CITIPOWER

INFORMATION AND COMMUNICATIONS TECHNOLOGY

INFRASTRUCTURE REFRESH

CP BUS 6.04 – PUBLIC

2026–31 REGULATORY PROPOSAL

Table of contents

1. Overview

IT infrastructure forms the foundation of our technology ecosystem, encompassing the hardware, software, networks, and systems required to deliver and manage IT services. It provides the necessary digital backbone for efficient management, monitoring, and optimisation of our operations, including the reliable and secure operations for our operating technology (OT) systems and customer interactions. Our IT infrastructure enables critical functions such as data processing, storage, communication and security, supporting the operation of applications and services across the business.

Investment is needed to maintain our IT infrastructure in the 2026–31 regulatory period with regard to both shorter-term asset lifecycles and longer-term drivers such as adapting to evolving technology needs and managing market obsolescence.

We have considered four infrastructure options to best meet our short term and long term needs:

1. **Base case (maintain existing infrastructure)**: this option implements a regular and structured lifecycle management approach to updating our IT infrastructure, consistent with our existing management practices (i.e. do-nothing different). That is, it continues a traditional on-premise infrastructure model that updates IT infrastructure beyond vendor recommended upgrade dates where possible.
2. **Maintain existing infrastructure with more frequent upgrades**: this option implements a regular and structured lifecycle management approach to updating our IT infrastructure, continuing on a traditional on-premise infrastructure model. Rather than prolonging lifecycles beyond recommended dates, this option will update 100% of IT infrastructure forecast to be out of vendor support by 2031.
3. **Criteria-based IT infrastructure refresh**: this option will evolve the implementation of our IT infrastructure to support growing operational and information technology workloads[1] using a criteria-based approach to optimise hosting solutions.
4. **Public cloud infrastructure refresh**: this option will evolve the implementation of our IT infrastructure to support growing operational and information technology workloads, with solutions favouring use of the public cloud.

Option three is our recommendation option. By strategically selecting the most appropriate hosting solution we are able to select the hosting solution that best matches the requirements of the workload. This will optimise infrastructure management and sustain stable operations as utilisation of technology to support network operations continues to outgrow our traditional on-premise physical infrastructure approach.

[1] Workload – refers to the set of tasks, processes, or applications that require computing, storage, and network resources to operate within an IT environment.

TABLE 1 OPTION SUMMARY ($M, 2026)

#	OPTION	CAPEX	OPEX	NPV
1	Maintain existing infrastructure	45.3	-	-
2	Maintain existing infrastructure with more frequent upgrades	54.5	3.1	246.7
3	Criteria based IT infrastructure refresh	45.0	10.0	289.8
4	Public cloud infrastructure refresh	25.3	36.4	281.2

Note: This includes costs and benefits for both CitiPower and Powercor

2. Background

IT infrastructure forms the foundation of our technology ecosystem, encompassing the hardware, software, networks, and systems required to deliver and manage IT services. It provides the necessary digital backbone for efficient management, monitoring, and optimisation of our operations, including the reliable and secure operations for our operating technology (OT) systems and customer interactions.

For example, our IT infrastructure supports the operation of applications and services across the business, including:

- **monitoring and control:** IT infrastructure enables real-time monitoring and control of various elements within the distribution network. Through sensors, smart meters, and supervisory control and data acquisition (SCADA) systems, operators can remotely monitor parameters like voltage, current, and power quality. This capability allows for proactive maintenance, rapid response to faults, and overall system reliability.
- **data management and analysis:** the volume of data generated by our network is substantial. IT infrastructure facilitates the collection, storage, and analysis of this data. Advanced analytics and machine learning algorithms can process this data to predict demand patterns, optimise energy flows, and improve network efficiency. This data-driven approach enhances decision-making and planning for network operators.
- **security:** as our infrastructure becomes more digitised, ensuring our foundations are modern, safe and secure is paramount. Prudent lifecycle maintenance of infrastructure hardware and technologies is not only important from a reliability perspective, but also a cyber resilience standpoint (noting that specific cyber security capabilities, such as firewalls, are considered in our separate cyber security business case).
- **customer engagement:** IT infrastructure facilitates communication with end-users through smart meters and customer portals. As we share more network data with market participants, underlying infrastructure and integrations will facilitate the data flows. Our customer-facing applications and portals are supported by on-premise or cloud infrastructure solutions.

2.1 Current infrastructure environment

Our current IT infrastructure comprises more than 3,000 hardware components across various data centres, depots, offices and buildings. A summary of these components is set out in table 2

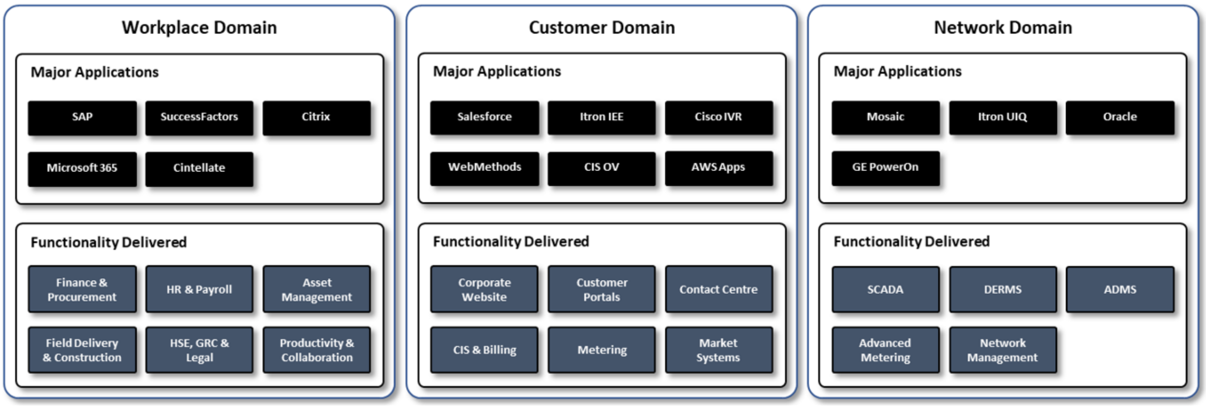
TABLE 2 CURRENT INFRASTRUCTURE COMPONENTS

CATEGORIES	COMPONENTS	DESCRIPTION
Data networking	• Application delivery • Fabric extenders • Load balancers • Routers • Switches	Ensures reliable connectivity, traffic flow optimisation, workload balance and enhanced scalability while maintaining data protection. These components work together to support communication within and between networks and ensures high availability and performance for critical applications
Storage	• SAN/NAS • SAN switches • Backup	Enables access, management, and protection of critical information. These technologies ensure high-speed data transfer, centralised storage and redundancy for data integrity and disaster recovery
Compute	Virtualisation Wintel/linux hardware and operating systems Other UNIX hardware and operating systems	The combination of these technologies provides the framework for processing data and running numerous IT applications. The elements provide processing power to run applications and execute tasks
Cloud	Cloud platform	Multiple AWS organisations supporting various applications and services

Our IT infrastructure also enables 500+ applications (including the functionality delivered by their associated applications) that support our network operations. These applications are broadly broken down into three key domains:

- **workplace domain**: applications that focus on our internal business operations and ensure we are able to efficiently and effectively manage our finances, payroll and asset management among other functions
- **customer domain**: applications that relate to our customers, such as providing customer data and billing as well as market systems to ensure compliance
- **network domain**: applications that monitor and interact with our network, ensuring safe and reliable supply is maintained.
- Some of the major applications and the associated functions they deliver are presented in figure 1. A failure in underlying infrastructure can cause a downstream issue in any of these functionalities.

FIGURE 1 CURRENT APPLICATION LANDSCAPE



2.2 Infrastructure hosting considerations

IT infrastructure hosting refers to how an organisation manages and operates the physical and digital resources needed to run its IT systems and applications. There are several hosting options available, each suited to different needs and levels of control, cost, and scalability.

2.2.1 On-premises hosting

On-premises hosting is how the majority of our infrastructure is currently structured. We own and operate servers, storage, and networking equipment across two centralised locations. This approach enables full internal control over infrastructure but relative to other approaches, incurs higher asset replacement costs.

2.2.2 Cloud infrastructure

Public clouds provide infrastructure resources (like servers and storage) but are managed by a third-party cloud service provider and delivered over the internet. With public cloud hosting, infrastructure is owned and managed by the cloud provider. This type of service is generally provided on a subscription basis and treated as operating expenditure.

A private cloud consists of cloud computing resources used exclusively by one organisation. The private cloud would be physically located at a business' dedicated data centre.

In a private cloud, the services and infrastructure are always maintained on a private network and dedicated solely to one organisation. For this reason, private clouds are often used by government agencies, financial institutions and other entities with business-critical operations seeking enhanced control over their infrastructure while providing scalability and flexibility benefits inherent in cloud services.

Within the cloud hosting solutions, there are also options as to what services are provided, these are generally categorised as:

- **infrastructure as a service (IaaS):** where traditional compute, storage and networking infrastructure is provided through an 'on-demand' service that is scalable. IaaS can be delivered both on-premises or in the public cloud
- **platform as a service (PaaS):** this moves up the technology stack and provides services related to databases, application integration, artificial intelligence (AI) and application hosting through an 'on-demand' scalable service. This is traditionally deployed manually on top of IaaS
- **software as a service (SaaS):** this is a fully managed, turnkey, end-to-end application with all underlying technology and software managed by a third party. While convenient, this option

reduces the level of customisability, as business processes are often required to be reconfigured to match the capabilities of the SaaS.

2.3 Shared IT systems

This business case covers IT expenditure related to both CitiPower and Powercor. Due to long term common ownership of these distribution businesses, over time we have brought together CitiPower's and Powercor's IT systems to enable the lowest cost delivery of our IT requirements. For example, when we are required to make changes to our business processes we are only required to make these changes once, rather than having to make similar changes across two separate IT systems.

3. Identified need

Historically, we have run the majority of our IT infrastructure on-premise. This current technology set-up has effectively ensured safe and reliable electricity services for customers over the past decade.

However, managing and adapting this infrastructure is growing increasingly complex due to evolving market options, industry demands and internal needs. As we increase reliance on technology to support network operations, market processes and customer interactions, we need agile, flexible and efficient hosting models.

The identified need, therefore, is to maintain our IT infrastructure in the 2026–31 regulatory period with regard to both shorter-term asset lifecycles and longer-term drivers such as adapting to evolving technology needs and managing market obsolescence.

3.1 Asset refreshment cycles

While specific IT components each have their own vendor-recommended lifecycles, most of our IT infrastructure is replaced every four to six years. For example, approximately 78 per cent of our infrastructure hardware will be beyond its typical refresh cycle in the 2026–31 regulatory period if not refreshed.

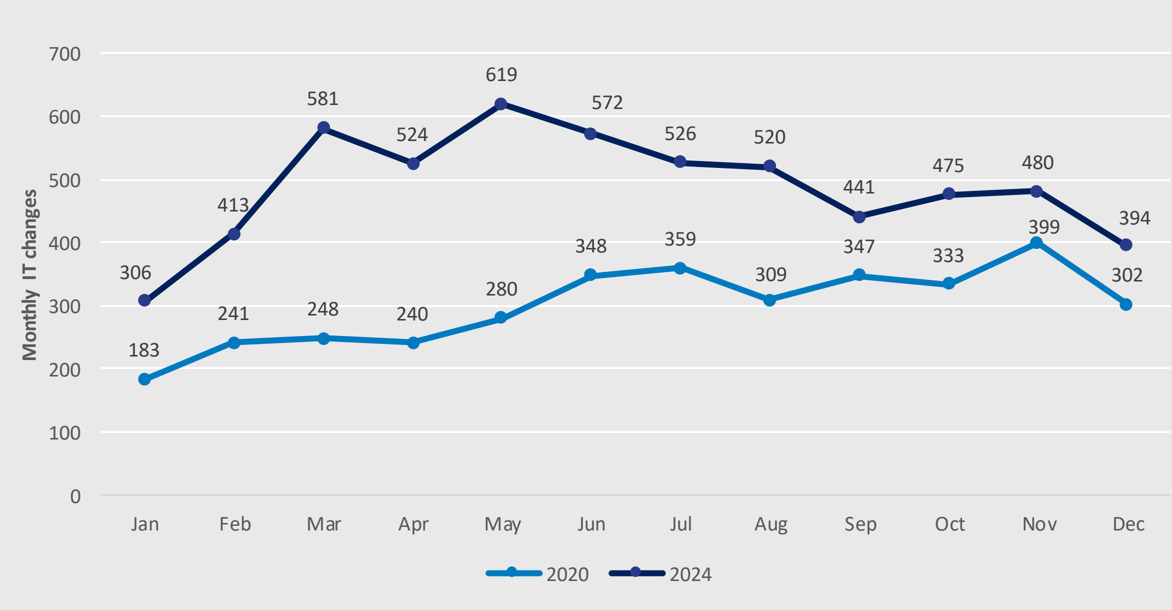
Maintaining IT infrastructure with a structured and timely approach is critical to ensuring the availability, resilience, and reliability of IT infrastructure platforms which can have operational impacts on critical systems. It also manages risks associated with data loss, service interruptions and system failures.

3.2 Adapting to evolving technology needs

The IT and electricity distribution industries are undergoing a rapid transition which will continue to build through the 2026–31 regulatory period. This is driving a growing number of system changes—as shown in figure 2, we have experienced 63 per cent growth in IT system changes between 2020 and 2024.[2]

[2] Across CitiPower, Powercor and United Energy combined

FIGURE 2 MONTHLY IT SYSTEM CHANGES COMPLETED: 2020 VS 2024



In addition to the growing number of IT changes, there is also growing complexity in the IT solutions our infrastructure needs to support, such as distribution energy resources management systems (DERMS) and cloud-based enterprise resource management systems. In the 2026–31 regulatory period, we are also proposing new capabilities as a distribution system operator to support the energy transition activities and major upgrades to our enterprise resource planning and network billing systems. These core platforms are central to network operations and will be implemented via cloud-based solutions, fundamentally changing how some of our largest core systems are managed.[3]

Our IT infrastructure needs to efficiently support the ongoing need for frequent system changes, as well as the increased complexity of the underlying systems.

3.3 Managing technical and market obsolescence

Where possible, the technology landscape needs to remove constraints of old technology so that the business can leverage applications and data in a secure manner to improve the efficiency of processes and the service offerings to customers.

Many non-recurrent solutions being proposed for 2026–31 utilise cloud-based applications or services, as this is where the IT industry is heading:

- Our current on-premise enterprise resource management (ERP) will be upgraded to S/4HANA, SAP's cloud ERP product. The current on-premise billing system will be replaced with an application from the cloud S/4HANA product suite.
- Our Distribution System Operator (DSO) capabilities to enable dynamic operation envelopes (DOEs) and DERMS will utilise cloud-hosted elements as part of our networks new capabilities to support energy transition.
- Cyber capabilities are largely SaaS-based applications, required for monitoring, threat detection and risk management functions.

[3] Implementation of these new capabilities are outlined in separate business cases

We need to ensure existing IT capabilities keep up with modern technology as we anticipate more IT solutions may cease being available as on-premise applications. It will require increasingly complex integrations between legacy and new application versions to keep operations running on older infrastructure, increasing technical debt we have to manage. Not upgrading old, physical infrastructure may also inhibit adoption of more efficient, modern cloud services, or increase costs of new projects due to workarounds, more complex integrations or reactive changes to infrastructure management. We need to assess alternative infrastructure services that enable scalability, expansion and ability to more rapidly support an increasing number of requests being asked of our IT systems.

4. Options analysis

As outlined previously, although we currently run the majority of our IT infrastructure on-premise, our options analysis considers alternative approaches to lifecycle maintenance that can better support current and future business operations and customer needs. Specifically, we have considered four infrastructure options:

1. **Base case (maintain existing infrastructure with structured lifecycle management)**: this option implements a regular and structured lifecycle management approach to updating our IT infrastructure, consistent with our existing management practices (i.e. do-nothing different). That is, it continues a traditional on-premise infrastructure model that updates IT infrastructure beyond vendor recommended upgrade dates where possible.
2. **Maintain existing infrastructure with more frequent upgrades** – this option implements a regular and structured lifecycle management approach to updating our IT infrastructure, continuing on a traditional on-premise infrastructure model. Rather than prolonging lifecycles beyond recommended dates, this option will update 100% of IT infrastructure forecast to be out of vendor support by 2031.
3. **Criteria-based IT infrastructure refresh**: this option will evolve the implementation of our IT infrastructure to support growing operational and information technology workloads using a criteria-based approach to optimise hosting solutions.
4. **Public cloud Infrastructure refresh**: this option will evolve the implementation of our IT infrastructure to support growing operational and information technology workloads, with solutions favouring use of the public cloud.

The costs and associated net present value of each of the options is presented in table 3, and set out in further detail in our attached infrastructure refresh cost and risk models.[4]

TABLE 3 OPTION SUMMARY ($M, 2026)

#	OPTION	CAPEX	OPEX	NPV
1	Maintain existing infrastructure	45.3	-	-
2	Maintain existing infrastructure with more frequent upgrades	54.5	3.1	246.7
3	Criteria based IT infrastructure refresh	45.0	10.0	289.8
4	Public cloud infrastructure refresh	25.3	36.4	281.2

Note: This includes costs and benefits for both CitiPower and Powercor

[4] CP MOD 6.07 - Infrastructure refresh cost - Jan2025 – Public; CP MOD 6.08 - Infrastructure refresh risk - Jan2025 – Public

4.1 Risk monetisation framework

To assess our investment options, we worked with EY to develop an ICT risk monetisation framework. This provides a standardised approach for identifying, classifying, and quantifying risks associated with potential IT investments.

The framework aims to support value-based decision making by translating risks into monetised values, facilitating consistent evaluation of cost-benefit analyses across potential investment scenarios.[5]

Figure 3 sets out the steps we have taken to quantify risks associated with this business case. Further information on each of these steps is included in the risk monetisation framework attachment.

FIGURE 3 RISK MONETISATION STEPS

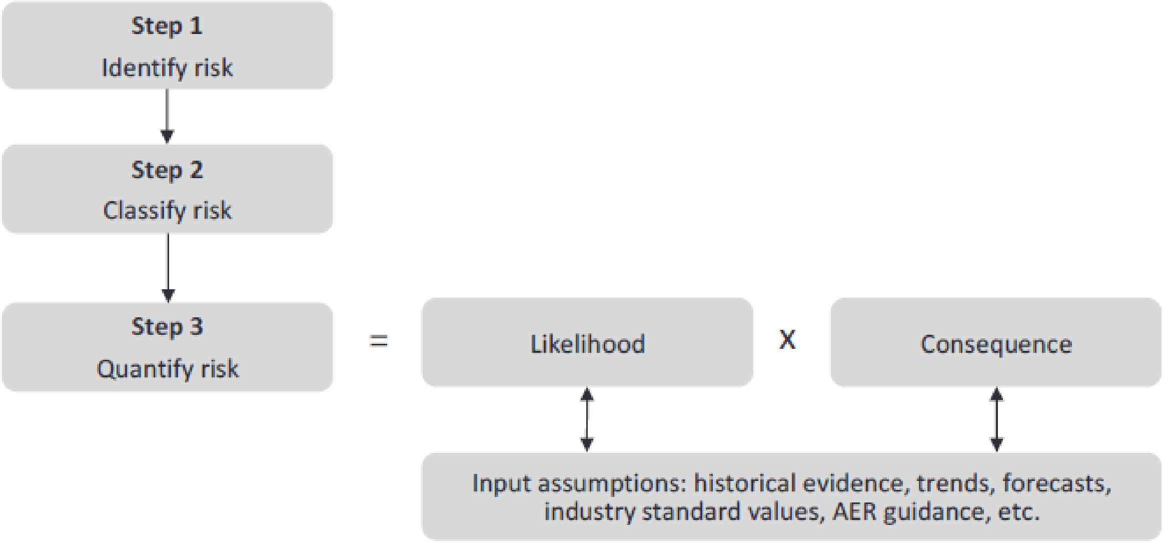

Step 1
Identify risk
Step 2
Classify risk
Step 3
Quantify risk
=
Likelihood
X
Consequence
Input assumptions: historical evidence, trends, forecasts, industry standard values, AER guidance, etc.

Table 4 provides a summary of each risk category included in our risk monetisation framework, which is itself attached with our regulatory proposal.

TABLE 4 RISK FRAMEWORK SUMMARY

CATEGORY	DESCRIPTION
Reliability	Risks related to events or failures that cause unforeseen impacts to electricity supply or export capability. For example, customer supply or solar export
Compliance	Risks of regulatory, legal, or financial penalties due to failure in meeting compliance obligations, such as delays in publishing key market data or unauthorised access to sensitive data

[5] CP ATT 6.02 - EY - IT risk monetisation framework - Jan2025 - Public

Bushfire	Risks that outages of critical operational systems may increase bushfire likelihood by impairing visibility of the network and timely decision-making
Safety	Risks affecting public and staff safety, such as loss of supply impacting life-support customers or disruptions to protective systems
Customer experience	Risks where customer interactions are impacted, such as outages of customer-facing IT systems
IT outage	Risks of systems becoming unavailable due to poor infrastructure maintenance or resource constraints, resulting in prolonged downtimes or outages
IT suitability and sustainability	Risks arising from legacy systems that are prone to failures, inefficiencies, and incompatibilities. These systems may lead to increased maintenance costs, failures, and cyber vulnerabilities if not updated

For each risk identified in the table above we have developed a list of sub-category risks. Each of these sub-category risks is set out in our framework alongside methodologies explaining how each of these risks are quantified.

For this business case key quantified risks relate to:

- Reliability
- Compliance
- IT outage, and
- IT suitability and sustainability.

4.2 Option one: maintain existing infrastructure

Option one focuses on maintaining our existing infrastructure and continuing with a traditional data centre model centred around on-premise hardware to support our required applications. While this is the lowest cost option it is unlikely to meet the identified need.

Our current approach, which would continue under this option would be to upgrade these components beyond the recommended timelines. Based on historical needs we have been able to manage the impact of delaying upgrades, however with increased forecast demand on our IT infrastructure amidst the energy transition and anticipated growth in technology-supported operations, there is an increased outage and suitability risk of continuing to manage IT infrastructure under this approach.

Our current on-premise infrastructure is projected to be increasingly unable to meet growing IT demands, leading to risks of data storage exhaustion, system performance degradation, and escalating operational consequences. Extending infrastructure asset life beyond vendor-recommended cycles will be detrimental to overall system reliability. This approach may also result in compatibility issues as more applications move away from on-premise offerings and towards more modern cloud services. Incremental upgrades fail to capture the cost efficiencies of newer platforms, while maintenance costs for aging infrastructure continue to rise, further hindering modernisation and alignment with industry best practices.

Table 5 sets out the application of our risk framework to option one.

TABLE 5 OPTION ONE RISK SUMMARY

#	RISK	DESCRIPTION
1	Reliability	Extending asset lifecycles beyond vendor recommended lifecycles increases the risk of an infrastructure issue that may impact downstream applications, which support field service, network maintenance operations, customer export capability via distributed energy resource management systems (DERMS), and other critical business processes. Option one has the highest risk of infrastructure outage/malfunction that could cause issues within the applications that support network operations.
2	Compliance	An infrastructure failure will impact the application it is hosting. This extends to our systems that support market processes and market gateways, such as providing market settlement data to AEMO and meter data to energy retailers for customer billing. If we do not meet compliance we are exposed to financial penalties. More frequent outages will increase the likelihood of us not being able to meet our compliance obligations.
3	Bushfire	Direct bushfire risk is negligible but if underlying infrastructure caused issues with field operation planning applications, our teams could experience major delays in performing maintenance or repairs which could result in heightened risk of fire hazards.
4	Safety	Our hazard and incident identification systems are digitised and if those systems go down, risk of personnel injury could increase due to lack of available reporting or reliance on manual procedures.

5	Customer experience risk	Our downstream systems that store customer and connections data would be susceptible to outage if underlying infrastructure fails. This could potentially prevent customers from being able to identify/check network outages online, log a supply or street light fault online, or receive updates regarding status of outages. This would result in loss of ability to utilise our online services and likely result in increase call centre volumes, and increased waiting times for customer support.
6	IT system outage	As this option does not upgrade or maintain all infrastructure to remain in support, it is inherently less stable due to age and out of date firmware versions. This option has the highest likelihood of major IT incidents occurring due to infrastructure reliability issues, resulting in loss of staff productivity and ability to perform operational duties.
7	IT system suitability and system sustainability	Without upgrading our infrastructure to meet greater IT requirements we are highly likely to exhaust data storage capacity and experience system performance degradation during the 2026–31 regulatory period. Even without considering implementation of new IT requirements, we anticipate data utilisation and general computing needs will increase over the next five years as dependency on technology-related solutions continues to increase. When data storage or compute capacity limits are exceeded, system performance degrades and may result in IT outages.

Table 6 sets out the capital and operating expenditure of option one which is reflective of historical infrastructure needs but doesn't factor future growth or new technologies. Currently, some hardware is utilised beyond recommended vendor timelines which carries a tolerable risk if IT consumption doesn't increase beyond 2026–31 levels.

TABLE 6 OPTION ONE EXPENDITURE FORECAST ($M, 2026)

OPTION ONE		FY27	FY28	FY29	FY30	FY31	TOTAL
CitiPower	Capex	2.6	3.3	2.5	3.5	1.7	13.6
	Opex	-	-	-	-	-	-
Powercor	Capex	6.1	7.6	5.9	8.1	4.0	31.7
	Opex	-	-	-	-	-	-
Total		**8.7**	**10.8**	**8.4**	**11.6**	**5.7**	**45.3**

*Rounding may lead to discrepancies between individual network costs and total costs

4.3 Option two: maintain existing infrastructure with more frequent upgrades

Option two focuses on maintaining our existing infrastructure and continuing with a traditional data centre model based around on-premise hardware to support our required applications.

Unlike option one, under option two we would refresh the respective IT components consistent with vendor-recommended timelines.[6] In total, approximately 78 per cent of our existing infrastructure will be refreshed in the 2026–31 regulatory period if upgraded in line with vendor recommendations.

However, as with option one, (our current on-premise infrastructure) this approach is projected to be increasingly limited in its ability to meet growing IT demands, and may result in compatibility issues as more applications move away from on-premise offerings and towards more modern cloud services. Incremental upgrades fail to capture the cost efficiencies of newer platforms, while maintenance costs for aging infrastructure continue to rise, further hindering modernisation and alignment with industry best practices.

Table 7 sets out the application of our risk framework to option two.

TABLE 7 OPTION TWO RISK SUMMARY

#	RISK	DESCRIPTION
1	Reliability	More frequent upgrades of the current state infrastructure environments may lead to minor reductions in the likelihood of system failure. As with option one, if a piece of underlying hardware fails then it will cause an unavoidable impact to the associated application. There is no failover or redundancy measure to protect critical operations supporting field service maintenance or ensuring residential solar can continue to be exported into the grid.
2	Compliance	By upgrading at vendor-recommended frequency, the failure rate will materially decrease due to keeping hardware up-to-date, in addition to benefits from updates and patches that further reduce risk of operational vulnerabilities that can impact our ability to publish market data and meet our compliance obligations.
3	Bushfire	Same as option one
4	Safety	Same as option one
5	Customer experience risk	Same as option one

[6] Extending critical IT infrastructure asset life beyond vendor-recommended cycles can be detrimental to overall system reliability, and can lead to increased risks of data storage exhaustion, system performance degradation, and escalating operational consequences.

6	IT system outage	For infrastructure enabling our broader OT and IT applications, we would expect to see a material reduction in likelihood of a general system outage caused by infrastructure. By upgrading 100% of our hardware as per vendor guidelines, we would achieve material reductions in risk of an infrastructure-derived outage compared to Option one. In the event of an outage it would still have a comparable resolution time to Option one.
7	IT system suitability and system sustainability	With increasing investment levels under Option two it's less likely that we'd experience a storage or performance degradation issue. However, inefficiencies related to uplifting IT capacity to meet our growing IT footprint would remain, as would our agility to meet these new requirements. As the majority of our operational IT capabilities remain on traditional on-premise infrastructure, we would have limited ability to efficiently scale for future needs. Many of our upgraded core capabilities will be cloud-hosted solutions (DERMS, SAP Enterprise Resource Planning upgrade, network billing system upgrade) and if we don't modernise our approach to existing infrastructure we may eventually experience compatibility issues between old and new systems.

Table 8 sets out the capital and operating expenditure of option two. This represents a similar approach to infrastructure management as option one, however replaces all hardware at the end of its recommended life. This includes replacing all hardware reaching the end of its recommend life during the 2026–31 regulatory period, as well as all aged hardware from the previous regulatory period.

TABLE 8 OPTION TWO EXPENDITURE FORECAST ($M, 2026)

OPTION TWO		FY27	FY28	FY29	FY30	FY31	TOTAL
CitiPower	Capex	5.3	2.7	4.1	2.8	1.5	16.3
	Opex	-0.8	-0.2	0.3	0.7	1.0	0.9
Powercor	Capex	12.3	6.3	9.5	6.5	3.6	38.1
	Opex	-1.8	-0.5	0.6	1.7	2.3	2.2
Total		**14.9**	**8.2**	**14.5**	**11.6**	**8.3**	**57.6**

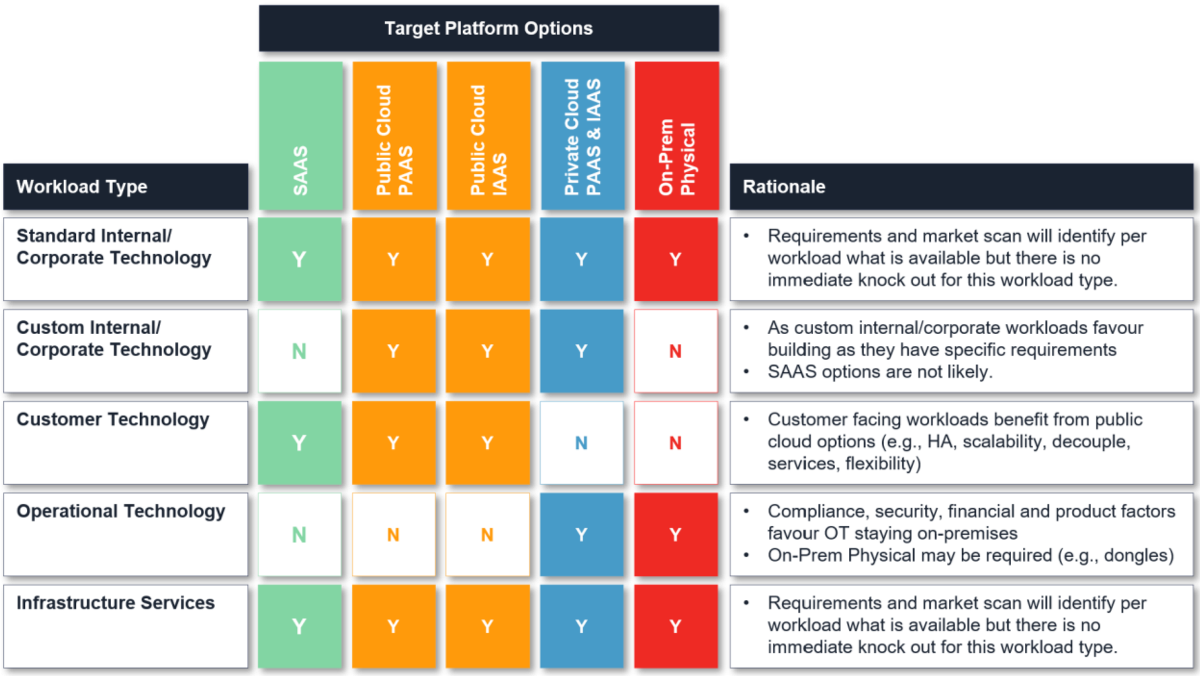
*Rounding may lead to discrepancies between individual network costs and total costs

4.4 Option three: criteria based infrastructure refresh

Option three changes how we manage our IT infrastructure, with this new approach supporting different technology hosting options through the placement of 'workloads' according to specific criteria (e.g. security, agility, available market options). A combination of SaaS, PaaS, IaaS and on-premise private cloud technologies are all used under this option and will allow us to meet the differing requirements of individual workloads. Our data centres would be updated to modern structures capable of supporting this new model.

Figure 4 provides an example of how we have applied this methodology to different types of workloads. The full workload placement methodology, including relevant selection steps, is included in appendix A.

FIGURE 4 MAPPING OF WORKLOAD TYPE TO TARGET PLATFORM OPTIONS



	Target Platform Options					
Workload Type	SAAS	Public Cloud PAAS	Public Cloud IAAS	Private Cloud PAAS & IAAS	On-Prem Physical	Rationale
Standard Internal/ Corporate Technology	Y	Y	Y	Y	Y	• Requirements and market scan will identify per workload what is available but there is no immediate knock out for this workload type.
Custom Internal/ Corporate Technology	N	Y	Y	Y	N	• As custom internal/corporate workloads favour building as they have specific requirements • SAAS options are not likely.
Customer Technology	Y	Y	Y	N	N	• Customer facing workloads benefit from public cloud options (e.g., HA, scalability, decouple, services, flexibility)
Operational Technology	N	N	N	Y	Y	• Compliance, security, financial and product factors favour OT staying on-premises • On-Prem Physical may be required (e.g., dongles)
Infrastructure Services	Y	Y	Y	Y	Y	• Requirements and market scan will identify per workload what is available but there is no immediate knock out for this workload type.

By selecting different platforms for different types of workloads we would transition away from a high reliance on traditional data centre structures. Instead, we would upgrade our traditional data centres to modern software defined data centres (SDDC).

By making this transition we will be able to better scale and adapt our IT assets, and better integrate the various hosting and platform options. Under this approach, far more of our hardware becomes multi-purpose rather than single purpose.[7] This allows us to move away from our traditional base-case model of replacing for-purpose hardware that can only be used for a single dedicated purpose.

[7] Hardware (such as servers) are currently built-for-purpose to support a specific IT workload. Once installed, it can only be used to support that workload. Under a software-defined data centre (SDDC) model, the hardware can be repurposed to support new IT demand, or act as a redundancy measure. I.e. Failure occurs in server A which would normally result in an outage, but under a SDDC there would be no outage as server B/C/D could cover server A's workloads.

The implementation of this methodology will also better optimise IT effort with customer outcomes. For example, common use applications (e.g. finance, procurement, legal) are candidates for 'software as a service' solutions, freeing up resourcing and investment to be focused on higher value customer and operational focused solutions which can be personalised and targeted.

A further benefit of this option is enablement of future IT growth and new capabilities that would otherwise not be possible under a traditional on-premise model, or comparatively costly.

Table 9 sets out the application of our risk framework to option two.

TABLE 9 OPTION THREE: RISK ASSESSMENT

RISK	DESCRIPTION
Reliability	Under option three the risk of an infrastructure outage causing downstream impacts to field service management or solar exports is lower than option one and two due to cloud infrastructure services being inherently easier to maintain and keep updated. Infrastructure updates can be implemented quicker and require less internal effort to maintain ongoing.
Compliance	This option offers a more flexible and scalable approach to infrastructure management, while ensuring mandatory market obligations continue to be met. The main performance gain over options one and two are that due to improved redundancy measures, we'd expect a material reduction in time to resolve outages impacting our ability to publish market data.
Bushfire	Same as option two
Safety	Same as option two
Customer experience	Same as option two
IT outage	Option three's infrastructure model minimises single points of hardware failure and provides a single management pane for all infrastructure capabilities rather than needing to separately manage functions (compared to option one and two). Simplifying our operating models will also build in greater redundancy measures, in the event of an incident occurring in data centre A, data centre B can fail-over to keep systems running (i.e. workloads are interchangeable, rather than applications being fully dependent on the original infrastructure it was configured on).
Suitability and sustainability	With option three's scalable infrastructure, compute and storage are managed as a holistic function rather than siloed buckets (as per current, traditional infrastructure configurations). Processes to provision new servers can also be automated rather than needing to increase capacity via manual installation. Under this option it is very unlikely we'd exceed data storage levels that could cause outages, or experience IT performance issues if implementing this option's upgrade plan.

Table 10 sets out the capital and operating expenditure of option two. Under this option, the costs relate to the upgrade of our current data centres and key IT network locations to implement the new hosting structures, migration of workloads into the updated hosting solutions and lifecycle maintenance of new and existing infrastructure.

TABLE 10 OPTION THREE: EXPENDITURE FORECAST ($M, 2026)

NETWORK		FY27	FY28	FY29	FY30	FY31	TOTAL
CitiPower	Capex	4.8	3.0	2.6	1.8	1.2	13.5
	Opex	0.1	0.3	0.7	1.0	1.0	3.0
Powercor	Capex	11.3	6.9	6.2	4.3	2.9	31.5
	Opex	0.2	0.7	1.5	2.3	2.3	7.0
Total		**16.4**	**10.9**	**11.0**	**0.4**	**7.4**	**55.1**

*Rounding may lead to discrepancies between individual network costs and total costs

4.5 Option four: infrastructure refresh favouring public cloud

Option four is similar to option three, with all activities identified in option three still required. This option, however, prioritises the utilisation of public cloud solutions where these are available (e.g. rather than the workload placement methodology outlined previously, which considers key criteria such as security, data sovereignty, regulatory compliance, solution availability and vendor strategy as part of specific workload hosting considerations).

Under this approach, a higher percentage of IT applications would be shifted to the public cloud solutions. OT application hosting decisions, however, would be remain identical to option three due to the need to maintain higher levels of internal control for network-reliant technologies and remain compliant with Foreign Investment Review Board (FIRB) requirements.

Overall, there is little additional risk reduction benefit associated with this option relative to option three. While there may be some reduction in risk associated with exceeding data storage and general performance degradation, this is likely balanced against a slightly higher operational risk due to the outsourcing most non-OT application infrastructure services.

Table 11 sets out the capital and operating expenditure of option three. The approach is the same as option 3, however chooses public cloud hosting services by default if there is an available solution for the workload. This results in a higher expenditure forecast due to greater utilisation of external vendor services.

TABLE 11 OPTION FOUR: EXPENDITURE FORECAST ($M, 2026)

NETWORK		FY27	FY28	FY29	FY30	FY31	TOTAL
CitiPower	Capex	3.0	1.4	1.0	1.5	0.4	7.2
	Opex	1.5	1.9	2.0	2.6	2.5	10.5
Powercor	Capex	7.5	3.4	2.4	3.6	0.9	17.7
	Opex	3.7	4.6	4.9	6.3	6.0	25.5
Total		**16.0**	**11.5**	**10.4**	**14.1**	**9.7**	**61.7**

5. Recommendation

Our current infrastructure footprint is sufficient for yesterday's needs but is not an efficient model to continue investing in its current form. Increasingly, we foresee issues in its ability to meet our future IT demand as more applications move towards cloud and SaaS products (both due to efficiencies, as well as available market offerings).

Modernising our infrastructure to be more scalable and adaptable to future compute and storage requirements is therefore considered a least-regrets investment. Under option three, we would maintain full control of critical hosting solutions while ensuring a balanced investment approach that utilises set criteria to manage risk specific to our IT networks.

Option four also shifts us towards a more modernised approach consistent with evolving market offerings, but reflects an outsourced operating model that would require relinquishing a level of internal control via higher reliance on public cloud services. In any event, outsourcing is likely to lead to higher overall costs compared to option three with immaterial additional benefit.

Accordingly, our preferred approach to refreshing our existing IT infrastructure is option three, a criteria-based infrastructure refresh.

Our recommendation also considered a number of general factors (e.g. project concurrency, resource availability) to ensure preferred option and upgrade timing was pragmatic, actionable, and would have the highest probability of delivering a successful outcome.

Our proposed expenditure profile is provided in table 12.

TABLE 12 RECOMMENDED OPTION EXPENDITURE FORECAST ($M, REAL 2026)

OPTION THREE		FY27	FY28	FY29	FY30	FY31	TOTAL
CitiPower	Capex	4.8	3.0	2.6	1.8	1.2	13.5
	Opex	0.1	0.3	0.7	1.0	1.0	3.0
Powercor	Capex	11.3	6.9	6.2	4.3	2.9	31.5
	Opex	0.2	0.7	1.5	2.3	2.3	7.0
Total		**16.4**	**10.9**	**11.0**	**0.4**	**7.4**	**55.1**

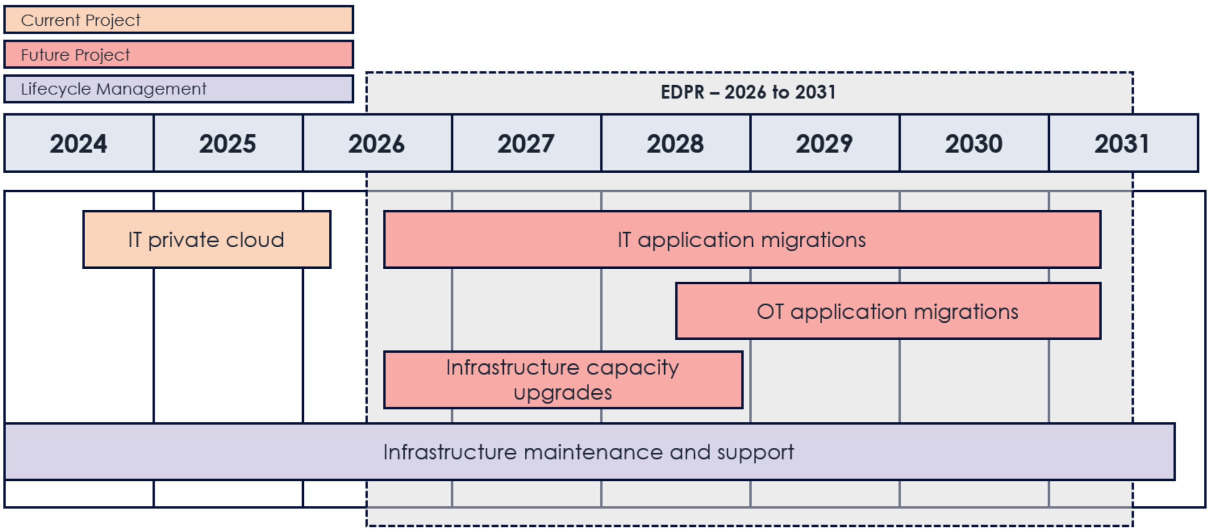
*Rounding may lead to discrepancies between individual network costs and total costs

5.1 Implementation plan

The majority of site and data centre upgrades are flagged for early in the next regulatory period, however, our plan to implement option three is already in progress, with assessments underway to implement the new IT private cloud environment prior to 2026.

As outlined in figure 5, the infrastructure lifecycle management program schedules capacity upgrades in the first half of next regulatory period to ensure our hardware is ready for the application migrations. The IT and OT application migrations will occur in a phased approach determined by lifecycle upgrade timings and optimal change windows between other projects.

FIGURE 5 HIGH LEVEL IMPLEMENTATION PLAN


Current Project
Future Project
Lifecycle Management
EDPR – 2026 to 2031
2024
2025
2026
2027
2028
2029
2030
2031
IT private cloud
IT application migrations
OT application migrations
Infrastructure capacity upgrades
Infrastructure maintenance and support

Private cloud: We have commenced establishment of the IT private cloud so it will be available prior to next regulatory period and available for relevant applications.

IT application migrations: As each IT workload becomes due for upgrade/replacement, it will undergo detailed assessments under the workload placement methodology (appendix A) then the appropriate target platform will be determined[8].

OT application migrations: As each OT workload becomes due to upgrade/replacement, it will undergo detailed assessments under the workload placement methodology then the appropriate target platform will be determined. This is phased later in the period as

Infrastructure capacity upgrades: This includes various data centre, branch office, networking and general capacity upgrades required to support IT and OT infrastructure requirements throughout the five year period.

Infrastructure maintenance and support: Ongoing managed support services and contracts for infrastructure services supporting on-premise and cloud footprint.

[8] Infrastructure requirements supporting SAP, billing systems, cyber and non-recurrent IT projects are out of scope and covered in the separate respective business cases.

A Workload placement methodology

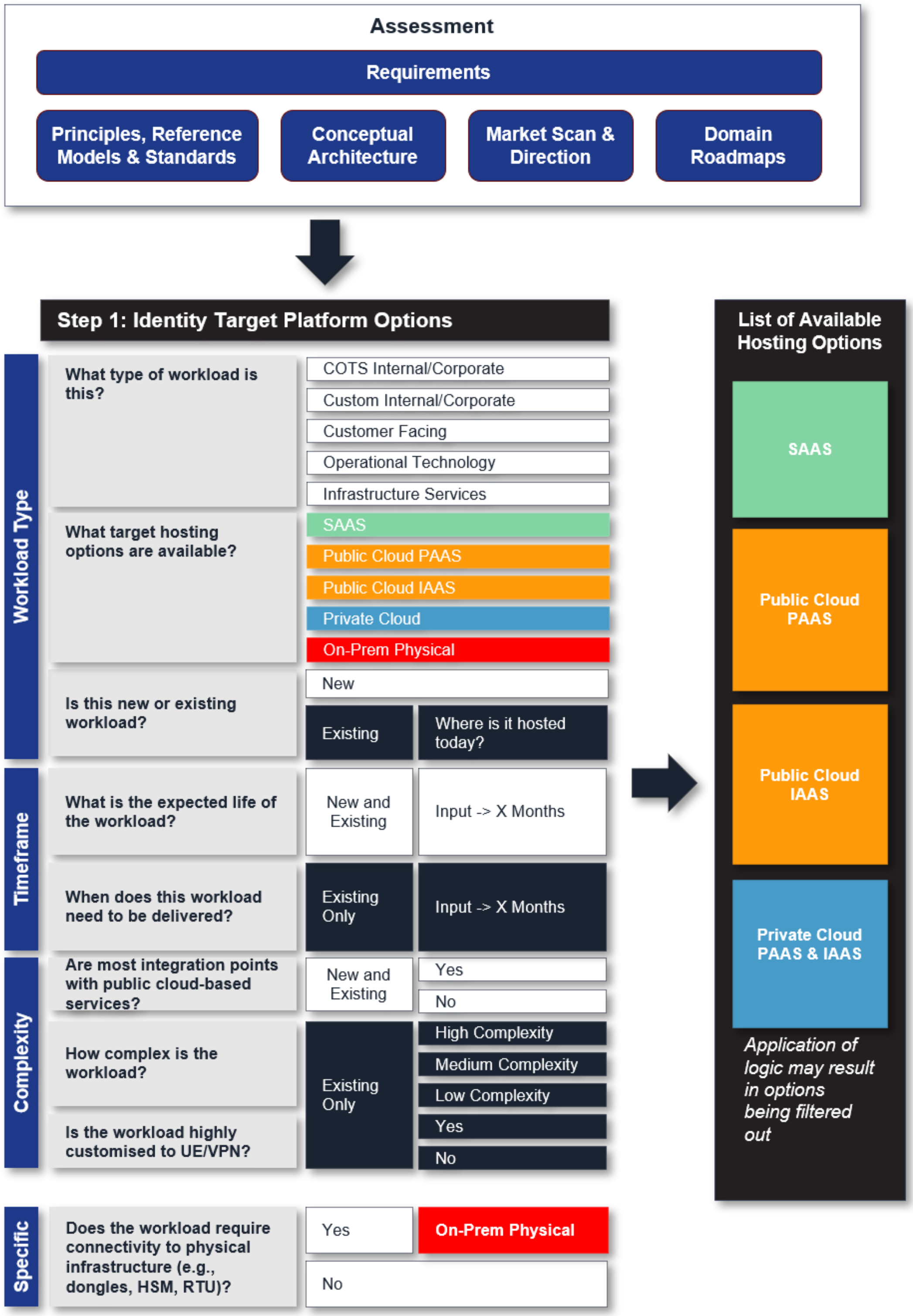
A structured workload placement methodology has been developed to allow us to make the right choice for where a workload should be deployed based on key business criteria that assess considerations such as asset life, complexity and area of the business the workload is supporting (detailed further in figure 6). The aim of the methodology is to ensure that the most suitable platform is selected based on the required work.

The development and application of the workload placement methodology comprises three stages, as defined below:

- Assessment: this step collates, develops and assesses different inputs such as requirements, reference models, principles, standards, conceptual architecture, market scan to generate a list of domain roadmap aligned hosting options
- Identify target platform options: this step uses a series of questions to identify the target platform options that are available for a specific workload and initiative. These options are then evaluated against specific questions (per below)
- Determine preferred target platform option: this step uses the available hosting options and applies further specific questions in order from top to bottom to derive the recommended placement. On-premise private cloud is the default option, and importantly, not all workloads are suitable for all target platform options (e.g. the methodology recommends that operational technology workloads stay on-premise to ensure safe and secure management of assets connected to the electricity distribution network).

These stages are presented visually in figure 6 below.

FIGURE 6 WORKLOAD PLACEMENT METHODOLOGY



Assessment

Requirements

Principles, Reference Models & Standards

Conceptual Architecture

Market Scan & Direction

Domain Roadmaps

Step 1: Identity Target Platform Options

Workload Type

What type of workload is this?
- COTS Internal/Corporate
- Custom Internal/Corporate
- Customer Facing
- Operational Technology
- Infrastructure Services

What target hosting options are available?
- SAAS
- Public Cloud PAAS
- Public Cloud IAAS
- Private Cloud
- On-Prem Physical

Is this new or existing workload?
- New
- Existing – Where is it hosted today?

Timeframe

What is the expected life of the workload?
- New and Existing – Input -> X Months

When does this workload need to be delivered?
- Existing Only – Input -> X Months

Complexity

Are most integration points with public cloud-based services?
- New and Existing – Yes / No

How complex is the workload?
- Existing Only – High Complexity / Medium Complexity / Low Complexity

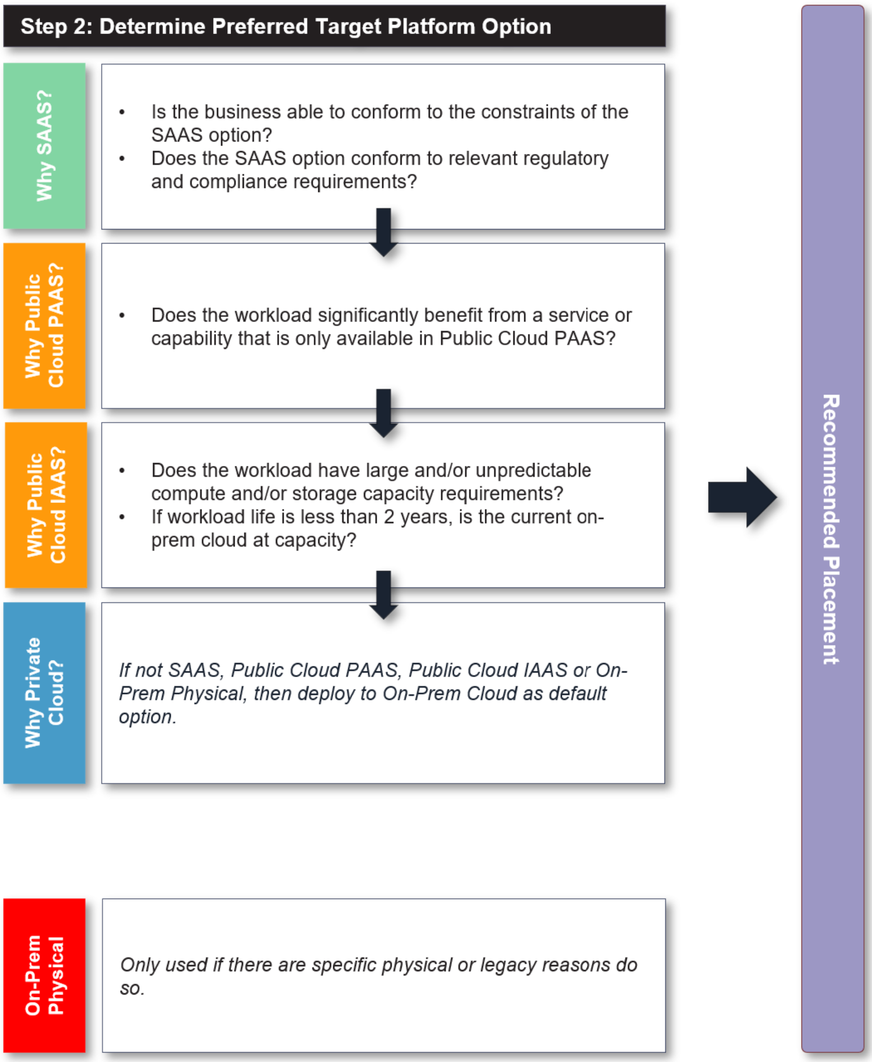
Is the workload highly customised to UE/VPN?
- Existing Only – Yes / No

Specific

Does the workload require connectivity to physical infrastructure (e.g., dongles, HSM, RTU)?
- Yes – On-Prem Physical
- No

List of Available Hosting Options
- SAAS
- Public Cloud PAAS
- Public Cloud IAAS
- Private Cloud PAAS & IAAS

Application of logic may result in options being filtered out



Step 2: Determine Preferred Target Platform Option

Why SAAS?

- Is the business able to conform to the constraints of the SAAS option?
- Does the SAAS option conform to relevant regulatory and compliance requirements?

Why Public Cloud PAAS?

- Does the workload significantly benefit from a service or capability that is only available in Public Cloud PAAS?

Why Public Cloud IAAS?

- Does the workload have large and/or unpredictable compute and/or storage capacity requirements?
- If workload life is less than 2 years, is the current on-prem cloud at capacity?

Why Private Cloud?

If not SAAS, Public Cloud PAAS, Public Cloud IAAS or On-Prem Physical, then deploy to On-Prem Cloud as default option.

On-Prem Physical

Only used if there are specific physical or legacy reasons do so.

Recommended Placement

CitiPower

For further information visit:

🌐 Citipower.com.au

CitiPower and Powercor Australia

CitiPower and Powercor Australia

CitiPower and Powercor Australia