

Corporate Site Security

Regulatory Business Case (RBC) 2024-29

Contents

1. Summary	2
1.1 Business need	2
1.2 Options analysis	3
1.3 Recommendation	3
2. Identified need	4
2.1 Asset overview	4
2.2 Compliance Requirements and considerations	5
2.3 Current management programs	6
2.4 Asset condition and emerging issues	7
2.5 Risk Assessment	8
2.6 Summary	9
3. Options analysis	10
3.1 Comparison of credible options	10
4. Recommendation	14
4.1 Strategic alignment	14
4.2 Benefits	14
4.3 Dependent projects	15
4.4 Deliverability	15
4.5 Expenditure profile	15
4.6 High-level scope	15
Appendix A. Key assumptions and limitations	16

1. Summary

This business case has been prepared to support the 2024-29 Regulatory Proposal. The business case demonstrates that Power and Water has undertaken appropriate analysis of the need for the expenditure and identified credible options that will resolve the need and ensure that Power and Water continues to meet the National Electricity Objectives and maintain the quality, reliability, and security of supply of standard control services and maintain the safety of the distribution system.

The proposed expenditure identified in this business case will undergo further assessment and scrutiny through Power and Water's normal governance processes prior to implementation and delivery.

This business case addresses the compliance requirements and associated risks associated with the physical security for our corporate offices.

1.1 Business need

The physical security for our corporate (and network facilities) require ongoing investment to ensure we continue to protect the safety of the public and our employees, maintain energy security for our customers and align with industry standards.

Our corporate sites include six corporate locations spread out over 1.3 million square kilometres. Maintaining the physical security of our corporate facilities is essential to the safe and secure management of our network. This includes ensuring only authorised personnel with required authorisations have access to certain facilities and intentional or unintentional entry or misuse of facilities is detected and/or prevented.

The environment we are operating in is becoming more challenging as we encounter increased incidents of security threats such as theft and vandalism. Without investment to maintain our current physical security capabilities, there will be increasing risks to the security of our energy supply and the safety of workers and the public. It is therefore imperative that we invest to maintain our existing security standards.

Recent amendments to the *Security of Critical Infrastructure Act* have resulted in a number of enhanced requirements for managing physical and cyber security risk which apply to Power and Water.

Power and Water must also comply with section 6.5.6(a)(iii) of the NT National Electricity Rules (the Rules), which state that a distributor must maintain the quality, reliability, and security of supply of standard control services. We must also meet the government's prioritisation of critical asset protection, which states that:

'those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact the social or economic wellbeing of the nation or affect Australia's ability to conduct national defence and ensure national security'.¹

The upgrade of electronic security infrastructure across corporate sites is a key requirement of the Power and Water approved *Protective Security Management Standard* and its deliverables framework. The combination of physical security measures and monitoring helps ensure that only appropriately authorised

¹ Australia-New Zealand Counter-Terrorism Committee, *National Guidelines for Protecting Critical Infrastructure from Terrorism* (Guidelines, 2015) 3.

access is allowed to critical sites. It is therefore essential to maintain our physical security systems so that security vulnerabilities are mitigated.

1.2 Options analysis

The options considered to resolve this need are shown in the tables below.

Table 1 Summary of credible options

Option No.	Option name	Description	Recommended
1	Do Nothing	No expenditure or mitigation actions taken	No
2	Head Office Upgrade	Replace/upgrade security infrastructure only at Head Office	No
3	All Corporate Sites Upgrade	Replace/upgrade security infrastructure across all Corporate sites	Yes

1.3 Recommendation

The recommended option is Option 3 – All corporate sites upgrade at an estimated cost of \$1.45 million (real 2021/22) over the next regulatory period. This option addresses the highest risks while ensuring cost efficiency.

The proposed expenditure is necessary for ensuring the continued functionality and operation of existing electronic security infrastructure. These works will witness the replacement and upgrade of electronic security hardware which is at end-of-life, obsolete and out of warranty. The proposed expenditure will enhance Power and Water’s security and safety processes for risk prevention, deterrence, detection and responsiveness. Works undertaken within the scope of this initiative also support the compliance obligations of the *Security of Critical Infrastructure Act* which have been forecast for Power and Water.

Whilst Option 2 has a lower capital expenditure it is not the preferred option due to unacceptable security risk it presents to our business and customers.

The forecast expenditure for the next regulatory control period allocated to Standard Control Services as per the CAM is outlined in Table 2 for the 2024-29 regulatory period.

Table 2 Annual capital and operational expenditure (\$m, real 2021/22)

Item	FY25	FY26	FY27	FY28	FY29	Total
Capex	-	-	0.47	0.48	0.50	1.45
Opex	-	-	-	-	-	-
Total	-	-	0.47	0.48	0.50	1.45

2. Identified need

The purpose of this section is to demonstrate and provide the background information for the identified need to invest based on the benefits of the proposed investment, and that the investment is aligned to Power and Water’s strategic objectives.

As a provider of critical infrastructure for the residents of the Northern Territory, Power and Water has a responsibility to ensure the security of that infrastructure. This business case focuses on investing in physical security, electronic security access and hardware access to mitigate the risk of physical security breaches at corporate sites only.² The completion of program works will enhance Power and Water’s security and safety processes for risk prevention, deterrence, detection and responsiveness.

The investment objective is to deliver on a safe and secure corporation through the protection of our people, information and assets. The investment drivers are described below.

2.1 Asset overview

Power and Water has six corporate site properties across the Northern Territory, set out in Table 4 below. Together they accommodate 1,060 staff who all rely on the continued level of functionality of the premises in order to perform their roles and facilitate the supply of power to residents of the Northern Territory.

Table 3 Power and Water Corporate Locations

Property	Location	Number of Staff	Description of Use
Ben Hammond Complex	Iliffe Street, Stuart Park NT 0820	520	An urban corporate site which accommodates people and infrastructure which is responsible for the operational delivery of essential utility services (power, water and gas)
Sadadeen Valley Complex	25 Berger Court, Sadadeen NT 0870	88	A regional corporate site which accommodates people and infrastructure who are responsible for providing strategic and corporate support needed to enable the delivery of essential utility services (power, water & gas).
Victoria Highway Complex	88 Victoria Highway, Katherine NT 0850	18	A regional corporate site which accommodates people and infrastructure who are responsible for providing strategic, operational and corporate support needed to enable the delivery of essential utility services (power, water and gas).
Mitchell Centre	55 Mitchell Street, Levels 2	312	An urban corporate site which accommodates people and infrastructure who are responsible for providing strategic and corporate support needed to enable the

² Operational technology (OT) and ICT cyber security is subject to a separate business case

Property	Location	Number of Staff	Description of Use
	/ 6 & 7, Darwin NT 0800		delivery of essential utility services (power, water and gas).
Jacana Place (Wood Street)	39 Woods Street, Levels 2 / 6 & 7. Darwin NT 0800	109	An urban corporate site which accommodates people and infrastructure who are responsible for providing strategic and corporate support needed to enable the delivery of essential utility services (power, water and gas).
Standley Street Complex (also called Tennant Creek Complex)	Lot 2505 Standley Street, Tennant Creek NT 0862	13	A regional corporate site which accommodates people and infrastructure who are responsible for providing strategic, operational and corporate support needed to enable the delivery of essential utility services (power, water and gas).

2.2 Compliance Requirements and considerations

There are a number of compliance requirements in legislation, standards and codes that are required to be met. Power and Water must comply with the *Security of Critical Infrastructure Act 2018* (Cth) ('SOCI Act'), the *Government Owned Corporations Act 2001* (NT) ('GOC Act') and the *Work Health and Safety (National Uniform Legislation) Act 2011* (NT) ('NT Health and Safety Act'). The specific obligations contained in these acts are discussed below.

Action is required to assess the new needs under these obligations and implement appropriate solutions to ensure all security systems are compliant.

Security of Critical Infrastructure Act

The SOCI Act creates a framework for the management of risks related to critical infrastructure. It has been subject to a number of reforms in recent years, culminating with the final amendment which was passed by Parliament on 31 March 2022. As a result, Power and Water is subject to new security-related obligations, including the requirement to create and maintain a critical infrastructure risk management program (Part 2A of the SOCI Act) and the obligation to report cyber incidents (Part 2B of the SOCI Act).

The amendments to the SOCI Act strengthen the existing framework for managing risks to critical infrastructure, including by introducing:³

- Positive Security Obligations (PSO) which in turn include:
 - The provision of prescribed ownership and operational information to the Register of Critical Infrastructure Assets managed by the Cyber and Infrastructure Security Centre.
 - Notification of certain cybersecurity incidents to the Australian Cyber Security Centre.

³ Australian Department of Home Affairs and the Cyber and infrastructure Security Centre, Draft Risk Program Management Rules

- Introducing a requirement for owners and operators of critical infrastructure assets to establish, maintain, and comply with a risk management program to manage the material risk of a hazard occurring, which could impact the availability, integrity, reliability or confidentiality of the critical infrastructure asset
- A mechanism for the declaration of Systems of National Significance (SoNS)— those being the assets most interconnected, interdependent, and essential to Australia’s social or economic stability, defence or national security
- A framework of Enhanced Cyber Security Obligations (ESCO), which may apply to SoNS
- An enhanced framework for the use and disclosure of protected information.

SoNS are a small subset of critical infrastructure assets that are most crucial to the nation, by virtue of their interdependencies across sectors and potential for cascading consequences to other critical infrastructure assets and sectors if disrupted.

Non-compliance with these obligations after they have entered into force⁴ can result in civil penalties of between \$11,100 (50 units) and \$166,500 (750 units) per breach, or per day of breach, depending on the nature of the breach and the specific obligation.

Government Owned Corporations Act

The GOC Act dictates the level of autonomy and accountability that corporations owned by the Northern Territory Government are subject to. One of those accountability measures pertains to Power and Water’s Statement of Corporate Intent (‘SCI’) and risk management governance. Section 40 of the GOC Act requires the SCI to include, among other things, the material risks faced by Power and Water and the strategies to minimise those material risks. Any risks to physical security and corresponding risk management actions identified in this business case must be recorded in the SCI.

NT Health and Safety Act

The NT Health and Safety Act sets out the key principles, duties, obligations and rights in respect to occupational health and safety in the Northern Territory. Under this Act, Power and Water and its management staff have a duty to ensure, so far as is reasonably practicable, that the workplace, means of entering and exiting the workplace and anything arising from the workplace are without risks to the health and safety of any person. The provision of a safe workplace will extend to ensuring the security of the workplace is up to date and safe. The duty is contained in section 20(2) of the NT Health and Safety Act.

Protective Management Standard

The upgrade of electronic security infrastructure is a key requirement of the Power and Water’s *Protective Security Management Standard*, which has been prepared to support the compliance obligations of the SOCI Act. The intent of this Standard is to provide purpose and direction for the safety and security of Power and Water’s information and physical assets and aligns Power and Water with Northern Territory and National arrangements for protective security.

2.3 Current management programs

Security upgrades were carried out in the 2019-24 regulatory period for Power and Water’s six corporate locations. A description of these projects incurred during the 2021/22 year is available in the table below.

⁴ Expected to be in January 2023

Table 4 Security Works at Corporate Locations in 2021/22

Property	Business Case	Description of Works
Sadadeen Valley Complex	CFD30053	Fencing upgrade.
Ben Hammond Complex	CFD30053	Mobile CCTV trailer; fencing upgrade including installation of barb wire; installation of crim safe; upgrade to security system cameras, computers; renovations to the security hut including window tinting, painting, shelving, and other fixtures.
Ben Hammond Complex	CFD30054	Security access and hardware upgrades.
Tennant Creek Complex	CFD30054	Security access and hardware upgrades.
Mitchell Centre	CFD30054	Security access and hardware upgrades.
Victoria Highway Complex	CFD30054	Security access and hardware upgrades.
Sadadeen Valley Complex	CFD30054	Security access and hardware upgrades.

2.4 Asset condition and emerging issues

Some of the security infrastructure is reaching the end of life, obsolescence, or end of warranty.

Over time, electronic hardware and other security infrastructure deteriorates and reaches end of life, becomes obsolete, or is no longer covered by warranty or insurance. In order to maintain appropriate security, these aging assets must be upgraded or replaced.

Additional considerations include:

Geographical operations and considerations: The remote location and nature of the terrain in the Northern Territory may impact the asset life and structural requirements of various aspects of Power and Water’s buildings and facilities. As a result, the geographical location of the building and facilities needs to be taken into consideration and may impact the level of expenditure and security requirements.

Customer expectations: Power and Water’s customer expect their power to be provided in an efficient, timely and secure manner. In order to uphold these expectations, Power and Water must ensure the security of its assets, including all Corporate sites, to ensure there are no disruptions to services.

2.5 Risk Assessment

In demonstrating the need to invest, Power and Water's "**Enterprise Risk Management Standard**" (reference number 02 in Appendix C) and Values Framework was applied. Of the risks contained in the standard, 5 were relevant: legal and regulatory, health and safety, people and culture, data and technology, and governance risks.

2.5.1 Legal and Regulatory Risks

Legal and regulatory risks specifically relate to Power and Water's ability to maintain its 'Licence to Operate' through adherence to the laws and regulations relevant to its business. These risks do not include those related to regulatory compliance in health and safety, which are covered separately. Legal and regulatory risks are identified and managed by the Business Units in consultation with Legal and Secretariat teams. Several pieces of legislation have been identified above as impacting Power and Water's security standards. Non-compliance with any of those legal obligations would enliven this risk.

2.5.2 Health and Safety Risks

Health and safety risks are identified and managed by the Health and Safety and Facilities teams, in collaboration with Site Managers and in accordance with the Work Health and Safety Management Standard. As mentioned above, despite being legislative in nature, any risks and obligations relating to the NT Health and Safety Act fall under this risk category. As set out in section 5.2.2, the obligation to provide a safe workplace under the Act extends to the security of the workplace, ensuring it is up to date, safe and fully functional.

2.5.3 People and Culture Risks

People and culture risks relate to Power and Water's commitment to attract and retain key talent necessary to meet its strategic objectives, and creation of a safe and constructive culture. These risks, which include physical security, are identified and managed by Operations and Corporate Services teams. While security tends to have a primary focus on network assets and electronic security, this business case is focused on Corporate sites, meaning it will affect the security measures in the buildings Power and Water staff and contractors live and work in. Care must be taken to ensure the physical security of all staff and contractors at all times.

2.5.4 Data and Technology Risks

Data and technology risks are associated with the use, ownership, operation, involvement, influence and adoption of technology within Power and Water. This includes risks associated with: information technology, operational technology and data management. Any electronic security assets and infrastructure will fall under this umbrella.

2.5.5 Governance Risks

Governance risks can be defined as the risks associated with failure of the governance framework including the design of structures, roles and responsibilities, policies and procedures and information communication. This includes those risks managed through corporate functions, such as physical security. Of particular note is the risk posed by overhauling the risk management program to ensure it is compliant

with the new SOCI Act obligations. This will need to be carefully managed to ensure there are no flow on impacts to other areas of governance, or to security operations and functions.

2.5.6 Likelihood of non-compliance and security breaches

It is likely that Power and Water's assets will be declared a SoNS and almost certain that if Power and Water does not take reasonable steps to demonstrate that it satisfies the Physical Security Obligations under the SOCI Act it will be in breach of federal legislation and likely to be non-compliant with relevant NT legislation.

It is also possible that without the enhanced physical security measures (required under legislation but also what a prudent operator would apply), there will be an increase in security breaches.

2.5.7 Consequence of failure to act

There are two major consequences of failure to act: non-compliance with legislation and the increased potential for security breaches.

Non-Compliance

Being non-compliant with SOCI Act obligations can result in substantial fines. Additionally, in order to maintain its Licence to Operate, Power and Water must ensure it is compliant with all legislative and regulatory obligations.

Security Breaches

Inadequate security infrastructure will lead to an increase in security breaches, which may impact on Power and Water's insurance and operating expenditure requirements. As outlined above, there are already a number of security incidences occurring each year. It is imperative that these breaches are limited as much as possible to ensure identified risks do not materialise or worsen. In addition, security breaches have flow on effects that impact customers. Minimising security breaches will avoid business disruption, ensure the physical safety of all employees and contractors and the physical protection of ICT assets such as servers containing confidential proprietary information.

The combination of these consequences is assessed to be 'Major'.

2.6 Summary

Physical and electronic security infrastructure deteriorates over time, reaching end of life, becomes obsolete or is void of warranty or insurance. In order to minimise the risks identified above and to remain compliant with all legislative and regulatory obligations, the infrastructure must be assessed and replaced or upgraded as needed. Maintaining the security and safety of all Corporate properties allows for the security of staff, contractors and assets, and therefore the proper provision of services to customers while upholding Power and Water's values.

The overall risk from not acting in accordance with the legislation and otherwise to improve Power and Water's security measures is rated as 'Very High'.

3. Options analysis

This section describes the various options that were analysed to address the identified need. The options are assessed based on ability to address the identified needs, prudence and efficiency, commercial and technical feasibility, deliverability, benefits and an optimal balance between long term asset risk and short-term asset performance.

3.1 Comparison of credible options

Credible options are identified as options that address the identified need, are technically feasible and can be implemented within the required timeframe. The following options have been identified:

- Option 1 – Do nothing. This option proposes no expenditure or mitigation actions taken.
- Option 2 – Head Office Upgrade. This option includes replace/upgrade security infrastructure only at Head Office.
- Option 3 – All Corporate Sites Upgrade. This option includes Replace/upgrade security infrastructure across all Corporate sites.

A comparison of the three identified options and the issues they address in the identified need is depicted in the table below. A detailed discussion of each option is provided below.

Table 5 Summary of options analysis outcomes

Assessment metrics	Option 1	Option 2	Option 3
NPV (\$m, real FY22)	-	-	-
Capex (\$m, real FY22)	-	0.73	1.45
Opex (\$m, real FY22)	-	-	-
Meets customer expectations	○	◐	◑
Aligns with Asset Objectives	○	◐	◑
Technical Viability	○	●	◑
Deliverability	●	●	◑
Preferred	✘	✘	✓
Ranking	3	2	1

- Fully addresses the issue
- ◑ Adequately addresses the issue
- ◐ Partially addresses the issue
- Does not address the issue

As this program of works is required for compliance, the benefits have not been quantified and hence the NPV is negative. A NPV has not been calculated.

3.1.1 Option 1 – Do Nothing

Under this option, no security improvement works will be carried out in association with the investment needs identified in this business case during the 2024-29 regulatory period. This will result in the continuation of the various instances of non-compliance and pose an unacceptable high-risk security situation discussed above in section 2.

The advantages and disadvantages of this options are shown in the table below.

Table 6 Option 1: Advantages and Disadvantages

Advantages	Disadvantages
No upfront or additional expenditure required (when possible fines are not taken into account)	Reduced functionality/operability of existing infrastructure, leading to an increased likelihood that a major security incident may result in a failure to deliver a safe and dependable supply of electricity to customers.
Reliance on existing security will prevent disturbance to program of work – no outages or external contractors on site	Increased security/safety risk profile. Reliance on existing security capabilities will reduce the ability of Power and Water to protect staff, contractors and the community and detect unauthorised intrusions, increasing the likelihood of a major security incident.
	Does not mitigate exposure to financial penalties that may arise due to non-compliance with codes, regulations or legislation
	Significant costs will be incurred by customers to respond to and remediate security breaches, including those resulting from personnel and public injuries.
	Unsupported security capabilities will prevent Power and Water from identifying and responding to new or emerging security threats. It will also prevent Power and Water from responding to uplifts in electricity security industry best practices.
	May result in increased insurance premiums and operational expenditure

This is not a viable option as it does not address the need identified in section 2.

Based on the above information, Option 1 - Do Nothing is not a credible option because it does not address any of the immediate “high” and “very high” level risks and leaves Power and Water non-compliant with numerous legislative and regulatory requirements and obligations. Accordingly, a financial assessment of this cost has not been undertaken.

This option is not recommended.

3.1.2 Option 2 – Head Office Upgrade

This option involves a limited approach combined with preventative action. The order of works will be based on risk assessment with the Corporate Head Office being prioritised, and medium and lower risks being actioned in the future regulatory periods.

This option is estimated to cost \$0.73 million (real 2021/22). The advantages and disadvantages of this options are shown in the table below.

Table 7 Option 2: Advantages and Disadvantages

Advantages	Disadvantages
Mitigates immediate safety and security risks that may be present on head office site	Medium and low risks will remain active for the 2024-29 regulatory period
Ensures immediate compliance at the Head Office with all relevant regulations and legislation, and industry best practice	Other sites may remain non-compliant and a security threat / risk.
Mitigates some exposure to financial penalties that may arise due to non-compliance with regulations or legislation at head office	Insurance coverage may be impacted if active steps are not taken to ensure security and prevent loss.
Allows for proactive and prioritised scheduling and completion of works. In addition, it targets the highest risk sites and provides a practical delivery approach.	
Lower upfront cost option	
Balanced investment option that includes reasonable provisions to address rising security threats according to industry best practice standards	

Based on the above information, Option 2 Head Office upgrade is not the preferred option because it does not address the identified need and poses an unacceptable risk for remaining sites.

Failure to address the identified issues at all sites will result in increased risk to Power and Water. Therefore, despite being the lowest cost option, Option 2 does not prudent represent a prudent option.

This option is not recommended.

3.1.3 Option 3 – Corporate Sites Upgrade

Under this option, all corporate sites will be upgraded in the next regulatory period to fully meet security and / or compliance risks at an estimated cost of \$1.45 million (real 2021/22).

The advantages and disadvantages of this options are shown in the table below.

Table 8 Option 3: Advantages and Disadvantages

Advantages	Disadvantages
Mitigates all safety and security risks that may be present on site	Higher upfront costs, although it will result in lower costs in the long term
Ensures full compliance with all relevant regulations and legislation, and industry best practices	Will require significant resources to plan and deliver the project. Additional resources may be required and they may not be immediately available.
Mitigates exposure to financial penalties that may arise due to non-compliance with regulations or legislation	
Cost efficiencies arising from bulk action (e.g. labour costs)	
Improved protection of people, assets and information	
Delivery on ELT commitments	

This option will fully address the need identified in section 2.2.

This is the recommended option.

4. Recommendation

The recommended option is Option 3 - Upgrade All Corporate Sites at an estimated cost of \$1.45 (real 2021/22). It is the prudent and cost effective approach to meet the identified needs.

The proposed program is consistent with the National Electricity Rules Capital Expenditure Objectives as the expenditure is required to maintain the quality, reliability, and security of supply of standard control services and maintain the safety of the distribution system.

4.1 Strategic alignment

The “Power and Water Corporation Strategic Direction” is to meet the changing needs of the business, our customers and is aligned with the market and future economic conditions of the Northern Territory projected out to 2030.

This proposal aligns with Asset Management System Policies, Strategies and Plans that contributes to the D2021/260606 “Power and Water Strategic Direction” as indicated in the table below.

Table 9 Strategic Direction focus areas

	Strategic direction focus area	Strategic direction priority
1	Always Safe	Embed a Proactive Safety Culture
2	Customer and the community at the centre	Trusted Partner

4.2 Benefits

The table below sets out the benefits and benefit measurements associated with carrying out the recommended option.

Table 10 Benefits of Recommended Option

Benefits	Benefit Measurements
Improved productivity	The number of disruptions arising from security events.
Improved customer service and outcomes	This is an indirect benefit linked to employee engagement and retention.
Improved safety	The number of incidents reported and the number of security-related events on Corporate sites.
Risk reduction and mitigation	The number of safety events, and the dollar value attached to insurance claims.

Benefits	Benefit Measurements
Improved operational efficiency and reduction of opex	There should be a corresponding reduction in insurance premiums.
Avoidance of reputational harm	This is an indirect benefit.
Reduced exposure to fines and penalties	The dollar value attached to fines arising from a breach of or non-compliance with legislative obligations including those under the Work Health and Safety Act and the SOCI Act.

4.3 Dependent projects

The SOCI Act and, particularly the Positive Security Obligations are expected to come into effect from January 2023. Regardless, Power and Water considers that the requirements of the act support the actions of a prudent operator of critical infrastructure and therefore considers the proposed capex to be essential.

4.4 Deliverability

This project will be reliant on third party contractors to be successfully delivered. Power and Water will undertake a competitive tender process to obtain more detailed quotations for work required. All sourcing will be in line with the requirements in the Power and Water Procurement Guidelines. As the external resources may not be immediately available, advanced scheduling will likely be required.

4.5 Expenditure profile

The forecast expenditure for the next regulatory control period allocated to Standard Control Services as per the CAM is outlined in Table 12 for the 2024-29 regulatory period.

Table 11 Annual capital and operational expenditure (\$m, real FY22)

Item	FY25	FY26	FY27	FY28	FY29	Total
Capex	-	-	0.47	0.48	0.50	1.45
Opex	-	-	-	-	-	-
Total	-	-	0.47	0.48	0.50	1.45

4.6 High-level scope

The program described in this business case forms part of an enterprise-wide program.

The scope included for this business case is restricted to the regulated electricity business of Power and Water Corporation. In addition, the scope of the project is limited to Corporate sites only. No other properties or network assets will be upgraded under this business case. Finally, any server software upgrades required in concert with the physical and electronic infrastructure upgrades are also outside of the project scope. There is a separate ICT business case for this activity.

Appendix A. Key assumptions and limitations

The following assumptions have been made for the purpose of this business case:

- It is assumed that only upgrading the security infrastructure, both physical and electronic, at the head office would be half the cost of a security infrastructure upgrade at all six corporate sites.

The following limitations exist for this business case:

- Due to previous data recording processes and management systems, Power and Water does not have a large amount of robust, high-quality data available for benefit quantification. Although the data recording processes and management systems have since been overhauled and will be accurate and reliable going forwards, this means that any past data on may be incomplete. For example, the number of safety incidents (and corresponding incident details).
- As such, it was not possible to conduct a full cost-benefit assessment or properly quantify the benefits and costs.

As per the 'Business Plan – Supply Chain Strategy and Operations (2021-2025)', this program has the following KPIs:

- Delivered on Time
- Delivered on Budget (+/- 10%)
- Delivered Safely (No Loss Time Injury / No Recordable Injuries / No Safety Incidents)

These KPIs will ensure the project is delivered prudently and efficiently, and in a manner which minimises potential risks.

Contact

Power and Water Corporation

55 Mitchell Street, Darwin NT 0800

Phone 1800 245 092

powerwater.com.au

PowerWater