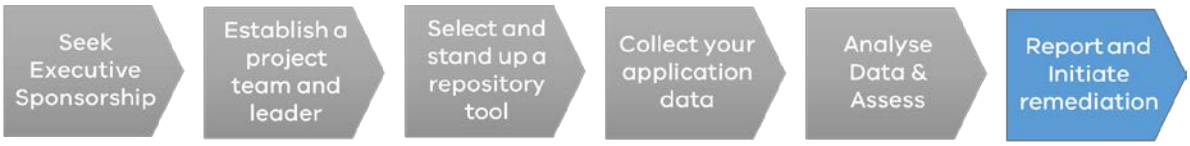
The assessment of individual applications will take time and may not be able to be completed as part of an initial implementation audit. If this is the case, then notionally rate an application lifecycle with the information available, then progressively undertake a more tourgoer application assessment to validate the initial assessment.

The following data is required to append to an application record:

- Application lifecycle rating.

[14] Adapted from the Victoria Police enterprise architecture assessment tool.

Annual application plan and reporting



The application roadmap plan reflects the insights collated from the lifecycle assessment and technology risk profile.

As part of the assessment phase, ensure “applications at risk” have been identified, for example:

- no disaster recovery environment for high availability rated applications
- high risk rating for obsolete technology components
- end of life applications.

Document the application’s plan and roadmap scenario, examples include:

- an identified project or incident response is currently underway that remediates the current risk position
- rationalisation candidate identified that indicates that the application / system will be transitioned or decommission by (insert planned date)
- a budget approval is required to uplift a critical disaster recovery environment
- replace application/system with alternative solution (e.g. existing strategic solution, or new commercial best of breed cloud solution)
- upgrade the specific component only to the latest possible version, i.e. upgrade/patch the existing application and/or infrastructure platform to latest possible versions.

For “at risk applications” see the annual risk reporting.

The following data is required to append to an application record:

- The application’s roadmap and plan.

Incident management & annual risk reporting

Obsolete software or hardware can pose a significant risk to Victorian government and the impact of incidents resulting from this can be severe.

Incident management

The repository can assist incident management in the following ways:

- when a cyber event materialises, to understand what has been compromised
- incident managers can get a greater sense of the associated complexities dependencies
- incident managers can develop better estimates of the recovery and remediation effort
- better considerations of data and privacy breaches and subsequent reporting requirements.

Where practical, repository administrators should leverage incident management reports as input to application lifecycle assessment tool.

Annual risk reporting

To proactively manage technology risk, Enterprise Solutions and VMIA have developed a risk reporting template. See Appendix B.

The risk template will ensure risks are appropriately managed and reported.

An illustrative example of a record within the IT application's repository[15]

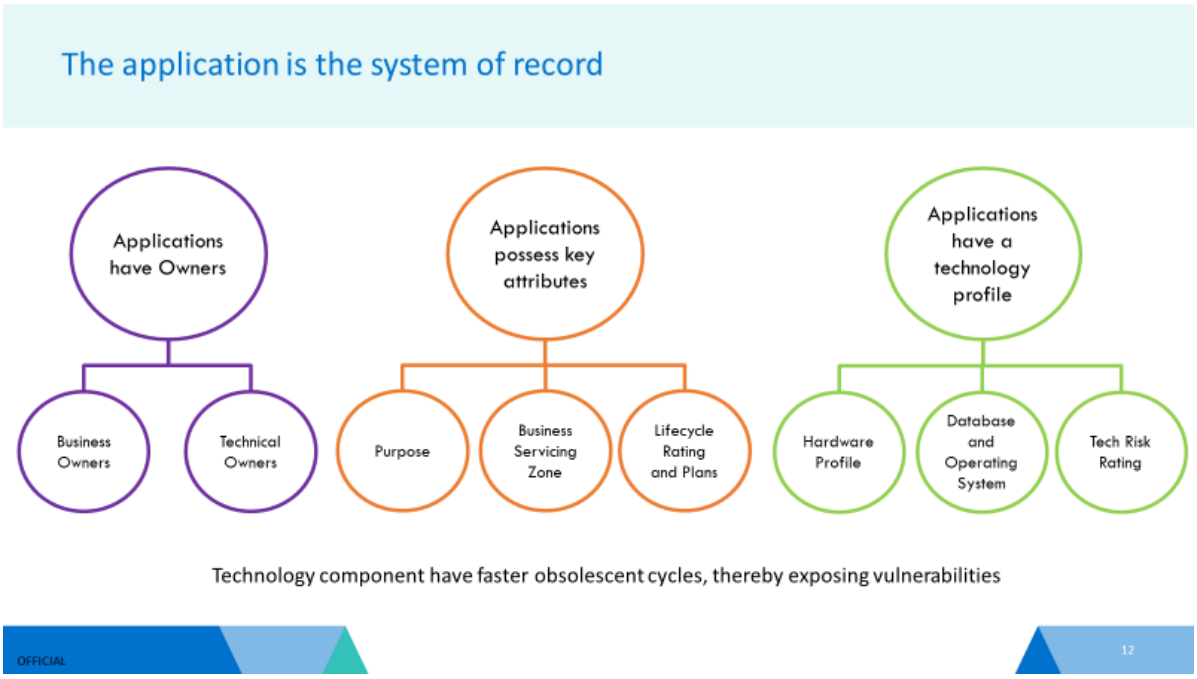
Field	Value
Application Status	Active
Application Name / Alias	Office 365 or O365
Description	A Microsoft office productivity application for mail, calendar, contacts, office tools and collaboration
Application Location	Melbourne
Hosting Profile	External
Confidentiality Rating	3 – Very High expected to cause harm/damage to ops/individuals
Integrity Rating	3 – Very High expected to cause harm/damage to ops/individuals
Protective Markings	Protected
Availability Rating	3 – Very High expected to cause harm/damage to ops/individuals
DR Rating	Available
User Profile	1200~ users
Support Profile	In-House
Department	DPC
Primary Business User	Enterprise
Hardware Profile	SaaS
Hosting Entity	Cenitex
Database Profile	Not Applicable
Hardware Profile	Not Applicable
Other Tech Components	Not Applicable
Primary Business Zone	IT Services
Sub Zone	Workplace

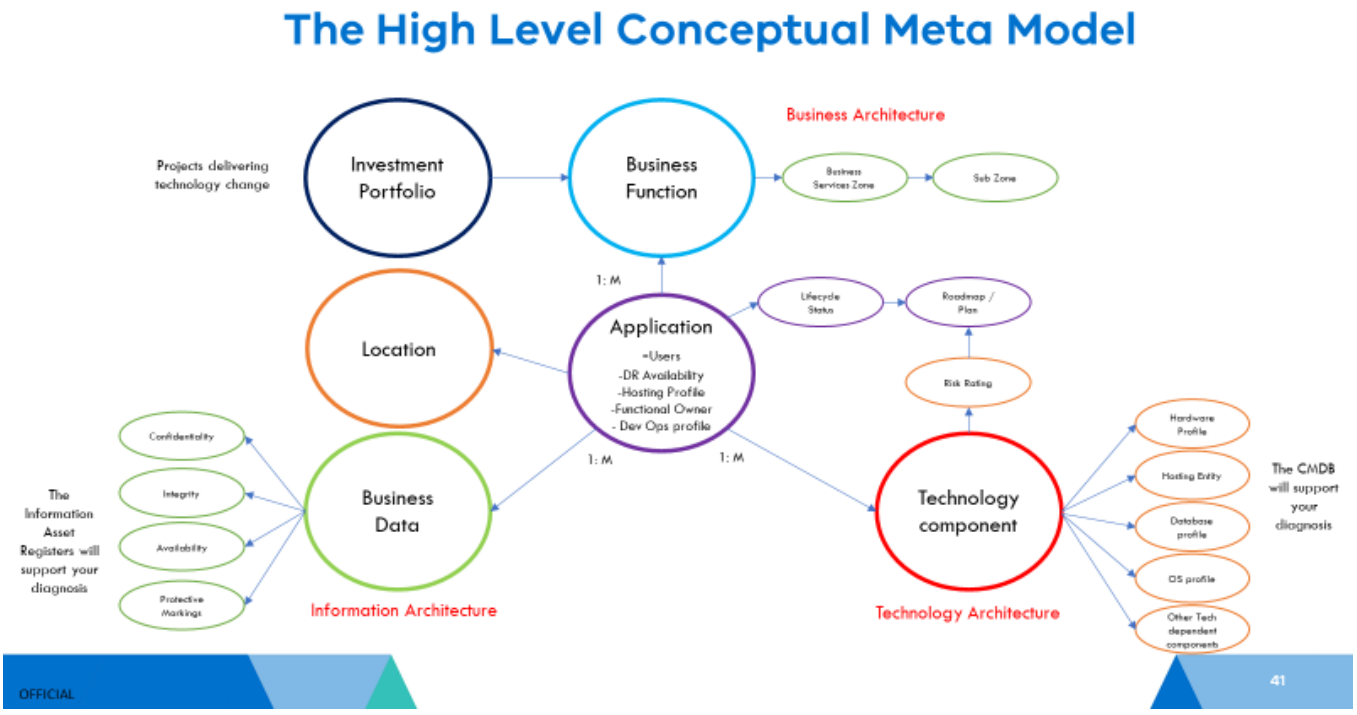
[15] Not actual DPC technology records but illustrative of what they may look like.

Tech Risk Rating	Low risk – N0
App Lifecycle Rating	Strategic
Roadmap	Extend and innovate

Field	Value
Application Status	Active
Application Name / Alias	Performance Development Plan (PDP)
Description	Employee performance management system that assesses objectives, behaviours and learning development.
Application Location	Melbourne
Hosting Profile	On-Premise
Confidentiality Rating	3 – Very High expected to cause significant harm/damage to individuals
Integrity Rating	2 – High expected to cause major harm/damage to individuals
Protective Markings	Protected
Availability Rating	1 – Low - Medium expected to cause limited/damage harm to operations
DR Rating	Available
User Profile	1200~ users
Support Profile	In-House
Department	DPC
Primary Business User	Enterprise and Human Resources
Hardware Profile	Physical
Hosting Entity	Cenitex
Database Profile	Domino DB version xx
Hardware Profile	Window OS version 10
Other Tech Components	Chrome Browser (not compatible with other browsers)
Primary Business Zone	Corporate or Common Government Services
Sub Zone	Corporate or Common Government Services - Human Resource Management
Tech Risk Rating	Medium risk – N-2 supported by HCL, via extended support contract.
App Lifecycle Rating	Retire
Roadmap	Archive and Decommission once migrated to SAP SuccessFactors by 2020.

Appendix A – The conceptual meta model of the repository





Appendix B – Enterprise Solutions tools and templates

The WOVG data collection spreadsheet

IT Applications Register - WOVG Te

The WOVG application lifecycle assessment tool

Application Framework_Applicat

The WOVG risk reporting template

The template has been jointly produced with VMIA.

Cyber and operational risks are to be extracted from the repository. The repository data will help organisations to complete the sample template.

Active applications with a lifecycle of retire and transition status are to be reported where technology risk rating is EOL and the total risk exposure rating is high to extreme based on the total Victorian Protective Data Security Standards (VPDSS) BILS risk exposure[16], that is the aggregate of confidentiality, availability and integrity exposure risk.

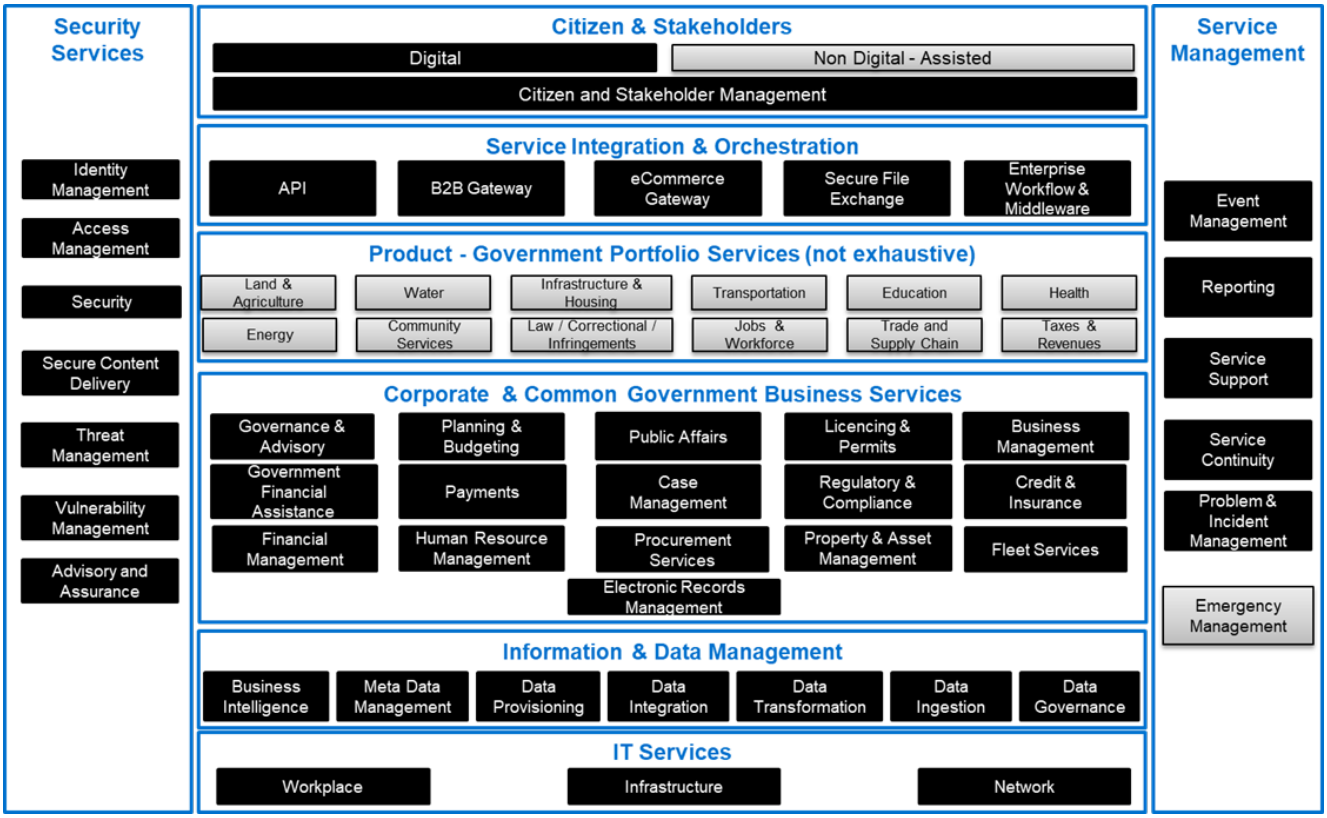
[16] https://ovic.vic.gov.au/wp-content/uploads/2018/08/VPDSF-Ch2-AppB-BIL-Table-V1.1.pdf

See the following table related to the total risk exposure score:

Aggregate Score	Exposure
11-12	**Extreme**: compromise of the information could be expected to cause serious harm/damage to government operations, organisations and individuals
9-10	**Very High:** Compromise of the information could be expected to cause significant harm/ damage to government operations, organisations and individuals
6-8	**High**: Compromise of the information could be expected to cause major harm/damage to government operations, organisations and individuals
3-5	**Medium**: Compromise of the information could be expected to cause limited harm/ damage government operations, organisations and individuals
1-2	**Low**: Compromise of the information could be expected to cause limited harm/ damage government operations, organisations and individuals
0	**No Risk**

WOVG IT
Obsolescence Risk F

Appendix C – A conceptual WOVG business zone framework



Appendix D - Glossary

General terms and definitions

Term	Description
Business Managed IT (BMIT)	Business unit or branched managed information technology (BMIT) are applications or systems that are not managed by the main IT function. Business units or branches have direct contracts with services providers outside the knowledge of the CIO function. Patching and support can be often overlooked. BMIT can introduce new risks to an organisation. Not recorded as an attribute in the repository but it should be appended to the application's description and document roadmap plans.
Configuration Management Database CMDB	Provides capabilities to identify, record, audit, and report on IT configuration items and their relationships.
Cyber Risk	A Cyber risk refers to a Cyber incident. A Cyber risk should be reported in annual risk reporting if an application has a technology risk rating of High risk EOL – unsupported
Cyber Security	There are various definitions used for the term cyber security. The Victorian government defines cyber security as measures relating to the confidentiality, availability and integrity of information and data that is processed, stored and communicated by electronic or similar means, protecting it and associated systems from an external or internal threat. Beyond these definitions, it is commonly recognised that cyber security involves the protection of critical information and IT infrastructure through alignment of people, processes and tools with shared security goals.
Cyber Security Incident	A cyber security incident is an occurrence that actually or potentially results in adverse consequences to (adverse effects on) (poses a threat to) an information system or the information that the system processes, stores, or transmits and that may require a response action to mitigate the consequences.
Data Sovereignty	The simplest description of data sovereignty refers to the fact that data stored digitally with a cloud service provider may be stored overseas and is, therefore, subject to the jurisdiction of more than one country. This situation can occur when a business uses a foreign or local cloud service provider. For example, a local service provider may, in fact, be a branch office of a company based elsewhere. Its head office handles all billing, but data is being sent and stored overseas. The data can include all kinds of information including credit card details, health records, personal information and financial records.

Term	Description
	The reason that data sovereignty matters is that it raises questions concerning: • compliance with privacy obligations • data protection and security • notification of data breaches.
Emerging (platforms) Technology	Emerging platforms are new technology developments and business models for which have yet to be scaled or matured. Emerging platforms are often incubated. These platforms offer high business value and potentially low technical maturity. Emerging technology platforms will usually be rated as transitional. Emerging technology platforms may create an operational risk if they are deployed without the appropriate environments and support arrangements.
Cyber Risk	A cyber risk refers to a Cyber incident. A Cyber risk should be classified in annual risk report if an application has a technology risk rating of High risk EOL – unsupported
Operational Risk	An operational risk refers an application that has a high availability requirement but has disaster recovery rating of either under development, not started or not yet assessed. An operational risk should be classified and captured in annual risk reporting.
Technology Obsolescence	This term relates to both applications and their technology components. Drivers for obsolescence include: • technology applications/systems that face unprecedented change, which cannot keep pace of user needs. Business cycles and workstreams are getting faster, so applications need to be continuously modernised. Legacy technology assets can constrain: the delivery of faster outcomes or creating richer experiences for citizens and employees • technical skills required to support the system are no longer available or becoming too expensive • the application/system scalability has reached its practical limits • the system's architecture is harder and harder to maintain, with too many patches (software upgrades) needed to sustain its continued operations • the software or hardware vendor announces to the marketplace that their older versions of their product can no longer be maintained.
Whole-of-Victorian-Government (WOVG)	For the purpose of this guide, this term relates to all Victorian Government organisations – encompassing public sector employer bodies.

Application repository terms, definitions & values

Term	Description	Repository Values if applicable
Application Description	A short description of the application and its purpose, including any names assigned by business users, including any references notated within configuration management databases.	Free Text.
Application Hosting Profile	The location of infrastructure that hosts an application. Externally hosted applications do not reside within an organisation's data centres. A third-party data centre hosts external application on a public cloud[17]. See the data sovereignty definition. A private cloud is internally hosted. The infrastructure architecture of a private cloud is designed to operate like a public cloud. Private clouds may also be referred to as enterprise clouds. Hybrid — the combination of internal and external cloud-based services.	The application hosting model can be either: • On-premises. • External - locally hosted. • External - Internationally hosted. • Hybrid.
Application Lifecycle Rating	The application lifecycle is the overall process of developing, implementing and retiring the system through a multi-step process. The ratings are assessed as follows: • Strategic - High business value and technology quality. • Transition - Low business value and high technology quality • Contain – High business value and low technology quality. • Retire - Low technology quality and business value.	The lifecycle rating is one of the following values: • Strategic. • Contain. • Transition. • Retire.

[17] https://www.bmc.com/blogs/saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose

Term	Description	Repository Values if applicable
	Lifecycle ratings are further explained below: **Strategic** applications possess the following characteristics: • Technology is pervasive across the enterprise and industry, and product vendor is a major player or market leader. • Product provides a sustained competitive advantage. • All system components are highly scalable and adaptive technology. • All system components are within one major iteration. • All system components are adaptive and interoperable with other major platforms. **Contained** applications possess the following characteristics: • System provides reliable operations. • System is considered cost-effective to maintain and operate in the near term. • System components are within two or three major iterations of latest version. • System components are adaptive to a single platform with minimal cross platform adaptability and may requires heavy customisation to meet new business requirements. • The application is not extensible or scalable to other parts of the enterprise. • The application has been surpassed by superior products in the marketplace. **Transition** applications have not yet scaled across the enterprise. The application as a target state is unclear. Transition applications possess the following characteristics: • New projects that is delivering emerging technology. • Application support is in hyper-	

Term	Description	Repository Values if applicable
	care by the project team. • Meets and supports fundamental business requirements for limited number of use cases. • Infrastructure component are on current releases. • Marketplace skills are easily accessible to develop and maintain the application. • Extended vendor support is available, if needed. • Infrastructure component is adaptive to a single function with reduced or limited functionality. Transition applications will evolve via the following scenarios: • If scaled across the enterprise as a target, the application lifecycle will mature to strategic status. • If the application has progressed into production and no further projects will extend the application to deliver enterprise-wide functions, then the application lifecycle will mature to contained status. • If the project implementing the emerging platforms fails and perishes, the application will be orphaned then the lifecycle will mature to retire status. **Retire** applications possess the following characteristics: • Limited functionality and users. • High maintenance cost. • Lack of agility to support business operational changes. • Limited skills in the marketplace to upkeep the application. • Application or Infrastructure component is at 'End of Life' (EOL). • Nearing end of extended support (within 6 months) or no extended vendor support available. Infrastructure component is un-adaptive technology (legacy) and cannot be integrated.	

Term	Description	Repository Values if applicable
Application Location	The location or site of the applications. Some applications may be deployed regionally.	Free text.
Application Name or Alias	The full name that has given to the application. Often an application will be known by an alias. It might have an acronym. Sometimes this is stored in the configuration management database. Notate if this is BMIT.	Free text.
Application Roadmap Plan	The documented plan recorded in the register that addresses risk	Free text field.
Availability Rating	VPDSF[18] rating as per the BILS table for the data hosted within the application. The application record should record the highest availability rating as the default position. The availability rating should reflect the disaster recovery position. An organisation's Information Asset Register should be referenced to reverse engineer the relationship of data to applications.	0 = Negligible: expected to cause insignificant harm or damages to ops & individuals. 1 – Low-Medium: expected to cause limited harm or damage to ops & individuals. 2 – High: expected to cause major harm/damage to ops & individuals. 3 – Very High: expected to cause significant harm/damage to ops & individuals. 4 – Extreme: expected to cause severe harm/damage to ops & individuals.
Application Status	The application is either active, in the progress of being decommissioned or decommissioned.	Active - assessed. Active – not yet assessed. Inactive – Decommissioned

[18] OVICs Victorian Protective Data Security Framework (VPDSF) BIL table.

Term	Description	Repository Values if applicable
Confidentiality Rating	VPDSF rating as per the BILS table for the data hosted within the application. The application record should record the highest confidentiality score as the default position. The Information Asset Register should be referenced to reverse engineer the relationship of data to applications.	0 = Negligible: expected to cause insignificant harm or damages to ops & individuals. 1 – Low-Medium: expected to cause limited harm or damage to ops & individuals. 2 – High: expected to cause major harm/damage to ops & individuals. 3 – Very High: expected to cause significant harm/damage to ops & individuals. 4 – Extreme: expected to cause severe harm/damage to ops & individuals.
Database Profile	The database (DB) will reside on hardware servers. The database is the structured or organised collection of information that may be accessed by the application. For SaaS, PaaS or IaaS the repository value is Not Applicable.	Record the Database vendor, the version and release number. E.g. • SQL Server 2005. • Oracle Database 10g Release 1 version 10.1.0.2.
Department or Portfolio Entity owner	The name of the department, agency, body or public entity that owns the application.	Free Text.
Dev / Ops Provider	The service provider that supports the application functionality development, upgrades and the first line of support should the application fail. Dev / Ops could be an in-house development and support team or a third-party provider. The application support provider is usually different than the entity or body that hosts the infrastructure to support the application. If internally managed, the Dev Ops provider will be “in-house.”	Free Text.
Disaster Recovery Rating	Disaster recovery (DR) reflects an agreed service level recovery of an application when it fails. The DR rating demonstrates the status of the environment to support	An application ‘Disaster Recovery Status’ can be in one of the following states: • Available.

Term	Description	Repository Values if applicable
	recovery.	• Under Development. • Not Started. • Not Yet Assessed. • No Business or Regulatory Need.
Hardware Profile	Hardware profile has a direct relationship to the application hosting profile. The hardware profile is more specific. Internally hosted will be classified as physical or virtualised Externally hosted will be either Software as a Service (SaaS), Platform as a Service (PaaS) or Infrastructure as a Service (IaaS).[19]	Hardware profile is one of the following values: • Virtualised. • Physical. • SaaS. • PaaS. • IaaS.
Hosting Entity	The name of the contracted technology government service provider that supports the application's hardware, database, operating system and other key technology components. For SaaS, PaaS or IaaS, the software provider will be the hosting entity.	Free Text.
Integrity Rating	VPDSF rating as per the BILS table for the data hosted within the application. The application record should record the highest integrity rating as the default position. The Information Asset Register should be referenced to reverse engineer the relationship of data to applications.	0 = Negligible: expected to cause insignificant harm or damages to ops & individuals. 1 – Low-Medium: expected to cause limited harm or damage to ops & individuals. 2 – High: expected to cause major harm/damage to ops & individuals. 3 – Very High: expected to cause significant harm/damage to ops & individuals. 4 – Extreme: expected to cause severe harm/damage to ops & individuals.

[19] https://www.bmc.com/blogs/saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose

Term	Description	Repository Values if applicable
Operating System Profile	The operating system (OS) is software that manages computer software resources and provides common services for computer programs.	Record the OS vendor, the version and release number. E.g. • Sun Solaris 2.3, OS 5.3. • Windows Server 2003 R2.
Other key dependent technology components – sometimes classified as compute technologies	Other than databases and operating systems, the application may have different key dependent components such as middleware, web servers etc., that are not a separate system. If these components break or become obsolete, then the application can cease to function. Examples include .Net Servers, WebSphere App Servers, Tibco integration, Mercator integration broker, Domino Servers, Tivoli Directory Server, Form builders etc.	Record each component the vendor, version and release number.
Primary Business Zone	The highest representation of business and technology services within the WOVG BZF. See Appendix C.	Primary business zone is one of the following values: • Security Services. • Citizens and Stakeholders. • Service Management. • Service Integration. • Agency Portfolio Services (the name of the relevant portfolio). • Corporate or Common Services. • Information and Data. • IT Services.
Primary Functional Business User	The business unit within the department or portfolio that has accountability and authority over the application, e.g. Finance	Free Text.
Protective Markings	VPDSF rating for the data hosted within the application. The application record should record the highest protective markings as the default position. The Information Asset Register should be referenced to reverse engineer the relationship of data to applications.	Protective markings are one of the following values: • 1: Official. • 2: Official – Sensitive. • 3: Protected. • 4: Secret.

Term	Description	Repository Values if applicable
Sub Business Zone	A lower level representation of business services zones within the WOVG BZF See Appendix C.	Sub business zone is one of the following values: • Citizens and Stakeholders - Digital Facing. • Citizens and Stakeholders - Non-Digital. • Citizens and Stakeholders – Management. • Service Orchestration and Integration – API Gateway. • Service Orchestration and Integration - B2B Gateway. • Service Orchestration and Integration - eCommerce Gateway. • Service Orchestration and Integration - Secure File Exchange. • Service Orchestration and Integration - Enterprise Workflow / Middleware. • Portfolio Agency Service - Land and Agriculture. • Portfolio Agency Service – Water. • Portfolio Agency Service – Energy. • Portfolio Agency Service - Community Services. • Portfolio Agency Service - Infrastructure and Housing. • Portfolio Agency Service - Law/ Corrections / Infringements. • Portfolio Agency Service - Emergency Managemen.t • Portfolio Agency Service – Transportation. • Portfolio Agency Service - Jobs and Workforce. • Portfolio Agency Service – Education. • Portfolio Agency Service - Trade and Supply Chain. • Portfolio Agency Service – Health. • Portfolio Agency Service - Revenue / Taxes. • Portfolio Agency Service - Sports / Arts. • Portfolio Agency Service – Regulator.

Term	Description	Repository Values if applicable
		• Portfolio Agency Service - Central Government. • Portfolio Agency Service – Other. • Corporate or Common Government Services - Governance and Advisory. • Corporate or Common Services - Government Financial Assistance. • Corporate or Common Government Services - Planning and Budgeting. • Corporate or Common Government Services – Payments. • Corporate or Common Government Services - Human Resource Management. • Corporate or Common Government Services – Finance. • Corporate or Common Government Services - Public Affairs. • Corporate or Common Government Services - Case Management. • Corporate or Common Government Services - Procurement Services. • Corporate or Common Government Services - Electronic Records Management. • Corporate or Common Government Services - Licensing and Permits. • Corporate or Common Government Services - Regulatory and Compliance. • Corporate or Common Government Services - Property and Asset Management. • Corporate or Common Government Services - Business Management. • Corporate or Common Government Services - Electronic Records Management. • Corporate or Common Government Servic.es - Credit and Insurances. • Corporate or Common Government Services - Fleet

Term	Description	Repository Values if applicable
		Management. • Information and Data Management - Business Intelligence. • Information and Data Management - Meta Data Management. • Information and Data Management - Data Provisioning • Information and Data Management - Data Integration. • Information and Data Management - Data Transformation. • Information and Data Management - Data Ingestion. • Information and Data Management - Data Governance. • IT Services - Workplace and End User Computing. • IT Services - Infrastructure Services. • IT Services - Network and Telecommunication Services. • Security Services - Identity Management. • Security Services - Access Management. • Security Services - Secure Content Delivery. • Security Services - Threat Management. • Security Services - Vulnerability Management. • Security Services - Advisory and Assurance. • Service Management - Event Management. • Service Management – Reporting. • Service Management - Service Support. • Service Management - Service Catalogue. • Service Management – Continuity. • Service Management - Problem and Incident Management.
Technology Risk	Technology currency risk rating is the highest risk rating associated with any	The technology risk rating is one of the

Term	Description	Repository Values if applicable
Rating	obsolete technology component supporting the application. Technology currency risk rating pertains to the assessment of obsolescence within the applications supporting technology components that can lead to their end of life. A technology component falls behind a significant release, e.g. N-1 or has a hyper-care arrangement with a vendor's extended support before it becomes unsupported or obsolete. The term 'unsupported' refers to the situation where vendors (or communities in the case of some open source software) no longer provide patches, updates or other technical support services for the product in question. In these situations, the Victorian government currently bears the full burden of risk associated with running unsupported software. These risks include: • Software with known vulnerabilities are often compromised exposing the related data to easy exploitation. • Decreased agility resulting from its inability to align with changes in business requirements. • Lack of capacity to integrate with up-to-date technologies. • Limited or scare skilled resources to maintain unsupported technologies.	following values: • N-0 - No Risk Current Release. • N-1 - Low Risk 1 Version behind current major release. • N-2 - Medium Risk 2 Versions behind current major release. • EOL -High Risk Mainstream vendor extended support. • EOL -High Risk Unsupported.
User Profile	The number of users that may be impacted via an incident or loss of availability (internal and external). Licencing data may provide an indicative view of the user base.	Number.