2023-27
POWERLINK QUEENSLAND REVENUE PROPOSAL

Supporting Document – PUBLIC

IT07 Cybersecurity Maturity 2023-27

IT07 Cybersecurity Maturity 2023-2027

Contents

EXECUTIVE SUMMARY

This investment case documents the justification for planned investment in cybersecurity management capability and infrastructure for Business IT only. It is based on the planning undertaken to date, the estimated costs (development, implementation, ongoing operations and maintenance), the anticipated business value to be gained and the associated risks.

It is proposed to invest in cybersecurity management capability and process improvement through the FY22/23 to FY26/27 regulatory period (referred to herein as 2023-27). The proposed investment is required to address the following drivers:

- Requirement to mitigate Powerlink's known, emerging and future cybersecurity risks within an appropriate managed risk profile.

  Powerlink is moving to a greater dependence on its digital assets and business processes through its data strategy and mobility initiatives. This requires mature, sophisticated and comprehensive security controls and processes to protect and make resilient critical information assets and systems which are central to Powerlink's operations and success. Powerlink's Information Security Strategy is risk based and in order to understand those risks Powerlink periodically undertakes formal threat and risk assessments of its cybersecurity exposure and acts on risks identified through these assessments to ensure a prudent residual risk position. An ongoing assurance program ensures that all controls maintain their effectiveness against current, emerging and future threats to Powerlink's information assets and systems.

- Requirement to perform information security practices at a maturity consistent with the broader industry, in line with government and community expectations, and in an environment of growing threat sophistication and complexity.

  Powerlink follows the Australian Energy Sector Cyber Security Framework (AESCSF), an information security maturity framework developed by industry and government in 2018. Under the AESCSF transmission network providers are expected to achieve and maintain a higher level of maturity in security practices than the broader industry.

This investment will ensure that Powerlink continues to address new and increasingly sophisticated cybersecurity threats while keeping information security related risk at a level that is commensurate with Powerlink's corporate risk appetite and in line with the government and community expectations of critical infrastructure operators. Powerlink will use a mature, AESCSF aligned Information Security Management System (ISMS) to identify and implement new security controls and practices (or enhance existing controls and practices) to manage these risks.

The following three options are considered:

- **Option 1: Base Case (counterfactual) – Maintain security practices at AESCSF SP-2 maturity (as achieved at the end of the 18/22 period) and sustain existing security risk management practices.**
- **Option 2: Continue to proactively mitigate known risks and manage with industry-typical practices, which may incrementally increase some AESCSF practices beyond SP-2 (Recommended)**
- **Option 3: Proactively mitigate known risks and uplift security practices to AESCSF SP-3 maturity.**

It is recommended that Option 2 be implemented as the least cost solution to meet the identified need. Total forecast non-network (IT) expenditure for the recommended option is [redacted] capex and [redacted] opex (FY21/22 real terms) with an NPV benefit of $0.28 million relative to the base case counterfactual.

1. INVESTMENT NEED

1.1. Problem / Opportunity

During the 2018-22 regulatory period Powerlink has invested in its cybersecurity threat management tools and capability. As a Transmission Network Service Provider (TNSP) within the Australian energy market, Powerlink is classified in the "High" criticality band for cybersecurity management as defined through the Australian Energy Sector Cyber Security Framework (AESCSF) and is expected to maintain a higher level of cybersecurity maturity compared to the broader energy industry.

Growth of the cybersecurity threat in the modern world is well documented. Threat actors seek to leverage organisations' dependence on information and systems for their own financial or political gain, which in turn, can disrupt customer service delivery, threaten the achievement of strategic objectives and harm business reputations.

Complex critical infrastructure organisations such as Powerlink present an attractive target. In the past decade, governments have become increasingly concerned with the resilience of critical infrastructure and have sought to ensure that services are protected against a wide range of threats. In late 2020 the Australian Government introduced legislation to enforce new cybersecurity regulations on critical infrastructure operators.

Powerlink has assessed the maturity of its security practices against the AESCSF annually since 2018. [redacted] This program of work will also address many of the risk mitigation recommendations advised as a result of security risk assessment undertaken by PwC.

Powerlink also conducts regular security threat and risk assessments. The most recent assessment in 2019 identified a number of information security risks outside of desired risk tolerance and initiatives to address these risks.

Directly in line with this current focus, the following cybersecurity investment drivers apply to Powerlink for the period FY22/23 to FY26/27 (referred to herein as 2023-27):

1. Requirement to mitigate Powerlink's known, emerging and future cybersecurity risks within an appropriate managed risk profile.
2. Requirement to manage Powerlink's information system and information assets consistent with industry-typical mature cybersecurity practices in an environment of growing threat, national focus and community expectation.

[1] See section 1.2 Compliance Requirements for further explanation of these terms.

1.2. Compliance Requirements

The AESCSF was developed in 2018 and refined in 2019 as a collaboration of energy industry and government stakeholders through the Cyber Security Industry Working Group (CSIWG), which included:

- the Australian Cyber Security Centre (ACSC) within the Australian Signals Directorate,
- the Australian Energy Market Operator (AEMO),
- the Critical Infrastructure Centre (CIC), and
- Representatives from TNSPs, DNSPs, Generators and Retailers.

Powerlink is a member of the CSIWG and supports the prudent management of cybersecurity risk consistent with the AESCSF.

The AESCSF prescribes the target maturity level for practices through definition of three security profiles, SP-1 to SP-3. These security profiles were defined by the Australian Signals Directorate's ACSC in consultation with the CSIWG as a measure of the target state cybersecurity maturity which industry participants should aim to achieve and maintain.

TNSPs such as Powerlink are identified as "High" criticality service providers within the AESCSF. Therefore, Powerlink would ultimately need to achieve security profile SP-3 across the AESCSF domains for alignment with the ACSC-defined "best practice" targets, i.e. MIL-3 maturity in all cybersecurity domains. At present, the maturity targets in the AESCSF are not binding however it is expected they will form part of the new critical infrastructure security and resilience regulatory legislation that was proposed by the Department of Home Affairs in late 2020.

As mentioned in section 2.1, during the regulatory control period FY18-22, Powerlink has invested in its cybersecurity threat management tools and capability and as at November 2019, Powerlink's aggregate AESCSF score was assessed at [redacted] This score was approximately midrange amongst TNSP industry peers.

[redacted]

If the higher maturity targets form part of the requirements of the new security regulatory legislation, then Powerlink will have to move from its SP-2 maturity level to SP-3 within the 2023-27 regulatory period to avoid regulatory or legislative noncompliance.

Regardless of the potential regulatory or legislative requirement, noncompliance with the recommended ACSC security position for an extended period may also be at odds with community expectations therefore it is prudent that Powerlink best positions itself to achieve a heightened ACSC security position within an acceptable period of time should it be stipulated.

In other jurisdictions, cybersecurity controls and work practices are also mandated through Network Service Provider (NSP) licence conditions or other mechanisms. Examples exist in NSW where in 2019, cybersecurity licence conditions were imposed regarding on-shore hosting, access controls, information protection, workforce management and reporting.

There are already many external obligations that Powerlink has on protecting information – such as that defined in contracts, regulation or legislation. The information itself may have a requirement to be protected, such as personally identifiable information (PII) per the Australian Privacy Act, or it may be information that is part of a commercial contract, or it may be the need to protect processes and other assets for which an information security breach may result in a compliance impact.

1.3. Risk Mitigation Requirements

In addition to the current and potential compliance obligations outlined in section 1.2 this investment is also required to mitigate assessed, known, emerging and future risks.

Powerlink periodically conducts cybersecurity Threat Risk Assessments (TRAs) involving:

- Assessment of the effectiveness of existing cybersecurity controls;
- Assessment of Powerlink's cybersecurity inherent and managed risk profile; and
- Recommendations on bridging the gap between the current and target risk profiles.

In late 2019 Powerlink engaged PwC to perform a detailed information security risk assessment across its key asset groups and assess the effectiveness of their existing control capabilities to determine their level of cyber risk exposure. This assessment was performed in line with the existing *Information Security Conceptual Architecture* and *Information Security Risk Management Standard*.

The TRA profiled Powerlink's potential cybersecurity vulnerabilities across four general Information Asset Groups:

- Asset Group 1: The Operating High Voltage (HV) Network
- Asset Group 2: Critical Business Functions
- Asset Group 3: Commercially and Personally Sensitive Information
- Asset Group 4: Other Information Assets

Key assets types (and subtypes) within each of the four groups are depicted in Figure 1 below.

Information Asset Types	Information Asset Groupings						
1. Operating HV Network	A.1.1 Network Operations Realtime Infrastructure Configuration & Environment	A.1.2 Network Operations Offline Infrastructure Configuration & Environment	A.1.3 Australian Electricity Market Data & HV Network Metering Data	A.1.4 HV Network Offline Configuration & Environment Data + HV Network Secondary Systems Offline Asset Data	A.1.5 HV Network Live Configuration & Environment Data + HV Network Secondary Systems Live Asset Data	A.1.6 HV Network Realtime Data	A.1.7 Digital Network Customer Data
2. Critical Business Functions	A.2.1 Telecommunication Network Asset Data	A.2.2 Network Asset Information	A.2.3 Information Technology Realtime Infrastructure Configuration & Environment	A.2.4 Information Technology Offline Infrastructure Configuration & Environment			
3. Commercial and Personal	A.3.1 Stakeholder Details	A.3.2 Employee Personal Data + Employee Health Data + Employee Certifications	A.3.3 Commercial Business Information + Business Development	A.3.4 Financial Data + Procurement and Supply Contracts			
4. Other	A.4.1 Business Strategy + Corporate Risk & Governance						

Note: Shaded asset groups and sub-types are not included in the scope of this investment as they are classified OT.

Figure 1: Asset Groups and Sub-Types

Through the TRA process the existing controls were examined to determine Powerlink's current managed risk profile. The target risk position at the end of the current regulatory period for each relevant (IT) Asset Sub-Type has been utilised in the base case risk profile.

With consideration of the managed risk profile, target risk position and existing control effectiveness identified through the process, the TRA recommended a set of risk mitigation actions which will be partially addressed [redacted] under the Information Security Management Program during the remainder of the current regulatory period.

Powerlink will conduct another Threat and Risk Assessment late in 2021, prior to the completion of this schedule program of work and before the end of the current regulatory period. This will inform the direction for the next regulatory control period in line with the managed risk profile at that time and any applicable recommended risk mitigation actions.

In additions to these known, managed risks it is likely given the constantly evolving nature of the cybersecurity threat environment there will be emerging and future risks that will need to be

Five key global trends that have been shaping the global Cyber Security landscape are:

1. increasing Cyber Security threat sophistication;
2. erosion of the perimeter due to proliferation of IoT and mobile networks and cloud-based channels;
3. diffusion of trust and identity due to the rise of multiple methods for users to access products and services and increased peer-to-peer transactions;
4. proliferation of data at great velocities as organisations collect more data to generate insights; and
5. developments in, and the increasing adoption of emerging technologies such as robotics, cognitive intelligence and quantum computing.

The analysis paints a picture of a future cyber security landscape, in which:

- there is more at stake due to Australia's dependence on ICT
- there is increasing exposure to potential cyber attacks
- security continues to lag technology
- future attacks may be more potent yet harder to detect, and
- response to attacks will be complicated by the complexity, interconnectedness and interdependence of systems.

Overall, the cyber security domain is rapidly evolving thus requiring a continual process of monitoring and adapting to emerging threats

2. INVESTMENT OPTIONS

The following options have been considered to address the investment needs identified in section 2.

Option	Description
Option 1: Base Case (Counterfactual) **Maintain security practices at AESCSF SP-2 maturity and sustain existing security risk management practices.**	No significant investments in Powerlink's cybersecurity systems and practices will be undertaken in the 2023-27 regulatory control period, with investment deferral until the next period (2028-32). Specifically: • Do not extend AESCSF maturity beyond existing activities (i.e. maintain Powerlink's expected SP-2 position). • Undertake no further work to address identified TRA risk mitigation recommendations.
Option 2: (Recommended) **Continue to proactively mitigate known risks and manage with industry-typical practices, which may incrementally increase some AESCSF practices beyond SP-2**	Powerlink will further extend its Cybersecurity Maturity by extending on the established SP-2 level and move towards SP-3 based on risk and threats. Investments will be limited to appropriate responses to emerging threats. SP-3 will not be set as a specific target and it is unlikely to be achieved across most practices in the 2023-2027 period. Powerlink will prioritise and undertake adequate investment, mitigation and protection against threats based on the risks that these threats pose to the enterprise according to the importance of the assets that are being targeted. To achieve sustained information security effectiveness in an evolving landscape, Powerlink needs to institute effective information security risk management practices which are consistent with industry-typical cybersecurity practices and which are appropriate and adapted to an environment of growing threat, national focus and community expectation.
Option 3: **Proactively mitigate known risks and uplift security practices to AESCSF SP-3 maturity.**	Address all TRA recommendations and extend to full AESCSF maturity SP-3 consistent with the recommended AESCSF TNSP maturity target. SP-3 is set as a target maturity level to be achieved by the end of the 2023-2027 period.

Table 1: Investment Options

Each of these options is evaluated in the sections which follow.

2.1. OPTION 1: Base Case (Counterfactual) Maintain AESCSF maturity level SP-2.

Under this option, Powerlink maintain maturity level SP-2 and not seek any increase in maturity level.

2.1.1. Base Case Assumptions

The base case has been estimated based on the following assumptions.

Construction Cost and Scope Assumptions

- Annual cybersecurity capital investment over the coming regulatory control period will be limited to cyclic renewal of existing assets and small ad hoc responses to new threats when encountered. This is "recurrent expenditure" and consistent for all options. It is therefore not included in the comparative NPV analysis.
- Actioning outstanding TRA actions and uplifting to the ACSC and AEMO SP-3 target maturity will likely be essential by the following regulatory control period (i.e. FY27/28 to FY31/32), at which point the cost of uplift is 115% the cost that it would be if the uplift occurred in the 2023-27 period in real terms. i.e. 115% of the program delivery costs of Option 3.
- Implementation costs will be greater as an equivalent level of cybersecurity maturity and risk containment in the latter part of the coming decade will be more demanding than it is now due to a ever-growing threat environment. In 28/32 period, a more significant uplift is required to both deliver new capability and address a higher threat environment.

Operating Cost Assumptions

- There is an efficiency penalty in the interim period until work practice maturity is addressed. The efficiency penalty is estimated at approximately $500,000 during the interim period. This is due to less mature, manual processes including monitoring, incident detection, investigation, assurance and incident management.

Other Assumptions (Non-Financial)

- Powerlink will remain well behind the target SP-3 security profile suggested by the ACSC as appropriate for "high" criticality infrastructure providers including TNSPs.
- In the event of a cybersecurity event with substantial network or societal consequences, a significant misalignment with ACSC targets and/or with the TRA recommendations may be at odds with community expectations for a prudent operator.

2.1.2. Base Case Benefits

The following benefits may be achieved with selection of this base case option. Financial benefits are identified as "per annum" ongoing savings where relevant, and will begin accruing six months following implementation of the option.

Benefit Description	Financial Value ($M Real 2021/22 p.a.)
1. Minimises businesses change disruption through continuation of existing work practices.	N/A (Non-Financial)

Table 2: Option 1 - Base Case Benefits

2.1.3. Risk Mitigation

Table 3 (below) summarises the inherent risks which would be experienced by the end of the coming regulatory control period (2027) if the base case (counterfactual) option is selected.

The equivalent risk analyses provided with the recommended option (Option 2) and the alternative option (Option 3) have been conducted with respect to their effectiveness in mitigating the below base case risks. This assessment has been undertaken in alignment with the Powerlink risk management framework.

Risk Description	Inherent risk 2027	Risk Level
R1 – HV Network Offline Configuration & Environment Data + HV Network Secondary Systems Offline Asset Data **(Asset Group 1 Critical Business Function – A1.4)** **Risk of leakage/theft/manipulation of Australian Electricity Market Data & HV Network Metering Data from actions of insider/third-party/external actor** **Risk categories – (Stakeholder, Business Strategy, Financial and Contractual)**	As the base case, this option does not address the existing risk profile. Therefore, this risk still remain High. Further improvement remains required to reach the Target Risk Position. Likelihood – **Almost Certain** Consequence – **Major**	**High**
R2 – Network Asset Information **(Asset Group 2 Critical Business Function – A2.2)** **Risk of leakage/theft/manipulation of Network Asset Information from actions of insider/third-party/external actor** **Risk categories – (Stakeholder, Business Strategy, Financial and Contractual)**	As the base case, this option does not address the existing risk profile. Therefore, this risk still remain Significant. Further improvement remains required to reach the Target Risk Position. Likelihood – **Moderate** Consequence – **Likely**	**Significant**
R3 – Information Technology Realtime Infrastructure Configuration & Environment **(Asset Group 2 Critical Business Function – A2.3)** **Risk of leakage/theft/manipulation of Information Technology Realtime Infrastructure from actions of insider/third-party/external actor** **Risk categories – (Stakeholder, Business Strategy, Financial and Contractual)**	As the base case, this option does not address the existing risk profile. Therefore, this risk still remain Significant. Further improvement remains required to reach the Target Risk Position. Likelihood – **Moderate** Consequence – **Likely**	**Significant**
R4 – Information Technology Offline Infrastructure Configuration & Environment **(Asset Group 2 Critical Business Function – A2.4)** **Risk of leakage/theft/manipulation of Information Technology Offline Infrastructure from actions of insider/third-party/external actor** **Risk categories – (Stakeholder, Business Strategy, Financial and Contractual)**	As the base case, this option does not address the existing risk profile. Therefore, this risk still remain Significant. Further improvement remains required to reach the Target Risk Position. Likelihood – **Unlikely** Consequence – **Moderate**	**Moderate**

Risk Description	Inherent risk 2027	Risk Level
R5 – Commercial and Personal – Stakeholder Details **(Asset Group 3 Commercial and Personal – A3.1)** **Risk of leakage/theft/manipulation of Stakeholder Details from actions of insider/third-party/external actor** **Risk categories – (Stakeholder, Business Strategy, Financial and Contractual)**	As the base case, this option does not address the existing risk profile. Therefore, most known risks still remain Moderate / Significant. Further improvement remains required to reach the Target Risk Position. Likelihood – **Unlikely** Consequence – **Moderate**	**Moderate**
R6 – Commercial and Personal - Employee Data **(Asset Group 3 Commercial and Personal – A3.2)** **Risk of leakage/theft/manipulation of Employee Data from actions of insider/third-party/external actor** **Risk categories – (Stakeholder, Business Strategy, Financial and Contractual)**	As the base case, this option does not address the existing risk profile. Therefore, most known risks still remain Moderate / Significant. Further improvement remains required to reach the Target Risk Position. Likelihood – **Unlikely** Consequence – **Moderate**	**Moderate**
R7 – Commercial and Personal - Commercial Business Data **(Asset Group 3 Commercial and Personal – A3.3)** **Risk of leakage/theft/manipulation of Commercial Business Data from actions of insider/third-party/external actor** **Risk categories – (Stakeholder, Business Strategy, Financial and Contractual)**	As the base case, this option does not address the existing risk profile. Therefore, most known risks still remain Significant. Further improvement remains required to reach the Target Risk Position. Likelihood – **Possible** Consequence – **Major**	**Significant**
R8 – Commercial and Personal - Financial Data/ Procurement and Supply Contracts **(Asset Group 3 Commercial and Personal – A3.4)** **Risk of leakage/theft/manipulation of Financial Data/ Procurement and Supply Contracts information from actions of insider/third-party/external actor** **Risk categories – (Stakeholder, Business Strategy, Financial and Contractual)**	As the base case, this option does not address the existing risk profile. Therefore, most known risks still remain Significant. Further improvement remains required to reach the Target Risk Position. Likelihood – **Unlikely** Consequence – **Moderate**	**Significant**

Risk Description	Inherent risk 2027	Risk Level
R9 - Business Strategy & Corporate Risk & Governance **(Asset Group 4 Other A4.1)** **Risk of leakage/theft/manipulation of Business Strategy & Corporate Risk & Governance information from actions of insider/third-party/external actor** **Risk categories – (Stakeholder, Business Strategy, Financial and Contractual)**	As the base case, this option does not address the existing risk profile. Therefore, most known risks still remain Moderate. Further improvement remains required to reach the Target Risk Position. Likelihood – **Unlikely** Consequence – **Moderate**	**Moderate**

Table 3: Option 1 - Base Case Risk Mitigation

Figure 2 below summarises the risk position of adopting the base case (assessment of each risk tabled above).

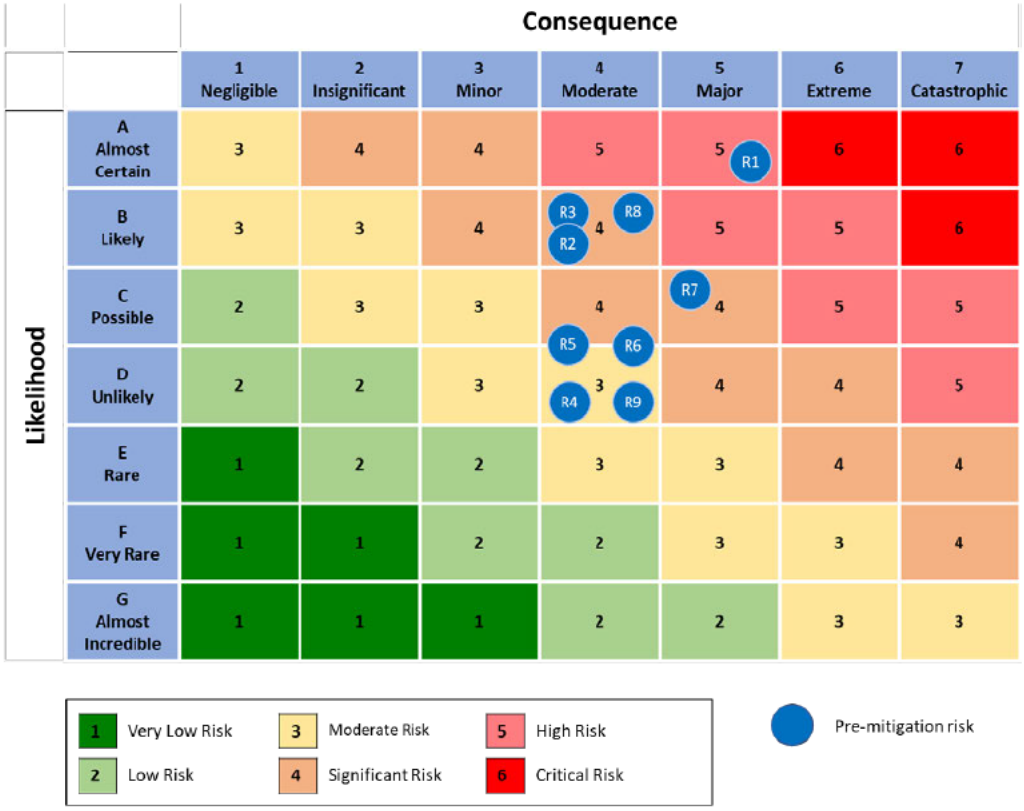

Figure 2: Base Case Risk Assessment

2.2. OPTION 2 Mitigate known risks and manage with industry-typical practices (recommended)

To keep up with the pace of cybersecurity threats and the nature of the changing threat landscape, Powerlink requires the ability to manage these threats in the context of information security risk.

Under this option Powerlink will mitigate Powerlink's known cybersecurity risks within an appropriate managed risk profile. An effective set of controls that address the likelihood and potential consequences of security risks will be implemented to reduce risk to a level that appropriately reflects the value of information assets in line with Powerlink's Enterprise Information Security Strategy. This allows prioritisation and adequate protection of threats based on the risks that these threats pose to the enterprise according to the importance of the assets that are being targeted.

To achieve sustained information security effectiveness in an evolving landscape, Powerlink needs to institute effective information security risk management practices which are consistent with industry-typical cybersecurity practices and which are appropriate and adapted to an environment of growing threat, national focus and community expectation.

This option seeks to build on the SP-2 maturity level achieved at the end of the 2018-2022 regulatory period, however will not seek to increase the maturity to SP-3 during 23-27 period. Some progress towards SP-3 in some practices is expected as a result of risk mitigation activities.

In the event that achievement of the target is mandated through regulatory or legislative mandate, the additional uplift would either be funded through de-prioritisation of other planned investments or through other funding mechanisms.

2.2.1. Option 2 Assumptions

This recommended option has been estimated based on the following assumptions.

Construction Cost and Scope Assumptions

- The project costs are based on a build-up of forecast resourcing and vendor & specialist services, as detailed in the table below.

[redacted]

Table 4: Option 2 Cost Build-Up (2021/22 $ real)

- This estimate is based on standard unit rates with estimates based on previous projects of similar size and complexity.
- The project is planned to run across a 24 month timeframe, inclusive of 9 month combined procurement and design phases. The delivery phase is forecast at 12 months, concluding with 3 months of hyper-care.
- Ongoing IT Operating costs are expected to be similar to current costs, therefore current costs have been used in estimating future costs
- The final business case development process will be used to refine the scope, costs and impacts for this investment. As indicated above, a procurement activity will likely be undertaken to inform costs and solution options.

Operating Cost Assumptions

- Ongoing IT operating costs are forecast to remain unchanged.

Other Assumptions (Non-Financial)

- Through this option, Powerlink will make substantial steps in maturity of cybersecurity practices and risk mitigation. Further investment to achieve the SP-3 target may still be required in the 2023-27 regulatory period and may become subject to a legislative or regulatory mandate as described in section 1.2.

2.2.2. Option Benefits

The following benefits may be achieved with selection of this recommended option. Financial benefits are identified as "per annum" ongoing savings where relevant and will begin accruing following implementation of the option.

Benefit Description	Financial Value ($M Real 2021/22 p.a.)
B1. Alignment of cybersecurity practices with Industry Peers Maintains and extends a level of cybersecurity risk mitigation and control practices responding the new and emerging threats consistent with the improvement plans of industry peers as reported through the CSIWG. Acts on the risk management imperative by addressing other priority TRA recommendations through targeted mitigation actions.	N/A (Non-Financial)
B2. Provides a level of risk consistent with Powerlink and cybersecurity community expectations	N/A (Non-Financial)

Table 5: Option 2 Benefits

2.2.3. Risk Mitigation

Listed below is a summary of how this option addresses risks identified through the base case. The opening risk position represents the risk level at the end of the coming 2023-27 period should the base case have been selected.

Risk Description	Inherent risk 2027	Risk Level
R1 – HV Network Offline Configuration & Environment Data + HV Network Secondary Systems Offline Asset Data **(Asset Group 1 Critical Business Function – A1.4)** **Risk of leakage/theft/manipulation of Australian Electricity Market Data & HV Network Metering Data from actions of insider/third-party/external actor** **Risk categories – (Stakeholder, Business Strategy, Financial and Contractual)**	Through further implementation of TRA risk mitigations and security control uplifts known risks will reduce in likelihood (**Possible**), impact will remain **Major** should a cybersecurity threat be realised.	**Significant**
R2 – Network Asset Information **(Asset Group 2 Critical Business Function – A2.2)** **Risk of leakage/theft/manipulation of Network Asset Information from actions of insider/third-party/external actor** **Risk categories – (Stakeholder, Business Strategy, Financial and Contractual)**	Through further implementation of TRA risk mitigations and security control uplifts known risks will reduce in likelihood (**Rare**), impact will remain **Moderate** should a cybersecurity threat be realised.	**Moderate**
R3 – Information Technology Realtime Infrastructure Configuration & Environment **(Asset Group 2 Critical Business Function – A2.3)** **Risk of leakage/theft/manipulation of Information Technology Realtime Infrastructure from actions of insider/third-party/external actor** **Risk categories – (Stakeholder, Business Strategy, Financial and Contractual)**	Through further implementation of TRA risk mitigations and security control uplifts known risks will reduce in likelihood (**Rare**), impact will remain **Moderate** should a cybersecurity threat be realised.	**Moderate**
R4 – Information Technology Offline Infrastructure Configuration & Environment **(Asset Group 2 Critical Business Function – A2.4)** **Risk of leakage/theft/manipulation of Information Technology Offline Infrastructure from actions of insider/third-party/external actor** **Risk categories – (Stakeholder, Business Strategy, Financial and Contractual)**	Through further implementation of TRA risk mitigations and security control uplifts known risks will reduce in likelihood (**Very Rare**), impact will remain **Moderate** should a cybersecurity threat be realised.	**Low**

Risk Description	Inherent risk 2027	Risk Level
R5 – Commercial and Personal – Stakeholder Details **(Asset Group 3 Commercial and Personal – A3.1)** **Risk of leakage/theft/manipulation of Stakeholder Details from actions of insider/third-party/external actor** **Risk categories – (Stakeholder, Business Strategy, Financial and Contractual)**	Through further implementation of TRA risk mitigations and security control uplifts known risks will reduce in likelihood (**Very Rare**), impact will remain **Moderate** should a cybersecurity threat be realised.	**Low**
R6 – Commercial and Personal - Employee Data **(Asset Group 3 Commercial and Personal – A3.2)** **Risk of leakage/theft/manipulation of Employee Data from actions of insider/third-party/external actor** **Risk categories – (Stakeholder, Business Strategy, Financial and Contractual)**	Through further implementation of TRA risk mitigations and security control uplifts known risks will reduce in likelihood (**Very Rare**), impact will remain **Moderate** should a cybersecurity threat be realised.	**Low**
R7 – Commercial and Personal - Commercial Business Data **(Asset Group 3 Commercial and Personal – A3.3)** **Risk of leakage/theft/manipulation of Commercial Business Data from actions of insider/third-party/external actor** **Risk categories – (Stakeholder, Business Strategy, Financial and Contractual)**	Through further implementation of TRA risk mitigations and security control uplifts known risks will reduce significantly in likelihood (**Rare**), impact will remain **Major** should a cybersecurity threat be realised.	**Moderate**
R8 – Commercial and Personal - Financial Data/ Procurement and Supply Contracts **(Asset Group 3 Commercial and Personal – A3.4)** **Risk of leakage/theft/manipulation of Financial Data/ Procurement and Supply Contracts information from actions of insider/third-party/external actor** **Risk categories – (Stakeholder, Business Strategy, Financial and Contractual)**	Through further implementation of TRA risk mitigations and security control uplifts known risks will reduce in likelihood (**Rare**), impact will remain **Moderate** should a cybersecurity threat be realised.	**Moderate**

Risk Description	Inherent risk 2027	Risk Level
R9 - Business Strategy & Corporate Risk & Governance **(Asset Group 4 Other A4.1)** **Risk of leakage/theft/manipulation of Business Strategy & Corporate Risk & Governance information from actions of insider/third-party/external actor** **Risk categories – (Stakeholder, Business Strategy, Financial and Contractual)**	Through further implementation of TRA risk mitigations and security control uplifts known risks will reduce in likelihood (**Very Rare**), impact will remain **Moderate** should a cybersecurity threat be realised.	**Low**

Table 6: Option 2 Risk Mitigation

Figure 3 below summarises the risk position of adopting option 2 (pre- and post-mitigation assessment of each risk tabled above).

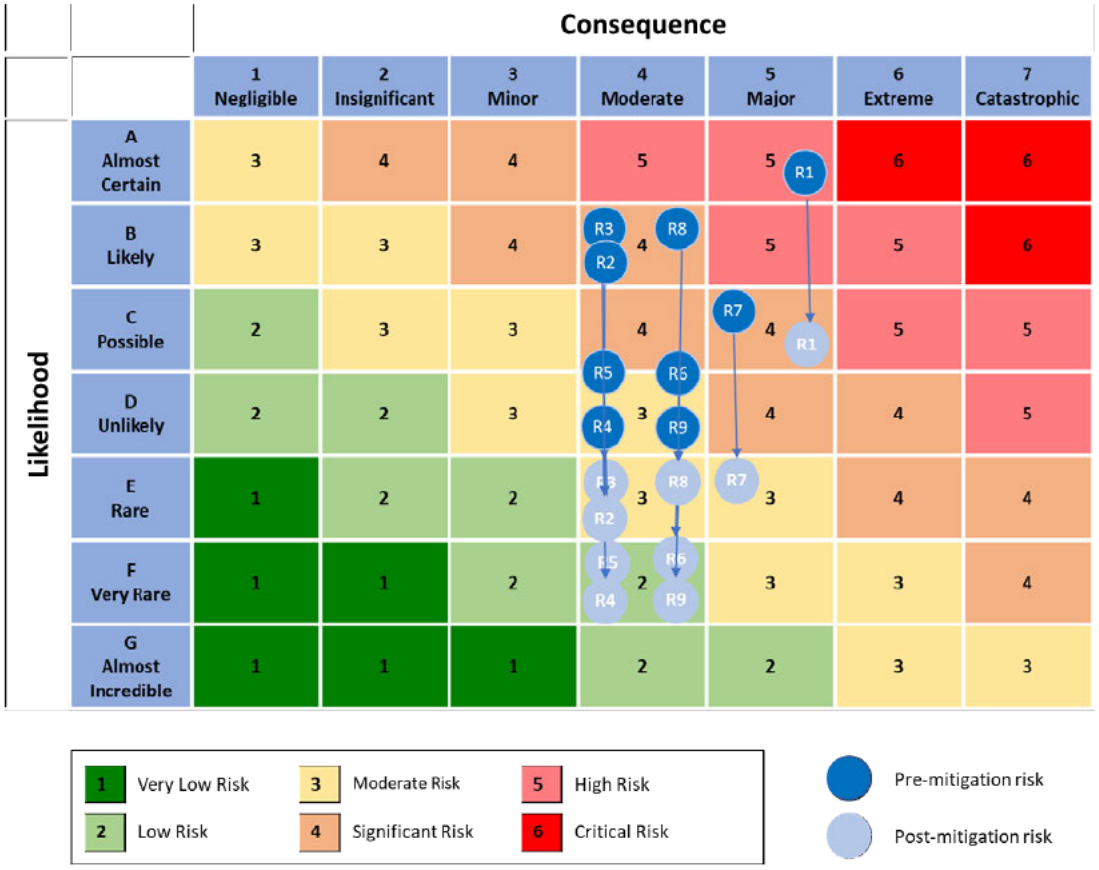

Figure 3: Option 2 - Risk Assessment

2.3. OPTION 3 Address risk and progress to full SP-3 maturity

This option will progress Powerlink to full achievement of the target AESCSF SP-3 maturity as defined by the ACSC and AEMO for “High” criticality market participants.

2.3.1. Option 3 Assumptions

This option has been estimated on the basis of the following assumptions.

Construction Cost and Scope Assumptions

- This option will implement the full set of AESCSF operational practice maturity uplifts necessary to achieve the SP-3 target.
- This option will implement the full set of AESCSF operational practice maturity uplifts necessary to achieve the SP-3 target.
- This preliminary estimate has been formulated using a combination of standard unit rates for Powerlink internal and external resourcing across the proposed timeline, leveraging current and previous projects for vendor estimates.
- The final business case development process will be used to refine the final scope, costs and impacts for this investment. One or more procurement activities will likely be undertaken to further inform costs and solution options.

Operating Cost Assumptions

- Cybersecurity operating costs will remain unchanged. Any increase in ongoing costs arising from the above improvements will be absorbed within operational budgets through offsetting with other group efficiencies.

Other Assumptions (Non-Financial)

- Powerlink will achieve full compliance with the recommended target security profile level define by the ACSC and AEMO. This is likely to be consistent with community expectations for a prudent operator. It would also avoid the necessity for de-prioritisation of other importance works, or provision of other funding mechanisms in the event that the ACSC and AEMO SP-3 target becomes mandated through either a regulatory or legislative instrument during the 2023-27 regulatory period.
- Commercially available solutions will be available and able to provide the outcomes for Powerlink to meet full SP-3 maturity.
- As the required maturity uplift to meet SP-3 maturity is significant, the implementation of more mature and sophisticated systems and practices will require business change management. It is possible that business areas are impacted significantly through the implementation process.

2.3.2. Option Benefits

The following benefits may be achieved with selection of this option (over and above those outlined in Option 2). Financial benefits are identified as "per annum" ongoing savings where relevant and will begin accruing following implementation of the option.

Benefit Description	Financial Value ($M Real 2019/20 p.a.)
B1. ACSC and AEMO Targets Achieved **Achieves the ACSC and AEMO target for cybersecurity maturity while also mitigating identified risk and acknowledging community expectations.**	N/A (Non-Financial)

Table 7: Option 3 Benefits

2.3.3. Risk Mitigation

Listed below is a summary of how this option addresses risks identified through the base case. The opening risk position represents the risk level at the end of the coming 2023-27 period should the base case have been selected.

Risk Description	Inherent risk 2027	Risk Level
R1 – HV Network Offline Configuration & Environment Data + HV Network Secondary Systems Offline Asset Data **(Asset Group 1 Critical Business Function – A1.4)** **Risk of leakage/theft/manipulation of Australian Electricity Market Data & HV Network Metering Data from actions of insider/third-party/external actor** **Risk categories – (Stakeholder, Business Strategy, Financial and Contractual)**	Through actioning of outstanding risk mitigation recommendations arising from the 2020 TRA and full achievement of the target AESCSF SP-3 maturity known risks will reduce significantly in likelihood **(Unlikely)**, impact will remain **Major** should a cybersecurity threat be realised.	**Significant**
R2 – Network Asset Information **(Asset Group 2 Critical Business Function – A2.2)** **Risk of leakage/theft/manipulation of Network Asset Information from actions of insider/third-party/external actor** **Risk categories – (Stakeholder, Business Strategy, Financial and Contractual)**	Through actioning of outstanding risk mitigation recommendations arising from the 2020 TRA and full achievement of the target AESCSF SP-3 maturity known risks will reduce significantly in likelihood **(Very Rare)**, impact will remain **Moderate** should a cybersecurity threat be realised.	**Low**
R3 – Information Technology Realtime Infrastructure Configuration & Environment **(Asset Group 2 Critical Business Function – A2.3)** **Risk of leakage/theft/manipulation of Information Technology Realtime Infrastructure from actions of insider/third-party/external actor** **Risk categories – (Stakeholder, Business Strategy, Financial and Contractual)**	Through actioning of outstanding risk mitigation recommendations arising from the 2020 TRA and full achievement of the target AESCSF SP-3 maturity known risks will reduce significantly in likelihood **(Very Rare)**, impact will remain **Moderate** should a cybersecurity threat be realised.	**Low**
R4 – Information Technology Offline Infrastructure Configuration & Environment **(Asset Group 2 Critical Business Function – A2.4)** **Risk of leakage/theft/manipulation of Information Technology Offline Infrastructure from actions of insider/third-party/external actor** **Risk categories – (Stakeholder, Business Strategy, Financial and Contractual)**	Through actioning of outstanding risk mitigation recommendations arising from the 2020 TRA and full achievement of the target AESCSF SP-3 maturity known risks will reduce significantly in likelihood **(Almost Incredible)**, impact will remain **Moderate** should a cybersecurity threat be realised.	**Low**

Risk Description	Inherent risk 2027	Risk Level
R5 – Commercial and Personal – Stakeholder Details **(Asset Group 3 Commercial and Personal – A3.1)** **Risk of leakage/theft/manipulation of Stakeholder Details from actions of insider/third-party/external actor** **Risk categories – (Stakeholder, Business Strategy, Financial and Contractual)**	Through actioning of outstanding risk mitigation recommendations arising from the 2020 TRA and full achievement of the target AESCSF SP-3 maturity known risks will reduce significantly in likelihood (**Almost Incredible**), impact will remain **Moderate** should a cybersecurity threat be realised.	**Low**
R6 – Commercial and Personal - Employee Data **(Asset Group 3 Commercial and Personal – A3.2)** **Risk of leakage/theft/manipulation of Employee Data from actions of insider/third-party/external actor** **Risk categories – (Stakeholder, Business Strategy, Financial and Contractual)**	Through actioning of outstanding risk mitigation recommendations arising from the 2020 TRA and full achievement of the target AESCSF SP-3 maturity known risks will reduce significantly in likelihood (**Almost Incredible**), impact will remain **Moderate** should a cybersecurity threat be realised.	**Low**
R7 – Commercial and Personal - Commercial Business Data **(Asset Group 3 Commercial and Personal – A3.3)** **Risk of leakage/theft/manipulation of Commercial Business Data from actions of insider/third-party/external actor** **Risk categories – (Stakeholder, Business Strategy, Financial and Contractual)**	Through actioning of outstanding risk mitigation recommendations arising from the 2020 TRA and full achievement of the target AESCSF SP-3 maturity known risks will reduce significantly in likelihood (**Very Rare**), impact will remain **Major** should a cybersecurity threat be realised.	**Moderate**
R8 – Commercial and Personal - Financial Data/ Procurement and Supply Contracts **(Asset Group 3 Commercial and Personal – A3.4)** **Risk of leakage/theft/manipulation of Financial Data/ Procurement and Supply Contracts information from actions of insider/third-party/external actor** **Risk categories – (Stakeholder, Business Strategy, Financial and Contractual)**	Through actioning of outstanding risk mitigation recommendations arising from the 2020 TRA and full achievement of the target AESCSF SP-3 maturity known risks will reduce significantly in likelihood (**Very Rare**), impact will remain **Moderate** should a cybersecurity threat be realised.	**Low**

Risk Description	Inherent risk 2027	Risk Level
R9 - Business Strategy & Corporate Risk & Governance **(Asset Group 4 Other A4.1)** **Risk of leakage/theft/manipulation of Business Strategy & Corporate Risk & Governance information from actions of insider/third-party/external actor** **Risk categories – (Stakeholder, Business Strategy, Financial and Contractual)**	Through actioning of outstanding risk mitigation recommendations arising from the 2020 TRA and full achievement of the target AESCSF SP-3 maturity known risks will reduce significantly in likelihood (**Almost Incredible**), impact will remain **Moderate** should a cybersecurity threat be realised.	**Low**

Table 8: Option 3 Risk Mitigation

Figure 4 (over page) summarises the risk position of adopting option 3 (pre- and post-mitigation assessment of each risk tabled above).

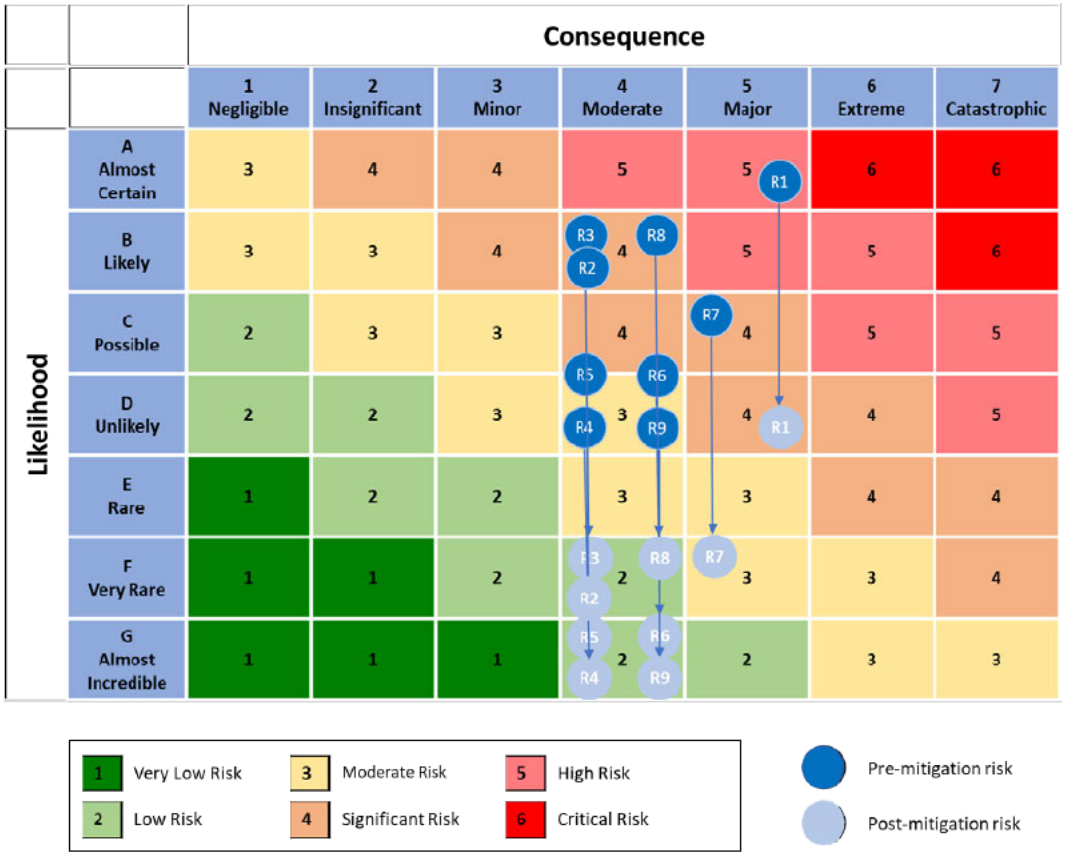

Figure 4: Option 3 - Risk Assessment

2.4. Option Financial Comparison

Table 10 (below) provides a summary comparison of the identified options.

Option	Title	NPV	Counterfactual Difference	Result
Option 1	Base Case (Counterfactual) Do not address outstanding TRA recommendations or significantly extend AESCSF maturity beyond SP-2.	(2,235,020)	-	
Option 2	Mitigate known cybersecurity risks and manage with industry-typical cybersecurity practices	(1,952,170)	282,850	**Least Cost**
Option 3	Address risk and progress to full SP-3 maturity	(3,953,642)	(1,718,622)	

Table 9: Option NPV Financial Comparison

Consistent with the above analysis, Option 2 "Mitigate known cybersecurity risks and manage with industry-typical cybersecurity practices" is recommended.

2.5. Cashflow Summary

Table 13 (below) provides a summary of forecast cashflow over the 10 year analysis period for the recommended option (i.e. Option 2).

[redacted]

Table 10: **Cashflow Summary (Recommended Option)**

3. RECOMMENDATION

3.1. Recommended Solution

The information security threat is increasingly more complex as the digital landscape evolves. Attacks against information assets are increasing, and Powerlink is not immune to this due to the nature of the industry and Powerlink's digital profile as a critical infrastructure provider.

It is recommended to endorse "**Option 2 Mitigate known cybersecurity risks and manage with industry-typical cybersecurity practices**". This option represents:

- Prudent mitigation of new, emerging and ever-changing cybersecurity risks within an appropriate risk profile and management of Powerlink's assets consistent with industry-typical cybersecurity practices which allows for response and adaption to growing and evolving threats and alignment to peers and community expectations.
- Prudent balance between risk mitigation and sustainable capability improvement without investing beyond the boundaries of a potential AESCSF legislative or regulatory mandate.

Delivery of the recommended option will begin in FY22/23.

Total forecast non-network (IT) expenditure for the recommended option within the 2023-27 regulatory control period is [redacted] capex and [redacted] opex (FY21/22 real terms) with a 10 year NPV benefit of $0.28 million relative to the base case counterfactual.

3.2. High Level Timeline

Figure 5 (below) depicts the planned timeframe for implementation of the recommended option.

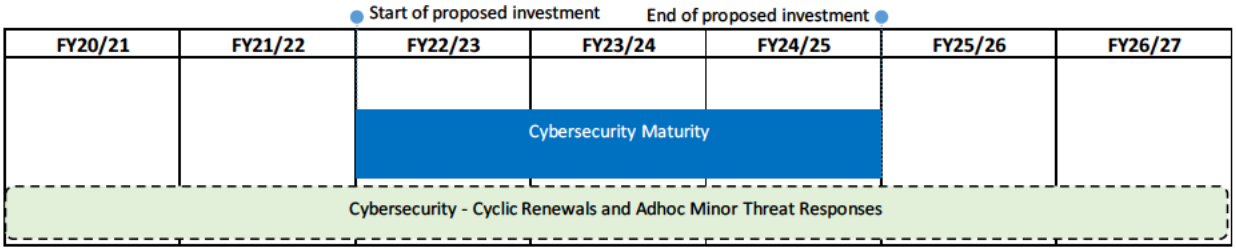

Figure 5: High Level Investment Timeline

3.3. Initiative Value Assessment

Figure 6 (below) summarises the planned initiative value across parameters of:

A: Strategic Alignment and Value
B: Ease of Business Change
C: Architecture Alignment
D: Ease of Delivery and Operation

As indicated in the figure below, the planned investment is at or above the 80th percentile in assessment against parameters B, C and D. The investment scores lower against parameter A, which is reflective of the nature of cybersecurity control uplift aligning more heavily with the protection of critical business activities and risk mitigation rather than the building of new, additional business products and value.

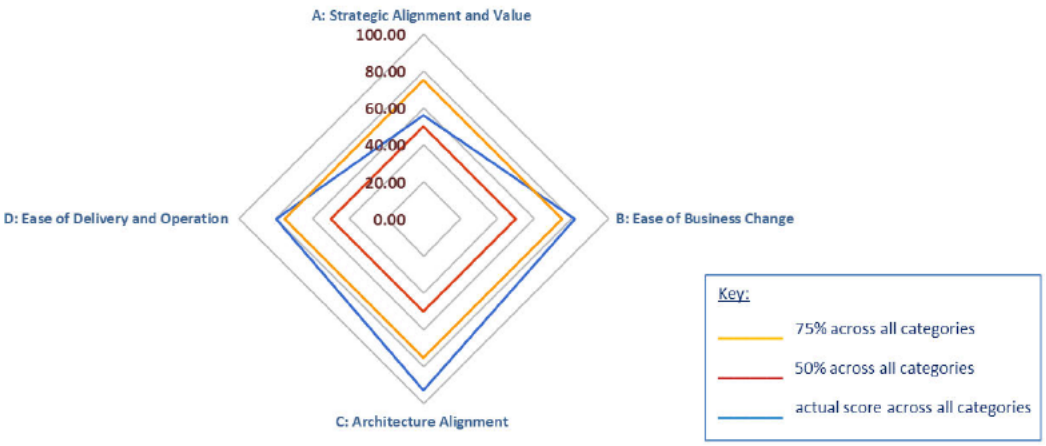

Figure 6: Initiative Value Assessment

Appendix A: Glossary of Terms

The following terms or abbreviations are used within this document.

Term	Definition
ACSC	Australian Cyber Security Centre - The Australian Cyber Security Centre is the Australian Government lead agency for cyber security. The ACSC is part of the Australian Signals Directorate.
AEMC	The Australian Energy Market Commission
AEMO	Australian Energy Market Operator
AER	Australian Energy Regulator
AESCSF	Australian Energy Sector Cybersecurity Framework
ALM	Asset Lifecycle Management
C2M2	Cybersecurity Capability Maturity Model
Capex	Capital Expenditure
CIC	Critical Infrastructure Centre
CSIWG	Cyber Security Industry Working Group
COAG	Council of Australian Governments
GAEC	Governance & Assurance Executive Committee
ISMP	Information Security Management Program
IT	Information Technology
MIL	Maturity Indicator Level
NPV	Net Present Value
Opex	Operating Expenditure
OT	Operational Technology
PQ	Powerlink Queensland
TNSP	Transmission Network Service Provider
TRA	Threat Risk Assessment