January 2026

Powerlink 2027-32 Revenue Proposal

Appendix 4.07
Operational Technology Plan

Contents

List of Figures

List of Tables

Document Version History

Revision Date	Version Number	Description
4 February 2025	0.1	Initial draft version
30 April 2025	0.2	Extension of initial drafting
4 June 2025	0.3	Incorporate 2027-32 Program of Work
10 June 2025	0.4	Rebase financials in FY27 terms
12 June 2026	1.0	Incorporate review feedback and mark as FINAL
25 July 2025	2.0	Updates following document review by key stakeholders
15 December 2025	3.0	Updates following final review of financials

Acronyms

Acronym	Definition
AEMS	Advanced Energy Management System
AER	Australian Energy Regulator
AESCF	Australian Energy Sector Cyber Security Framework
ATS	Automatic Transfer Switches
BCS	Business Continuity Site
BITDD	Business Information Technology and Digital Delivery
CAPEX	Capital Expenditure
DIMA	Database Integrations & Management Application
DWDM	Dense Wavelength Division Multiplexing
EDM	Energy and Digital Management
NEM	National Electricity Market

NGNO	Next Generation Network Operations Program
OMS	Outage Management System
OT	Operational Technology
OTAMP	Operational Technology Asset Management Plan
OTAMS	Operational Technology Asset Management Strategy
PDU	Power Distribution Units
PoaP	Plan-on-a-Page
POPEX	Project Operating Expenditure
PoW	Program of Work
RCP	Regulatory Control Period
SAMP	Strategic Asset Management Plan
SDSs	Service Delivery Switches
TCO	Total Cost of Ownership
TNSP	Transmission Network Service Provider
UPS	Uninterruptible Power Supplies
VPN	Virtual Private Network

1. EXECUTIVE SUMMARY

Operational Technology (OT) is a foundational component of Powerlink's network operations, critical to the day-to-day delivery of the company's services to its customers and stakeholders. Modern digital technology is a key enabler of efficient and stable grid operations and is a cornerstone of continuous improvement in the way Powerlink delivers it services.

In the current (2022–27) Regulatory Control Period (RCP), the OT focus has been to maintain supportability of our existing operational infrastructure, whilst also prioritising allocation of key OT resources to support delivery of the Next Generation Network Operations (NGNO) program[1]. Throughout the current RCP, cyber security investment has also been a critical priority, to mitigate our security risk exposure in an escalating threat environment.

For the coming (2027-32) RCP, the OT program has been developed with the following focuses:

Compliance and risk mitigation
As a Transmission Network Service Provider (TNSP), Powerlink is subject to a range of legislative, regulatory and electricity market obligations. The OT Asset Management approach contributes to maintaining compliance through prudent asset lifecycle management and risk mitigation.

Sustainability
OT assets must remain supportable, reliable and sustainable through management of system currency and avoidance of technical obsolescence.

Balancing of risk and total cost of ownership (TCO)
A TCO-focused approach to OT Asset Management seeks to minimise the whole-of-life costs of assets spanning acquisition, operations, maintenance and disposal, prudently balanced with management of risk.

Service agility
To meet Powerlink's evolving service requirements, the organisation's OT must remain flexible to meet current and future operational needs.

The planned OT capital expenditure program for 2027-32 is $89.82M[2], with investments spanning seven (7) asset categories as depicted in Figure 1.

[1] The NGNO program is transformational in nature and is managed separately from the OT Program of Work.

[2] Financials for 2027-32 RCP are shown in FY26 terms.

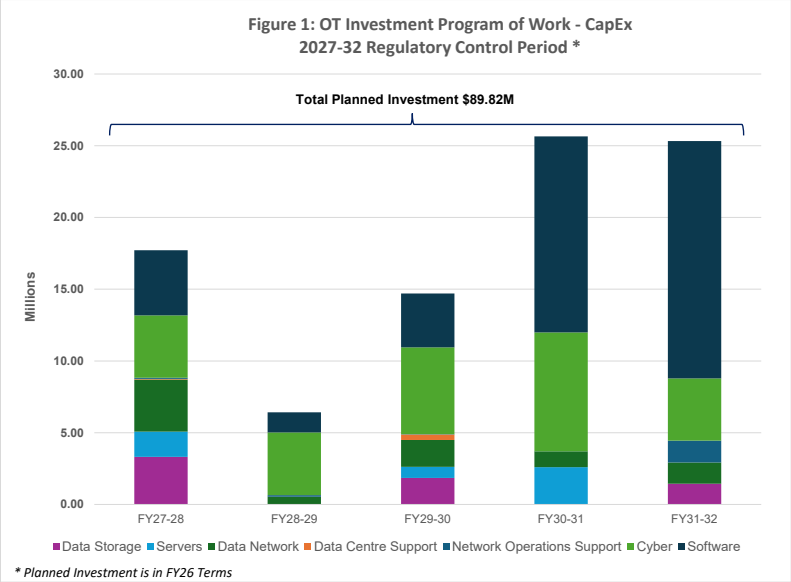


Figure 1: OT 2027-32 RCP Program of Work Investment Profile

2. POWERLINK OT CONTEXT

2.1. Scope of OT within Powerlink

Operational Technologies (OT) provide the day-to-day capabilities to remotely monitor, measure and control the operation of Powerlink's Transmission Network, including interconnection with the National Electricity Market.

OT is critical to the safe and reliable delivery of energy and related services to customers and stakeholders. A key requirement for OT is the need for 24x7x365 operations – which necessitates resilient, highly available and fault tolerant capability.

The scope of OT investments spans physical infrastructure through to complex specialised application software. These assets are primarily contained within Powerlink's on-premise data centres and control rooms. Figure 2 depicts the seven (7) categories of OT assets within Powerlink's overall digital asset base.

Figure 2: Powerlink OT Asset Categories

The above OT asset categories are further broken into a set of sub-categories as described in the Table 1[3].

Asset Category	Sub-Categories	
Software *Operational computer systems and software used to manage or support the operation of the Powerlink transmission grid and telecommunications services.*	**Control Systems**	Control Systems Software supporting the 365x24x7 management and operation of the Powerlink transmission network. This sub-category includes the control systems application software, as well as the underlying "ecosystem" of dependent assets. Software examples include the Advanced Energy Management System (AEMS), Outage Planning & Scheduling Management, Switching Order Management System, Network Device Log Management, Data Integration and Management (DIMA) and related software.
	OT Support	OT Support Software to manage the security, infrastructure, storage and networking platforms. Includes the time-series historian [redacted] telecommunications management software (e.g. [redacted] Operational Support and Control Systems, Configuration Management software (e.g. [redacted]
	Core Infrastructure	Other operational infrastructure software including Operating Systems, Database Management Systems, Directories and Infrastructure Configuration Management Software.
Cyber Security *Operational network security equipment and services, facilitating Access Controls, Traffic Filtering, VPN Services, Intrusion Detection & Prevention and other security functions.*	**Security Infrastructure**	Security infrastructure and appliances play a vital role in securing the data centre from "untrusted" networks, be they external and internal. This includes core, edge and head-end firewalls, as well as Virtual Private Network (VPN) equipment and other related security assets.
	Security Software & Services	Security software includes Identity and Access Management, Privileged Access Management, Vulnerability Management and Intrusion Detection/Prevention. In addition, Security services are used to supplement (and/or are in lieu of) additional infrastructure and resources for specific functions.
Network Operations Support *Specialised visualisation and communications equipment for use by operators within the Network*	**Operational Telephony Systems**	Telephony systems for operational communications including Control Room Telephony, the [redacted] Operational Telephony Network (OTN) and Remote Satellite Telephony
	Network Operations Workstations	High-end workstations for power network control and management applications

[3] Note: Within each sub-category, the software and infrastructure examples detailed within the Table 1 are provided for clarity and should not be considered exhaustive.

Asset Category	Sub-Categories	
Operations control room and other operational locations to monitor and manage the electricity transmission network and provide unified telecommunications services.	**Network Operations Displays**	Wallboards and dashboard displays for real time systems visualisation
Data Centre Support *Physical infrastructure within Powerlink's data centres that houses OT servers, storage and networking equipment.*	**UPS and Batteries**	Contingency power backup for operational equipment and services
	Racks and Cabling	Server and equipment housings within for OT infrastructure
	Power Distribution	Power management for OT infrastructure
	Automatic Transfer Switches (Power)	Power cutover switching for OT infrastructure
	SMS Alerting	Operational alerting of OT infrastructure failure or functional anomalies
Data Network *Data centre networking facilities enabling the interconnection of server, storage and other data equipment, and facilitating secure segregated organisational access to these services.*	**Core Switches**	Data network switch equipment, enabling high-capacity, high-performance data traffic between devices and systems (incl. servers, storage and other network components)
	Access Switches	Access switch equipment providing entry point in and out of the data centre, aggregating traffic from multiple endpoints
	Routers, Gateways and Load Balancers	Network data routing, gateway and load management devices
Servers *Server equipment hosting the OT services including application, network, communications, database and security services.*	**Servers**	Physical servers host dedicated computing tasks, requiring direct control of the hardware. Virtualised (software-based) servers run on physical server hardware but are abstracted using a hypervisor (e.g. [redacted] The hypervisor is responsible for allocating and managing underlying physical resources (CPU, memory, storage) among multiple virtual servers. Includes [redacted] ervers, [redacted] Hypervisor and [redacted]. Includes Remote USB Hub (IP) devices that allow USB licence dongles to be connected to the network for software authentication.
	Clock Appliances	Devices that provide synchronised time alignment for connected equipment
	High-end Workstations	AEMS and other workstations required for high-end services / workloads, specific to the OT domain and require significant processing power

Asset Category	Sub-Categories	
		(e.g. simulation, network modelling and other power network analysis software).
Data Storage *Data storage and backup equipment supporting operational databases, file systems, time-series historian and other requirements.*	**Storage Area Networks (SAN)**	Centralised, high-performance, scalable, reliable and efficient storage management for servers, databases and applications
	Backup System	Storage facilities to backup, protect and recover critical operational data in event of system data loss, system failure, or other disaster

Table 1: Asset Category and Sub-categories

2.2. OT Linkage to Corporate Strategy

The Australian energy industry has embarked on a period of unprecedented change and transformation. The Powerlink electricity transmission network is a key enabler of this change. The corporate strategic plan themes depicted in Figure 3 describe Powerlink's vision for the coming period.

- **Deliver safe, reliable and affordable electricity to Queenslanders**
- Strengthen Queensland's economy through internationally **competitive energy prices**
- Continue to grow a world class non-regulated business **with efficient and effective customer connections**
- **Effectively engage and support communities to unlock lasting legacy benefits**

- Be celebrated as **an inclusive and diverse workforce where safety is non-negotiable**
- Operate as a **highly competent and collaborative workforce**
- Cultivate **inspirational leaders**, and a culture of **flexibility and innovation**
- Foster **enduring productive relationships** with our communities, customers and partners

- Drive a **whole of system, flexible and cost-effective approach** to the energy transition
- **Influence policy, investment decisions, regulation and market design** for the benefit of Queenslanders
- **Guide the location and characteristics of future connections** and enable investment in Queensland

- Support the achievement of **Queensland's energy roadmap**
- **Optimise the transmission network** to meet changing dynamics of the energy market
- Operate the **most reliable and efficient energy system**
- **Maximise the use of the existing network**

.

Figure 3: Corporate Strategic Themes

In support of the above strategic themes, Powerlink's OT Asset Management Strategy (OTAMS):

- Prudently leverages modern digital technologies and techniques to ensure high levels of **availability**, **reliability** and **sustainability** for our operational systems and services.
- Optimises system uptime, enhances **operational stability** and extends the **longevity of our assets**.
- Maintains robust and resilient systems, fostering continuous improvement, and implementing strong **cyber security** measures to safeguard our operations.

Key Powerlink OT management focus areas are summarised in Figure 4.

1	OT Service Management & Availability	We'll apply modern Service Management practices for OT, including service performance management, capacity management, release management and problem/event management.
2	Operational Efficiency & Readiness	Through use of automation, streamlined interfaces and repeatable processes, we'll continuously improve OT service delivery efficiency and change readiness.
3	Cyber Security	We'll continue to protect and secure our operational systems, networks and data from cyber threats and attacks, in an escalating threat environment.
4	OT Sustainability & Reliability	We'll enhance the sustainability and reliability of Powerlink's OT platforms and prioritise support for the next generation of network management systems.
5	Operational Data Enablement	We'll make the right data available at the right time (inc. SCADA, IoT and Historian data), for optimal network management and decision making.

Figure 4: OT Management Focus Areas

3. OT ASSET MANAGEMENT APPROACH

3.1. OT Asset Management Principles

Key principles that guide the planning and investment in Powerlink's OT assets include:

Strategic alignment

Asset management strategies are aligned with Powerlink's goals and compliance obligations.

Safety and reliability

Assets are managed prudently and effectively to deliver consistent performance and safety for the workforce and community.

Cost Efficiency and lifecycle optimisation

A whole-of-life approach is undertaken from investment decision-making through to end-of-life, ensuring prudent and efficient management of OT assets to meet organisational needs over time (i.e. planning, acquisition, commissioning, operating, maintaining, decommissioning and disposal).

Risk management

Ownership and operation of OT assets requires regular identification, assessment and mitigation of risk. This includes operational, compliance, cybersecurity, financial, regulatory and strategic risks.

Asset standardisation

The standardisation of OT assets supports efficiency improvements in procurement, deployment, security management, operational management and skills management.

Asset monitoring and performance

Information from asset monitoring is essential for informed decision-making in OT asset management. By leveraging data insights, OT asset utilisation, maintenance requirements and vulnerabilities are assessed to forecast growth and future asset requirements.

3.2. Outcomes of Asset Management

The application of the OT Asset Management Principles enables:

Compliance and risk mitigation

As a Transmission Network Service Provider (TNSP), Powerlink is subject to a range of legislative, regulatory and electricity market obligations. The OT Asset Management approach contributes to maintaining compliance through prudent asset lifecycle management and risk mitigation.

Sustainability

OT assets must remain supportable, reliable and sustainable through management of system currency and avoidance of technical obsolescence.

Balancing of risk and total cost of ownership (TCO)

A TCO-focused approach to OT asset management seeks to minimise the whole-of-life costs of assets spanning acquisition, operations, maintenance and disposal, prudently balanced with management of risk.

Service agility

To meet Powerlink's evolving service requirements, the organisation's OT must remain flexible to meet current and future operational needs.

3.3. Regulations, Rules and Codes Compliance

As a TNSP in the Nation Electricity Market (NEM), Powerlink has a range of legislative and regulatory compliance obligations. Table 2 lists the instruments and associated obligations for Powerlink and outline impacts for the management and use of Operational Technology.

Instrument	Obligations and Implications for OT Asset Management Strategies
Security of Critical Infrastructure Act 2018 (the SOCI Act)	▪ Requirement to notify external data service providers of data handling requirements for sensitive critical infrastructure data and their obligations under the Act. ▪ Entities must register some information related to critical infrastructure assets with the Cyber and Infrastructure Security Centre. ▪ Entities must maintain a compliant Risk Management Program for their critical infrastructure assets. ▪ Entities must report cyber security incidents that have a significant or relevant impact on their asset. ▪ [redacted]
Australian Energy Sector Cyber Security Framework (AESCSF)	▪ Consistent with the organisation's SOCI obligations, the Powerlink Board has set a target of achieving and maintaining cyber security [redacted]
National Electricity Law and National Electricity Rules	▪ Compliance with all TNSP obligations under National Electricity Law. ▪ Requirement to establish and operation SCADA systems and processes consistent with the AEMO SCADA Standard (Guide).
Electricity Act 1994 (Queensland)	▪ Compliance with all Licence Obligations of a Transmission Authority holder in Queensland.

Table 2: Statutory and Regulatory Obligations

3.4. OT Asset Management Guidelines

The OT Asset Management Strategy defines asset management guidelines for all categories of OT assets operated by Powerlink. A "Standard Guideline" is defined for each asset category identified in Table 1 (see Section 2.1, Page 6). Then, for each sub-category, "Specialised Guidelines" are further defined where relevant. In each case, the guidelines describe the approach taken to manage the asset category (or sub-category) as well as the typical asset lives based on vendors' published end-of-life guidance.

Furthermore, for each asset category (or sub-category) the table indicates one of three "Renewal Types" as follows:

- **Individual assets (I)**
  These assets are relatively unique and have no dependency (or limited dependency) on other assets. They are therefore managed and refreshed on an individual basis. E.g. Stand-alone software packages.
- **Ecosystem assets (E)**
  These assets collectively deliver an integrated critical service for the organisation. As such, they are managed and refreshed on a collective basis. E.g. Software and equipment assets that collectively support the Powerlink Advanced Energy Management Systems (AEMS).
- **Fleet assets (F)**
  These assets form part of a "fleet" of similar assets, which are managed and refreshed as a group, enabling efficiencies of scale in purchasing and operational management.

4. OT INVESTMENT CURRENT PERIOD SUMMARY

During the current RCP delivery of a structured OT Program of Work has progressed, consistent with the OT asset management approach described in section 3 (see page 11). Table 3 provides a summary description of key current RCP OT PoW outcomes within the seven asset categories.

Asset Category	Current Period OT Works
 *Operational computer systems and software used to manage or support the operation of the Powerlink transmission grid and telecommunications services.*	**Current period to-date:** ▪ Asset lifecycle refresh of the OT infrastructure supporting the [redacted] SCADA Control System. **Current period remainder:** ▪ Asset lifecycle upgrade of the control systems data historian [redacted] and supporting infrastructure. ▪ Asset lifecycle upgrades of OT operating systems. **Other:** ▪ As well as the asset lifecycle investments to maintain currency and supportability of OT infrastructure and systems, the NGNO program is deploying Powerlink's long-term sustainable Advanced Energy Management System (AEMS), Outage Management System (OMS), Database Integrations & Management Application (DIMA) and related software and business processes. (As the NGNO program is transformational in nature, it is managed separately from the OT Works Program).
 *Operational network security equipment and services, facilitating Access Controls, Traffic Filtering, VPN Services, Intrusion Detection & Prevention and other security functions.*	**Current period to-date:** ▪ Through the Cyber Security Program, Powerlink has uplifted its cyber security defence and response capabilities, consistent with the Australian Energy Sector Cyber Security Framework (AESCSF) [redacted] ▪ Asset lifecycle upgrade of the core OT firewalls consistent with current cyber security policies, architecture and standards. Includes transfer of configuration settings and transition into the Powerlink cyber security ecosystem (initiative currently underway). **Current period remainder:** ▪ Cyber security continuous improvement consistent with [redacted] d ad hoc threat response.
 *Specialised visualisation and communications equipment for use by operators within the Network Operations control room and other operational locations to monitor and manage the electricity transmission network and provide unified telecommunications services.*	**Current period to-date:** ▪ Asset lifecycle refresh of the [redacted] operational telephony system and related infrastructure (includes control room telephony). **Other:** ▪ The NGNO program is also delivering a Primary Control Room Refurbishment, Alternate Control Room (both of which include upgraded wallboards and workstations), Simulation Centre and Emergency Operations Centre Upgrade. (As the NGNO program is transformational in nature, it is managed separately from the OT Works Program)

Asset Category	Current Period OT Works
Data Centre Support *Physical infrastructure within Powerlink's data centres that houses OT servers, storage and networking equipment.*	**Current period to-date:** ▪ Asset lifecycle refreshes of the OT data centre automated "SMS" alerting capability. These appliances provide critical alerts when temperature, power load, fire detection or other sensor thresholds are triggered. ▪ Asset lifecycle refresh of the OT data centre Uninterruptible Power Supplies (UPSs). These units are essential to ensure smooth power supply to all equipment in the data centre and provide operational continuity during power outages until the on-site emergency power supply (genset) is started and producing stable power supply. ▪ Asset lifecycle refresh of the OT data centre Power Distribution Units (PDUs). These units distribute stable power supply to all equipment in the data centre and enable isolation of zones and racks as required. ▪ Asset lifecycle refresh of the OT data centre Automatic Transfer Switches (ATSs). These units automatically switch power from the primary power source to the backup supply upon a power outage or other supply instability.
Data Network *Data centre networking facilities enabling the interconnection of server, storage and other data equipment, and facilitating secure segregated organisational access to these services.*	**Current period to-date:** ▪ Asset lifecycle refresh of OT data network switches and fabric. This OT network infrastructure is critical to Powerlink's operational systems and communications. ▪ Asset lifecycle refresh of device authentication equipment (including core routers) and network "edge" perimeter gateway routers. **Current period remainder:** ▪ Asset lifecycle refresh of OT Access Network equipment. ▪ Upgrade or replacement of OT serial input/output racks. ▪ Upgrade or replacement of OT Load Balancers and Virtual Private Networking (VPN) infrastructure.
Servers *Server equipment hosting the OT services including application, network, communications, database and security services.*	**Current period to-date:** ▪ Asset lifecycle upgrade or replacement of the core OT operational server fleet. (currently underway)
Data Storage *Data storage and backup equipment supporting operational databases, file systems, time-series historian and other requirements.*	**Current period to-date:** ▪ Asset lifecycle replacement of OT data protection and backup system, including capacity growth enablement. **Current period remainder:** ▪ Asset lifecycle replacement of OT Core Storage Area Network (SAN) data storage infrastructure, including capacity growth enablement.

Table 3: Current RCP OT Program of Works Summary

5. OT INVESTMENT PLAN

5.1. OT Investment Summary

The 2027-32 RCP OT Investment Plan has been developed consistent with the Operational Technology Asset Management Framework (OTAMF) asset renewal guidelines and is a subset of the broader Operational Technology Asset Management Plan (OTAMP).

Total planned investment for the OT Program of Work over the period 2027-32 RCP is $89.82M[4] which represents an average annual investment of $18.0M. The profile of planned investment is shown in Figure 5 with the underpinning financial values shown in Figure 6, noting that the program's peak load occurs in the later segment of the plan (FY31-32), where significant software upgrades and associated infrastructure renewals for the AEMS, DIMA and OMS solutions are due to occur.

The vast majority of investment is driven by recurrent upgrade and renewals initiatives to ensure OT assets are prudently and efficiently managed within their defined lifecycle. A modest level of investment has been included for new capability within the cyber security stream of activity.

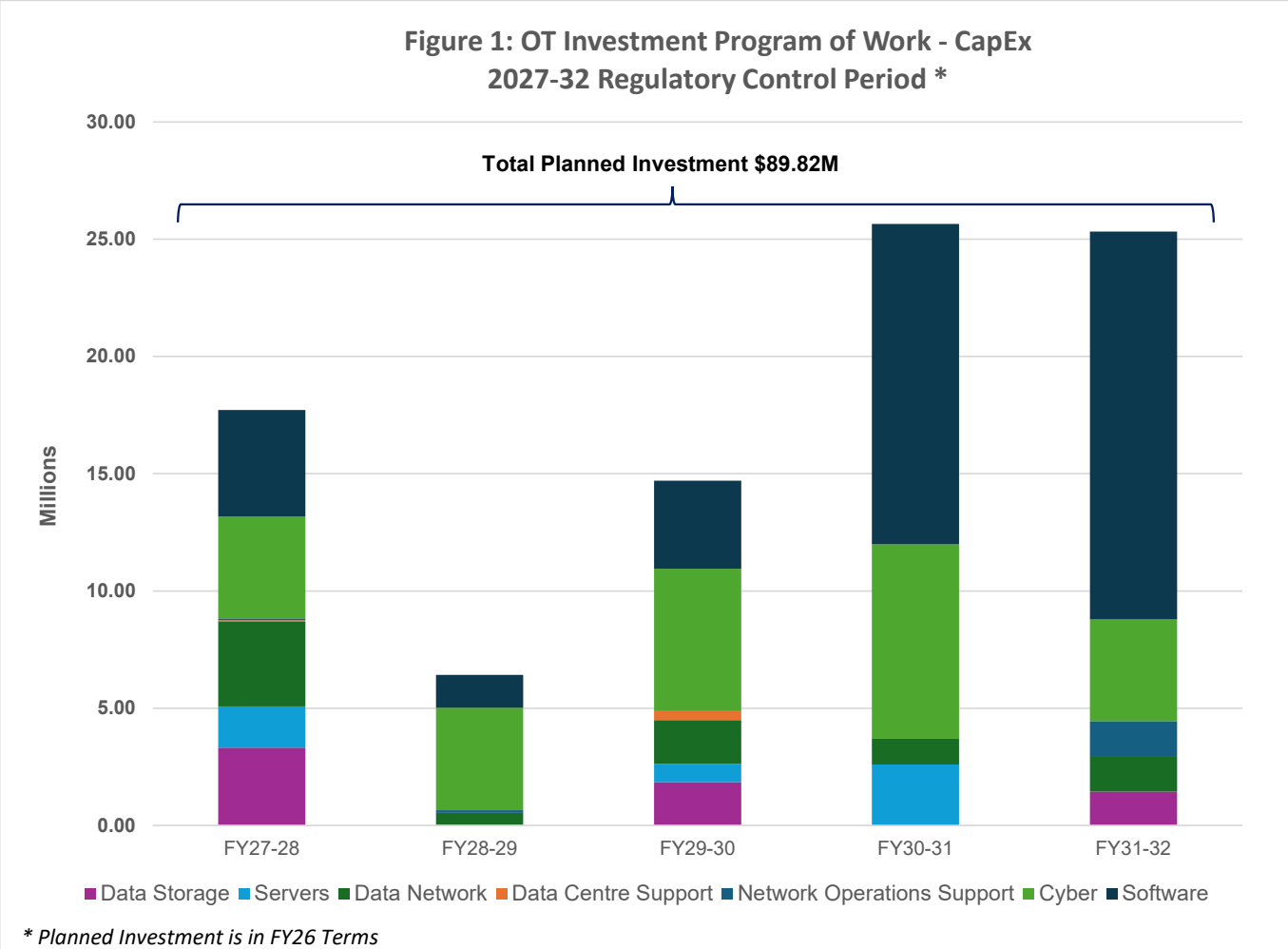


Figure 5: 2027-32 RCP OT Program of Work Investment Profile

[4] Financials for 2027-32 RCP are shown in FY26 terms.

	FY27-28	FY28-29	FY29-30	FY30-31	FY31-32	Total
Software						39,884,715
Cyber						27,385,610
Network Operations Support						1,751,050
Data Centre Support						418,040
Data Network						8,600,728
Servers						5,139,300
Data Storage						6,635,948
Total	17,719,387	6,425,256	14,699,819	25,644,303	25,326,627	89,815,391

Figure 6: 2027-32 RCP OT Program of Work Investment Summary

5.2. OT Investment Roadmap

The OT Investment Roadmap is shown in Figure 7. Approximately 44% of the investment program is focussed on maintaining operational software ecosystems, with a further 31% focussed on maintaining a robust approach to securing the OT environments from cyber security threats.

Planning of the OT Program of Work has been influenced by the following factors:

- A significant amount of new capability is being delivered through the NGNO program during the FY25-27 period. Implementation of this new capability will require an ongoing investment in software upgrades and infrastructure renewals. The OTAMP is based on the latest NGNO forecasts (at the time of preparing the document) which sees the OMS go-live occurring in March 2026 and the AEMS and DIMA go-lives occurring in August 2027. The timing of NGNO go-live dates drives the significant level of investment in the FY31-32 period. Whilst the OTAMS provides the guidance for lifecycle renewal AEMS upgrade investment is driven by the contractual arrangements agreed with the software vendor.
- Where there is tight coupling of software and infrastructure, the investment is treated as a consolidated ecosystem. E.g. AEMS Major Upgrade, Control Room Telephony Major Upgrade. This coupling is done to maximise delivery synergies and to reduce risk of multiple changes to the environments i.e. undertaking software upgrades and hardware renewal as separate activities.
- The ability to efficiently resource delivery of the Program of Work (PoW) given some key technical resource constraints. This has driven some resequencing of investment to alleviate overloads on critical and scarce resources.

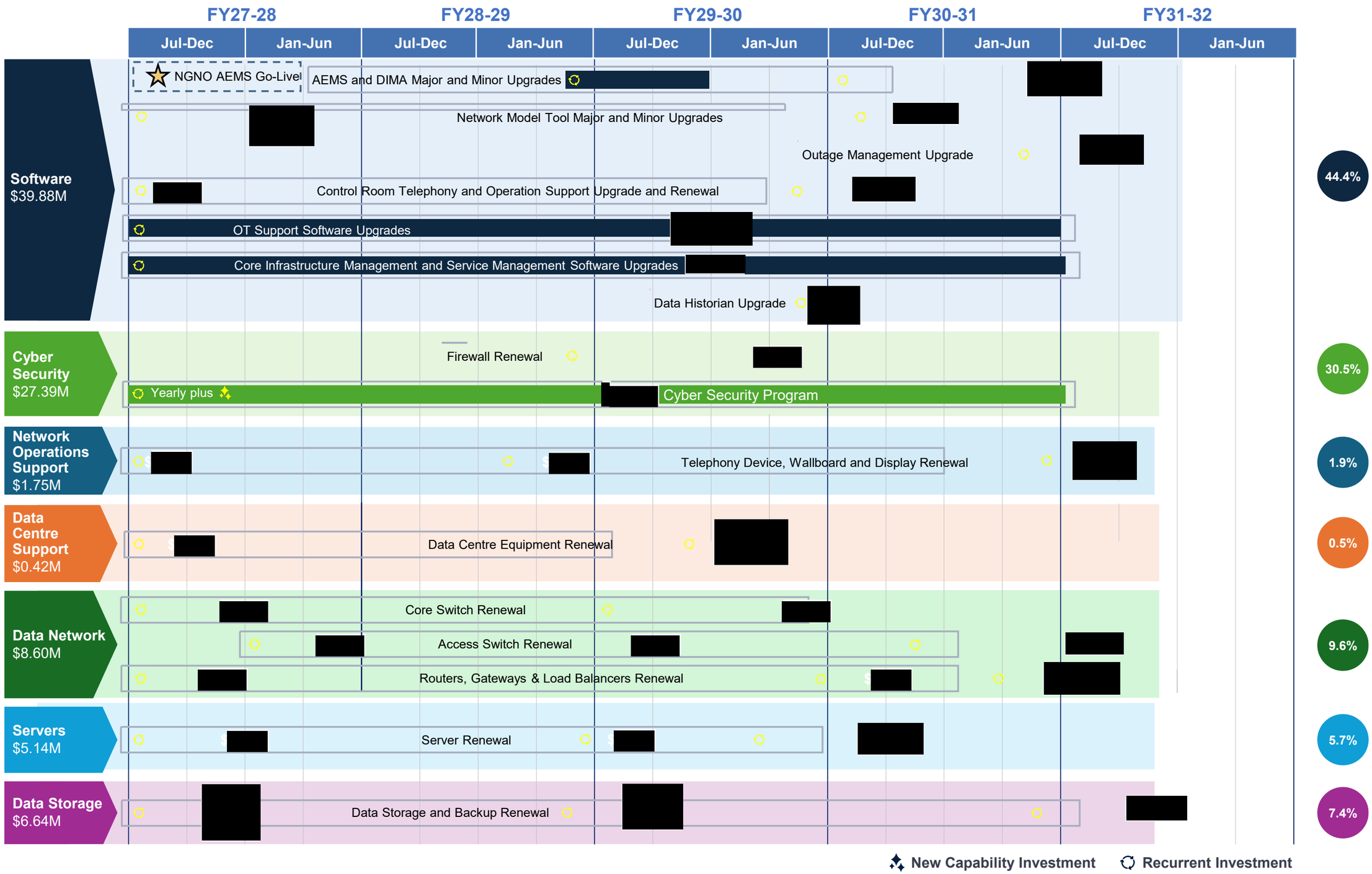


Figure 7: 2027-32 RCP OT Program of Work Roadmap

5.3. Initiative Briefs

In the following section, a one-page initiative brief has been prepared for each initiative within the seven (7) Asset Categories. In some cases, several sub-initiatives have been rolled up into an overarching initiative. In aggregate the one-page initiatives briefs correlate to the overall 5-year investment plan summarised in Section 3.2.

5.3.1. Asset Category – Software

Asset Sub-Category	Initiative Name	Initiative ID	Initiative Sub-ID(s)
Control Systems	**Advanced Energy Management System Upgrades**	**SFWAEM**	**SFW001, SFW002, SFWAEM, SFWDMA**

Overview:

This initiative will undertake software upgrades for the Advanced Energy Management System (AEMS) and Database Integrations & Management Application (DIMA). The AEMS is a foundation solution supporting control room operations across the power network. DIMA enables integration services between the AEMS and other technology platforms. These two solutions are tightly coupled, with changes in the AEMS necessitating changes in DIMA to ensure interoperability. The underpinning technology infrastructure servicing the AEMS also requires renewal on each AEMS major upgrade cycle.

Rationale:

The AEMS will go-live in FY27 as part of the NGNO Program and will then move into a recurrent upgrade cycle. The AEMS upgrade cycle is driven by contractual arrangements with the product vendor[redacted], which requires recurrent minor upgrades every 2 years and recurrent major upgrades every 4-5 years.

Risks & Issues:

Given the fundamental role that the AEMS provides in terms of power network control, it is critical that Powerlink maintains currency at n-1 software versioning. This enables Powerlink to effectively manage risk of software defects and enables Powerlink to leverage new capability delivered in new versions of the AEMS.

Considerations:

The time to perform an AEMS major upgrade is in the order of 18 months (post the initiation phase) given the criticality of the business functions it supports. Extensive analysis of new functions and their impacts needs to be undertaken as well as reconfiguration and testing of the platform on an end-to-end basis. This will require significant involvement of SMEs, technical and vendor resources.

Assumptions:

The infrastructure underpinning the AEMS will be upgraded in line with the AEMS major upgrade cycle as it is treated as part of the AEMS ecosystem

Financial:

Total Investment over 2027-32 RCP is **$27.74M** consisting of:

1. AEMS Minor Upgrade occurring in FY30 - [redacted]
2. DIMA Minor Upgrade occurring in FY30 - [redacted]
3. AEMS Major Upgrade spanning FY31-FY32 - [redacted]
4. DIMA Major Upgrade spanning FY31-FY32 - [redacted]

Timeline: *(grey shaded areas represent the initiation phase of each project)*

Sub-Initiative ID	Sub-Initiative Name	FY27/28		FY28/29		FY29/30		FY30/31		FY31/32	
		Jul-Dec	Jan-Jun	Jul-Dec	Jan-Jun	Jul-Dec	Jan-Jun	Jul-Dec	Jan-Jun	Jul-Dec	Jan-Jun
SFW001	Advanced Energy Management System (AEMS) Minor Upgrade										
SFW002	Database Integrations & Management Application (DIMA) Minor Upgrade										
SFWAEM	Advanced Energy Management System (AEMS) Major Upgrade										
SFWDMA	Database Integrations & Management Application (DIMA) Major Upgrade										

Asset Sub-Category	Initiative Name	Initiative ID	Initiative Sub-ID(s)
Control Systems	**Network Modelling Tools Upgrade**	**SFWNMT**	**SFW003, SFWODM**

Overview:

Network modelling tools play a crucial role in planning for changes to the Powerlink Network including determining data points and settings in the Energy Management System. Maintenance of currency of these tools is essential, particularly as the profile of generator connections and associated transmission changes with a shift to increasing renewables. This initiative plans for minor and major updates following vendor release cycles.

Rationale:

The upgrade cycle of network modelling tools is driven by the Asset Management Strategy which defines an upgrade cycle of 5 years. It should be noted that some software patches would be applied as part of business-as-usual.

Risks & Issues:

As the profile of generator connections to the transmission network changes, the variety of models will increase and so the volume and complexity of testing associated with an upgrade also increases.

Considerations:

There may be a need to align updates to the operational network modelling suite with other related tools used in Network Planning.

Assumptions:

There is no need or desire to change the product used to perform this function

Financial:

Total Investment over 2027-32 RCP is **$4.44M** consisting of:

1. ODMS Major Upgrade spanning FY28-FY29 - [redacted]
2. ODMS Minor Upgrade occurring in FY31 - [redacted]

Timeline: *(grey shaded areas represent the initiation phase of each project)*

Sub-Initiative ID	Sub-Initiative Name	FY27/28				FY28/29				FY29/30				FY30/31				FY31/32			
		Jul-Dec		Jan-Jun		Jul-Dec		Jan-Jun		Jul-Dec		Jan-Jun		Jul-Dec		Jan-Jun		Jul-Dec		Jan-Jun	
SFW003	PQ Network Model Tool Minor Upgrade (ODMS)																				
SFWODM	PQ Network Model Tool Major Upgrade (ODMS)																				

Asset Sub-Category	Initiative Name	Initiative ID	Initiative Sub-ID(s)
Control Systems	**Outage Management Upgrade**	**SFWOMS**	**SFWOMS**

Overview:

The Outage Management System is the tool used for managing planned and unplanned outages to the High Voltage (HV) Network. Alongside the AEMS, this is a primary tool used by Real Time Network Operations to provide surety of network resilience and certainty of supply. Keeping this software updated will ensure that it remains within vendor support parameters and is a reliable tool.

Rationale:

The OMS will go-live in FY26 as part of the NGNO Program and will then move into a recurrent upgrade cycle. The OMS upgrade cycle is driven by the Asset Management Strategy which defines an upgrade cycle of 5 years. It should be noted that some software patches would be applied as part of business-as-usual.

Risks & Issues:

Given the fundamental role that the OMS provides in terms of power network control, it is critical that Powerlink maintain currency at n-1 software versioning. This enables Powerlink to effectively manage risk of software defects and enables Powerlink to leverage new capability delivered in new versions of the OMS.

Considerations:

The time to perform an OMS upgrade is in the order of 10 months given the criticality of the business functions it supports. Extensive analysis of new functions and their impacts need to be undertaken as well as reconfiguration and testing of the platform on an end-to-end basis. This will require significant involvement of business SME, technical and vendor resources.

Assumptions:

The OMS upgrade will run in parallel to the AEMS major upgrade albeit with a planned go-live in Q3 FY32. Running in parallel enables synergies in term of project management oversight and integrated testing with the AEMS

Financial:

Total Investment over 2027-32 RCP is **$2.58M** consisting of OMS Upgrade occurring in FY32.

Timeline:

Sub-Initiative ID	Sub-Initiative Name	FY27/28		FY28/29		FY29/30		FY30/31		FY31/32	
		Jul-Dec	Jan-Jun	Jul-Dec	Jan-Jun	Jul-Dec	Jan-Jun	Jul-Dec	Jan-Jun	Jul-Dec	Jan-Jun
SFWOMS	Outage Management System (OMS) Upgrade										

Asset Sub-Category	Initiative Name	Initiative ID	Initiative Sub-ID(s)
Control Systems	**Control Systems Software Upgrades**	**SFWCSY**	**SFW004, SFW005**

Overview:

This initiative includes key systems used in the Network Operations environment outside of the primary energy management system, outage management and integration tools. It includes updates to the Control Room telephony system to maintain currency and support within vendor parameters.

Rationale:

The upgrade cycle of control systems software is driven by the Asset Management Strategy which defines an upgrade cycle of 6 years. It should be noted that some software patches would be applied as part of business-as-usual.

Risks & Issues:

Final implementation of an upgrade will likely require a brief outage in primary telecommunication for the Control Room that will need to be planned to minimise disruption.

Considerations:

Scheduling of major upgrades is planned aligned to vendor published support and maintenance dates. Careful review of release notes and comprehensive testing is required to ensure that no core or essential functionality is deprecated in a release.

Assumptions:

Telephony end point devices will be upgraded alongside a software upgrade

Financial:

Total Investment over 2027-32 RCP is **$1.26M** consisting of:

1. Control Room Telephony Minor Upgrade occurring in FY28 - [redacted]
2. Control Room Telephony Major Upgrade occurring in FY31 - [redacted]

Timeline:

Sub-Initiative ID	Sub-Initiative Name	FY27/28		FY28/29		FY29/30		FY30/31		FY31/32	
		Jul-Dec	Jan-Jun	Jul-Dec	Jan-Jun	Jul-Dec	Jan-Jun	Jul-Dec	Jan-Jun	Jul-Dec	Jan-Jun
SFW004	Control Room Telephony Minor Upgrade										
SFW005	Control Room Telephony Major upgrade										

Asset Sub-Category	Initiative Name	Initiative ID	Initiative Sub-ID(s)
OT Support	**Data Historian Capability Renewal**	**SFWDNA**	**SFW008B**

Overview:

Data Insights and Analytics tools, including historians, are an integral component of the energy management ecosystem. This initiative upgrades the existing data historian capability to provide better real time information to support decision making, analysis of incidents and caters for the growth in data volumes relating to the increasing scale of the transmission network.

Rationale:

The capability renewal is driven by the ever-growing base of data flowing from the operational network and the need for sophisticated decision support based on real-time data. The upgrade cycle of data insights and analytics tools is driven by the Asset Management Strategy which defines an upgrade cycle of 5 years, noting that some software patches would be applied as part of business-as-usual processes.

Risks & Issues:

With increasing diversity and expansion of the power network the volume of data points being collected and used for decision making is increasing steadily and so all elements of the ecosystem – data, software, network performance, server and storage capacity will need to be considered in planning

Considerations:

Changes in product ownership have impacted commercial models associated with product licensing including data volumetric licensing that will need to be considered in planned changes. Improvements in use of data and analytics can provide efficiency benefits in both real time network operations and network planning.

Assumptions:

There is no need or desire to change software product or vendor in this period.

All systems in this category will remain 'on-premises' for this period.

Financial:

Total Investment over 2027-32 RCP is **$0.13M** consisting of Data Historian Upgrade occurring in FY31.

Timeline:

Sub-Initiative ID	Sub-Initiative Name	FY27/28		FY28/29		FY29/30		FY30/31		FY31/32	
		Jul-Dec	Jan-Jun	Jul-Dec	Jan-Jun	Jul-Dec	Jan-Jun	Jul-Dec	Jan-Jun	Jul-Dec	Jan-Jun
SFW008B	Data Historian Upgrade										

Asset Sub-Category	Initiative Name	Initiative ID	Initiative Sub-ID(s)
OT Support	**OT Support Software Upgrades**	**SFWOTS**	**SFW009, SFW010, SFW011, SFW012B**

Overview:

A suite of operational tools such as digital and telephony network management systems, security incident and event monitoring and dynamic load rating provide essential telemetry and configuration management services to support reliable operation of the OT network including incident analysis, diagnosis and recovery. Regular updating of these tools ensures that they maintain support and currency for their important role.

Rationale:

The upgrade cycle of operational tools is driven by the OT Asset Management Strategy which defines an upgrade cycle of 5 years. It should be noted that some software patches would be applied as part of business-as-usual activities.

Risks & Issues:

In house developed or highly customised systems will require assessment across the delivery stack to ensure all elements are considered in the upgrade planning and that testing fully exercises all essential requirements to maintain capability.

Considerations:

Access to and the ability to perform upgrades will require appropriate commercial arrangements and licensing to be in place and maintained.

Vendor release and support cycles will inform detailed scheduling and planning.

The degree of integration or dependence on other systems will also inform planning.

Assumptions:

To maintain support currency and cyber resilience there will be an ongoing need to maintain systems.

Financial:

Total Investment over 2027-32 RCP is **$1.95M** consisting of:

1. Network Management Systems Minor Upgrade spanning FY28-FY32 - [redacted]
2. Network Monitoring System Upgrade in FY29 - [redacted]
3. Dynamic Load Rating Software Minor Upgrade occurring in FY31 - [redacted]
4. Security Information and Event Management System Minor Upgrade occurring in FY28 and recurring in FY32 [redacted]

Timeline:

Sub-Initiative ID	Sub-Initiative Name	FY27/28		FY28/29		FY29/30		FY30/31		FY31/32	
		Jul-Dec	Jan-Jun	Jul-Dec	Jan-Jun	Jul-Dec	Jan-Jun	Jul-Dec	Jan-Jun	Jul-Dec	Jan-Jun
SFW009	Network Monitoring System Upgrade										
SFW010	Security Information and Event Management System Minor Upgrade										
SFW011	Dynamic Load Rating Software Minor Upgrade										
SFW012B	Network Management Systems Minor Upgrade										

Asset Sub-Category	Initiative Name	Initiative ID	Initiative Sub-ID(s)
OT Core Infrastructure	**Core Infrastructure Management Software Upgrades**	**SFWCIN**	**SFW013, SFW014, SFW015**

Overview:

This initiative incorporates maintenance and upgrades of a range of underpinning software and tools for the OT environment ranging from server operating systems to the service management tool used for technology incident, service request and change management. Maintaining currency of these systems ensure that they are able to be updated for cyber and business resiliency and improved functionality can be leveraged as required.

Rationale:

The upgrade cycle of core infrastructure management tools is driven by the Asset Management Strategy which defines an upgrade cycle of 4 years. It should be noted that some software patches would be applied as part of business-as-usual.

Risks & Issues:

Formal vendor certification of compatibility of software with operating system may be required for some systems.

Considerations:

Access to and the ability to perform upgrades will require appropriate commercial arrangements and licensing to be in place and maintained.

Vendor release and support cycles will inform detailed scheduling and planning.

The degree of integration or dependence on other systems will also inform planning.

Assumptions:

To maintain support currency and cyber resilience there will be a constant need to maintain systems including operating systems.

All systems in this category will remain 'on-premise' for this period.

Financial:

Total Investment over 2027-32 RCP is **$1.78M** consisting of:

1. Miscellaneous Software Tools Minor Upgrade spanning FY28-FY32 - [redacted]
2. Operating Systems Upgrade occurring in FY28 and recurring in FY32 - [redacted]
3. Configuration Management Tools Minor Upgrade occurring in FY28 and recurring in FY32 - [redacted]

Timeline:

Sub-Initiative ID	Sub-Initiative Name	FY27/28		FY28/29		FY29/30		FY30/31		FY31/32	
		Jul-Dec	Jan-Jun	Jul-Dec	Jan-Jun	Jul-Dec	Jan-Jun	Jul-Dec	Jan-Jun	Jul-Dec	Jan-Jun
SFW013	Operating Systems Upgrade										
SFW014	Miscellaneous Softw are Tools Minor Upgrade										
SFW015	Configuration Management Tools Minor Upgrade										

5.3.2. Asset Category – Cyber Security

Asset Sub-Category	Initiative Name	Initiative ID	Initiative Sub-ID(s)
Security Infrastructure	**Security Infrastructure Renewal**	**CYSSIN**	**SCF002, SCF004**

Overview:

Regular updates and upgrades to cyber security infrastructure are an essential component of defence in a contemporary energy management environment. These upgrades also provide a foundation component of maintaining compliance with the AESCSF. This initiative primarily encompasses updating and upgrading of firewalls on a regular cycle. Firewalls encompass protection of the OT core, the SCADA network and operational offices.

Rationale:

The upgrade cycle of cyber security infrastructure is driven by the Asset Management Strategy which defines an upgrade cycle of 5 years. This also ensures the equipment remains within vendor support and maintenance parameters.

Risks & Issues:

Given the fundamental role that the core cyber security infrastructure including firewalls provides in terms of power network control, it is critical that Powerlink maintain currency.

Considerations:

Vendor release and support cycles will inform detailed scheduling and planning, as will compatibility across the environment.

Core cyber security architecture and services for OT are planned alongside IT to maintain consistency and maximise protection.

Assumptions:

Growth capacity will be considered in selecting the equipment for the renewal

Financial:

Total Investment over 2027-32 RCP is **$5.67M** consisting of:

1. Core Firewall Renewal (OT) occurring in FY31 - [redacted]
2. Edge Firewall Renewal (SCADA, Internet) occurring in FY30 - [redacted]

Timeline:

Sub-Initiative ID	Sub-Initiative Name	FY27/28		FY28/29		FY29/30		FY30/31		FY31/32	
		Jul-Dec	Jan-Jun	Jul-Dec	Jan-Jun	Jul-Dec	Jan-Jun	Jul-Dec	Jan-Jun	Jul-Dec	Jan-Jun
SCF002	Core Firew all Renew al (OT)										
SCF004	Edge Firew all Renew al (SCADA, Internet)										

Asset Sub-Category	Initiative Name	Initiative ID	Initiative Sub-ID(s)
Security Software & Services	**Cyber Program and OT Security Services Upgrades**	**CYSSSS**	**SCFISM, SCF005A**

Overview:
Powerlink's Cyber Security Program provides centralised governance, risk management, assurance and delivery of cyber security initiatives across the organisation's Information Technology (IT), OT and Secondary Systems Field environments. The Cyber Security Program consists of three primary initiatives being:

1. Sustaining cyber security defence maturity
2. SOCI Act and ASD guidance
3. Managing the evolving cyber security threat

Further detail on these initiatives is provided in the Information Technology & Operational Technology Investment Program Cyber Security Program Preliminary Business Case

Rationale:
The rapid growth of the cyber security threat within Australia and around the world is well documented. Complex critical infrastructure organisations such as Powerlink present attractive targets. In the past decade, governments have become increasingly focussed on the resilience of critical infrastructure and have sought to ensure that services are protected against a wide range of threats. Prudent and efficient management of strong cyber security defences is therefore inherent in Powerlink's responsibilities to the Australian community. Through the Cyber security Program and related investments, Powerlink will continue to ensure compliance with legislative and regulatory requirements through defined and targeted risk management practices, preparedness, prevention and resilience, and with necessary information exchange between industry and government.

Risks & Issues:
Maintaining the AESCSF [redacted] security defence maturity is not a set-and-forget proposition. Instead, Powerlink must continue to invest to adapt and extent our cyber security capabilities to address the growing threat.

Considerations:
Continued investment in cyber activities are required to meet government cyber compliance requirements, which necessitates an ongoing assurance program of works.

Assumptions:
Powerlink will be required to maintain the security defence maturity.

Financial:
Total Investment over 2027-32 RCP is **$21.71M** consisting of:

1. Cyber Security Program (OT) spanning FY28-FY32 - [redacted]
2. Security Management and Services Upgrades spanning FY28-FY32 [redacted]

Timeline:

Sub-Initiative ID	Sub-Initiative Name	FY27/28		FY28/29		FY29/30		FY30/31		FY31/32	
		Jul-Dec	Jan-Jun	Jul-Dec	Jan-Jun	Jul-Dec	Jan-Jun	Jul-Dec	Jan-Jun	Jul-Dec	Jan-Jun
SCFISM	Cyber Security Program (OT)										
SCF005A	Security Management and Services Upgrades										

5.3.3. Asset Category – Network Operations Support

Asset Sub-Category	Initiative Name	Initiative ID	Initiative Sub-ID(s)
Telephony Systems **Network Ops Workstations** **Network Operations Displays**	**Network Operations Device Renewal**	**NOSTWD**	**NOS002, NOS003, NOS004**

Overview:

This initiative encompasses the key physical infrastructure in the Network Operations environment. It ensures that the physical technology infrastructure, used 24/7 in the environment, is maintained and updated on a regular basis to conform to and comply with NER but also to maintain timely support, repair and update in the event of failure. The initiative includes real time, large format displays in the Control Rooms and desktop workstations used to access and operate the energy management system.

Rationale:

The upgrade cycle of Network Operations technology infrastructure is driven by the Asset Management Strategy which defines upgrade cycles of 4 years for desktop devices up to 7 years for wallboards.

Risks & Issues:

Ensuring reliable and robust equipment is maintained in the Control Room is foundational to providing Network Operations services.

As the Control Room environment is a 24/7 operation all changes need to be carefully planned and scheduled to ensure that they are minimally disruptive.

Considerations:

Vendor release and support cycles will inform detailed scheduling and planning, as will compatibility across the environment.

Assumptions:

Refresh of this equipment will only be required at the primary and one business continuity site.

Financial:

Total Investment over 2027-32 RCP is **$1.75M** consisting of:

1. Dashboard Display Renewal occurring in FY28 - [redacted]
2. OT Workstation Renewal spanning FY29-FY30 - [redacted]
3. OT Wallboard Renewal occurring in FY32 - [redacted]

Timeline:

Sub-Initiative ID	Sub-Initiative Name	FY27/28		FY28/29		FY29/30		FY30/31		FY31/32	
		Jul-Dec	Jan-Jun	Jul-Dec	Jan-Jun	Jul-Dec	Jan-Jun	Jul-Dec	Jan-Jun	Jul-Dec	Jan-Jun
NOS002	OT Workstation Renewal										
NOS003	OT Wallboard Renewal										
NOS004	Dashboard Display Renewal										

5.3.4. Asset Category – Data Centre Support

Asset Sub-Category (s)	Initiative Name	Initiative ID	Initiative Sub-ID(s)
UPS & Batteries **SMS Alerting**	**Data Centre Equipment Renewal**	**DCSEQP**	**DCS002, DCS006**

Overview:

Underpinning all critical equipment and services in the operational technology environment are the primary and secondary data centres that house them. Maintaining these centres to a high standard is essential for the reliability of the network. This initiative, primarily, covers power management in the data centre environment and includes renewal of UPS units, UPS batteries and power distribution within the data centres. This is essential to ensure that consistent power is maintained to essential services during any power variation event. The initiative also includes maintenance of services that notify support staff of alarms and any variation from expected environmental parameters such as temperature, humidity and power readings. It also includes planned refresh of racks housing the equipment.

Rationale:

The upgrade cycle of data centre equipment is driven by the Asset Management Strategy which defines upgrade cycles of 5 years for alert appliances and UP batteries, 10 years for power management equipment including UPS units to 20 years for racks.

Risks & Issues:

Core power management equipment needs to be maintained within vendor support parameters to ensure continued support, maintenance and reliability in the event it is required.

Considerations:

Redundancy has been built into the designs for these services, but this may need to be temporarily reduced during cutover activities.

Assumptions:

Data centre metrics will not alter significantly during the refresh period.

There will not be any material or significant migration to cloud for core OT systems.

Financial:

Total Investment over 2027-32 RCP in **$0.42M** consisting of:

1. Data Centre SMS Appliance Renewal occurring in FY28 - [redacted]
2. Data Centre UPS and Battery Renewal occurring in FY30 - [redacted]

Timeline:

Sub-Initiative ID	Sub-Initiative Name	FY27/28		FY28/29		FY29/30		FY30/31		FY31/32	
		Jul-Dec	Jan-Jun	Jul-Dec	Jan-Jun	Jul-Dec	Jan-Jun	Jul-Dec	Jan-Jun	Jul-Dec	Jan-Jun
DCS002	Data Centre UPS Battery Renewal										
DCS006	Data Centre SMS Appliance Renewal										

5.3.5. Asset Category – Data Network

Asset Sub-Category (s)	Initiative Name	Initiative ID	Initiative Sub-ID(s)
Core Switches	**Core Switch Renewal**	**DNWCSW**	**DNS001A, DNS001B, DNS002A, DNS002B**

Overview:

This initiative is for the core 'head end' OT network equipment. The 'head end' network is a critical component of the power management ecosystem and regular maintenance, and refresh is essential to ensure reliability and resilience. Included in this initiative are the core switches and associated extension switches at primary and business continuity sites.

Rationale:

The upgrade cycle of core network equipment is driven by the Asset Management Strategy which defines an upgrade cycle of 5 years for all equipment.

Risks & Issues:

The core switches are configured as a fault tolerant, highly available environment but there will be some compromise of resilience whilst changeovers occur. Planning with all stakeholders will be undertaken to minimise disruption.

Considerations:

Existing commercial arrangements should be able to be leveraged for these purchases to maintain consistency and compatibility in the fleet.

Assumptions:

Refresh of these switches will only be required at the primary and one business continuity site.

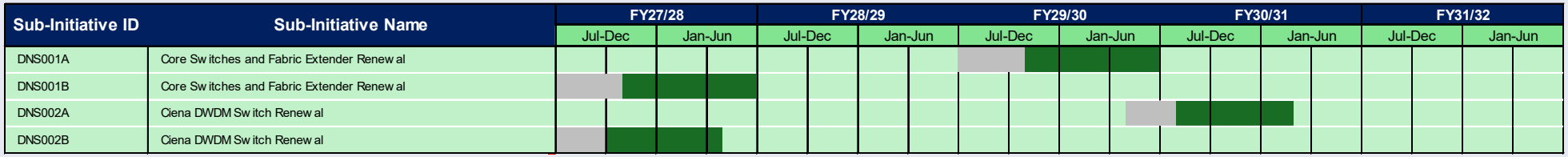
These services will remain 'on-premises' for the refresh period.

Financial:

Total Investment over 2027-32 RCP is **$4.09M** consisting of:

1. Core Switch Renewal (Tranche B) occurring in FY28 - [redacted]
2. Ciena DWDM Switch Renewal (Tranche B) occurring in FY28 - $[redacted]
3. Core Switch Renewal (Tranche A) occurring in FY30 - [redacted]
4. Ciena DWDM Switch Renewal (Tranche A) occurring in FY31 - [redacted]

Timeline:



Asset Sub-Category (s)	Initiative Name	Initiative ID	Initiative Sub-ID(s)
Access Switches	**Access Switch Renewal**	**DNWACS**	**DNS004, DNS005A, DNS005B**

Overview:

This initiative incorporates primary 'head end' OT network equipment from the core to the edge. The 'head end' network is a critical component of the power management ecosystem and regular maintenance, and refresh is essential to ensure reliability and resilience. Included in this initiative is the equipment beyond the core switches at primary and business continuity sites such as distribution and access switches in data centres, authentication services to facilitate access by verified devices and edge switches to manage connections at sites.

Rationale:

The upgrade cycle of network equipment is driven by the Asset Management Strategy which defines an upgrade cycle of 5 years for all equipment.

Risks & Issues:

Considerations:

Existing commercial arrangements should be able to be leveraged for these purchases to maintain consistency and compatibility in the fleet.

Assumptions:

Refresh of these switches will only be required at the primary and one business continuity site.

These services will remain 'on-premise' for the refresh period.

Financial:

Total Investment over 2027-32 RCP is **$3.00M** consisting of:

1. Access Network (OT) Renewal B occurring in FY28-FY29 - [redacted]
2. Authentication Service Renewal occurring in FY30 - [redacted]
3. Access Network (OT) Renewal A spanning FY31-FY32 - [redacted]

Timeline:

Sub-Initiative ID	Sub-Initiative Name	FY27/28		FY28/29		FY29/30		FY30/31		FY31/32	
		Jul-Dec	Jan-Jun	Jul-Dec	Jan-Jun	Jul-Dec	Jan-Jun	Jul-Dec	Jan-Jun	Jul-Dec	Jan-Jun
DNS004	Authentication Service Renewal										
DNS005A	Access Network (OT) Renewal										
DNS005B	Access Network (OT) Renewal										

Asset Sub-Category (s)	Initiative Name	Initiative ID	Initiative Sub-ID(s)
Routers, Gateways & Load Balancers	**Routers, Gateways, Load Balancer Renewal**	**DNWRGL**	**DNR002, DNR003A, DNR003B**

Overview:

Alongside firewalls and core network equipment, access to and use of the network is managed by routers, gateways and load balancers. Maintenance and refresh of this equipment also significantly contributes to network reliability and resilience. This initiative incorporates upgrades to VPN equipment, routers and load balancers.

Rationale:

The upgrade cycle of core network access and management equipment is driven by the Asset Management Strategy which defines an upgrade cycle of 5 years for all equipment.

Risks & Issues:

These are common services for the environment with little or no business tolerance for any outage, so the transition to and commissioning of replacement equipment will need to be planned and co-ordinated.

Considerations:

Existing commercial arrangements should be able to be leveraged for these purchases to maintain consistency and compatibility in the fleet.

Assumptions:

Refresh of these switches will only be required at the primary and one business continuity site.

These services will remain 'on-premise' for the refresh period.

Financial:

Total Investment over 2027-32 RCP is **$1.51M** consisting of:

1. Load Balancer Renewal – B occurring in FY28 - [redacted]
2. Edge Router Renewal occurring in FY31 [redacted]
3. Load Balancer Renewal – A spanning FY31-FY32 - [redacted]

Timeline:

Sub-Initiative ID	Sub-Initiative Name	FY27/28		FY28/29		FY29/30		FY30/31		FY31/32	
		Jul-Dec	Jan-Jun	Jul-Dec	Jan-Jun	Jul-Dec	Jan-Jun	Jul-Dec	Jan-Jun	Jul-Dec	Jan-Jun
DNR002	Edge Router Renew al										
DNR003A	Load Balancer Renew al - A										
DNR003B	Load Balancer Renew al - B										

5.3.6. Asset Category – Servers

Asset Sub-Category (s)	Initiative Name	Initiative ID	Initiative Sub-ID(s)
Servers, Clock Appliances & High-end Workstations	**Servers, Clock Appliances & High-end Workstation Renewal**	**SVRSVR**	**SVS002A, SVS002B, SVS004**

Overview:

Powerlink maintains a fleet of physical and virtual servers, housed in its data centres, to host all operational technology systems. The server fleet encompasses all environments across development, test, simulation, production and business continuity to provide a fault resilient and highly available domain. To ensure that the fault resiliency and availability is not compromised, regular maintenance and refresh of the fleet is required. This initiative incorporates servers, clock appliances and other peripheral equipment for all systems and services apart from the energy management system, the infrastructure refresh of which is covered by SFWAEM.

Rationale:

The upgrade cycle of server equipment is driven by the Asset Management Strategy which defines upgrade cycles of 5 years for servers and 10 years for clock appliances.

Risks & Issues:

Most of this equipment underpins critical and important business systems in a fault tolerant and highly available environment. Refreshes will be planned to maintain overall capacity and availability in the environment with planned outages minimised.

Considerations:

Existing commercial arrangements should be able to be leveraged for these purchases to maintain consistency and compatibility in the fleet.

Assumptions:

Outside of the Energy Management System, most other systems are able to be hosted in a virtualised environment.

There will not be any material or significant migration to cloud for core OT systems.

Financial:

Total Investment over 2027-32 RCP is **$5.14M** consisting of:

1. OT Server Renewal – B occurring in FY28 - [redacted]
2. High-end Workstation Renewal occurring in FY30 - [redacted]
3. OT Server Renewal – A occurring in FY31 - [redacted]

Timeline:

Sub-Initiative ID	Sub-Initiative Name	FY27/28		FY28/29		FY29/30		FY30/31		FY31/32	
		Jul-Dec	Jan-Jun	Jul-Dec	Jan-Jun	Jul-Dec	Jan-Jun	Jul-Dec	Jan-Jun	Jul-Dec	Jan-Jun
SVS002A	OT Server Renewal - A										
SVS002B	OT Server Renewal - B										
SVS004	High-end Workstation Renewal										

5.3.7. Asset Category – Data Storage

Asset Sub-Category (s)	Initiative Name	Initiative ID	Initiative Sub-ID(s)
Storage Area Networks & Backup System	**Storage and Backup Systems**	**DSTSAB**	**DSN001A, DSN001B, DSB001**

Overview:

Powerlink maintains fault tolerant and highly available storage and backup for the OT environment and platforms. This includes hyperconverged, highly performant equipment and services across multiple data centres. Securely storing and protecting data within the OT environment is essential to maintaining integrity of network control and operations. This initiative includes the upgrade and refresh of storage area network (SAN) and backup solutions.

Rationale:

The upgrade cycle of storage equipment is driven by the Asset Management Strategy which defines an upgrade cycle of 7 years for storage and backup appliances.

Risks & Issues:

Storage and backup solutions are common services for the environment with little or no business tolerance for any outage, so the transition to and commissioning of any new solution will need to be planned and co-ordinated.

Considerations:

The growth of data collected, stored and processed across the OT environment will continue steadily as the power network evolves and so storage and backup solutions will need to be expandable and adaptable to accommodate the growth. A minimum growth of 100% on existing capacity over 5 years should be considered.

Testing the market at the time of refresh may be required.

Assumptions:

Storage and Backup solutions will remain 'on-premise' for the refresh period.

There will not be any material or significant migration to cloud for core OT systems.

Financial:

Total Investment over 2027-32 RCP is **$6.64M** consisting of:

1. Core SAN and Fabric Switching – A occurring in FY28 - [redacted]
2. Core SAN and Fabric Switching – B occurring in FY30 - [redacted]
3. Core Data Protection occurring in FY32 - [redacted]

Timeline:

Sub-Initiative ID	Sub-Initiative Name	FY27/28		FY28/29		FY29/30		FY30/31		FY31/32	
		Jul-Dec	Jan-Jun	Jul-Dec	Jan-Jun	Jul-Dec	Jan-Jun	Jul-Dec	Jan-Jun	Jul-Dec	Jan-Jun
DSN001A	Core SAN and Fabric Switching - A										
DSN001B	Core SAN and Fabric Switching - B										
DSB001	Core Data Protection										

6. OT GOVERNANCE

6.1. Measurement of Effectiveness

Powerlink's OT business function is continuously improving the processes of OT Asset Management. This includes a focus on program delivery planning and governance.

Delivery effectiveness of the OT investment plan will be measured on the following three (3) dimensions:

1. Achievement of the overall program on time, on cost and consistent with planning business outcomes;
2. Delivery of individual plan initiatives against the agreed timeframe and funding windows; and
3. Annual assessment of the OT asset risk profile at an aggregate level, ensuring upgrades and renewals are contributing to maintaining Powerlink's residual risk within agreed tolerance levels.

Further planned measurement improvements may include:

- Key Performance Indicators (KPIs). E.g. Mean Time Between Failure (MTBF), Mean Time to Repair, (MTTR), Overall Equipment Effectiveness (OEE).
- Asset Utilisation Rates measuring how efficiently assets are being utilised.
- Asset Performance Monitoring through tracking the health and performance of assets over their lifecycle.
- Asset Lifecycle Cost Analysis where total cost of owning and operating an asset throughout its lifecycle is analysed to inform further upgrade and renewal investment.
- Enhanced Compliance Management focussing on achievement of compliance with regulatory and legal obligations.

6.2. Plan Review and Update

The OT investment plan, which forms part of the OTAMP, will be reviewed on an annual basis to ensure it remains relevant and provides the necessary information to inform upgrade and renewal investment in OT assets. Elements considered in the review of the plan may include:

- Measurement of asset performance over the prior year.
- New and emerging trends in technology capability.
- Increasing requirements to ensure Powerlink assets are protected from evolving cyber-security threats.
- Changing technology standards.
- Changes to business plans and objectives.
- Emerging opportunities for improvement in the way OT services are delivered.
- Changing stakeholder and customer expectations of Powerlink.
- Changes to regulatory standards and requirements including evolution of the NEM.

6.3. OT Program Delivery Model

The OT Leadership team will oversee delivery performance of the program through a quarterly review process which will focus on:

- Project initiation cycle times;
- Resource allocation and optimisation across the PoW; and
- Individual project performance against agreed time, cost and quality metrics.

Contact us

Registered office	33 Harold St Virginia Queensland 4014 ABN 82 078 849 233
Postal address	PO Box 1193 Virginia Queensland 4014
Telephone	+61 7 3860 2111 (during business hours)
Email	pqenquiries@powerlink.com.au
Website	powerlink.com.au
Social	