**Risk Assessment**

Boondearwah Dam Risk Assessment

**Prepared for**: BME Energy

**Dated**: 10 December 2021

# DISCLAIMER

This document is based on information gathered by the assessor during the risk assessment process. Observations and recommendations are based upon the assumption that any documented and other forms of information provided to the assessor was complete, factual, accurate and relevant in the circumstances and that processes observed during any inspection activities were indicative of regular practice (unless indicated otherwise).

The intent of this document is to provide an independent perspective on risks included within the scope of the assessment. Recommendations must therefore be reviewed by a suitably authorised person to ensure that each is suitable and appropriate for the organisation.

# TERMS AND DEFINITIONS

| **Term** | **Definition** |
| --- | --- |
| Asset | An item, process or other thing that an individual, organization or community values as important in achieving outcomes and objectives. |
| Consequence | The outcome of an event expressed qualitatively or quantitatively, being a loss, injury, disadvantage or gain. There may be a range of possible outcomes associated with an event. |
| Control | Any existing physical, operational, logical, behavioral, institutional, or cultural mechanism by which a risk is managed (compare with ‘treatment’ definition). |
| Criticality | The importance or dependence that an organisation has on a person, function, process, item or infrastructure or specific facility. |
| Event | A thing that happens or takes place (linked to hazards). |
| Hazard | A situation or thing that has the potential to harm a person (i.e., a source of harm - taken to be non-human induced). |
| Likelihood | Likelihood is the chance that something might happen. Likelihood can be defined, determined, or measured objectively or subjectively and can be expressed either qualitatively or quantitatively. |
| Risk | The chance of something happening that will have an impact upon objectives. Risk is a function of likelihood x consequence. |
| Threat Act | An act committed by a Threat Actor. |
| Threat Actor | An individual, or group of individuals, that could cause harm to an organisation. For example, an insider, petty or serious criminal, issue motivated group or a terrorist. |
| Treatment | The implementation of a risk control/measure that is designed to reduce or mitigate the likelihood or consequence of a risk event occurring. |
| Vulnerability | A weakness that can be exploited to make an asset susceptible to change. |

# TABLE OF CONTENTS

[DISCLAIMER 1](#_Toc1)

[TERMS AND DEFINITIONS 2](#_Toc2)

[TABLE OF CONTENTS 3](#_Toc3)

[EXECUTIVE SUMMARY 4](#_Toc4)

[SCOPE, CONTEXT AND CRITERIA 5](#_Toc5)

[ANNEX A: ASSET CRITICALITY ASSESSMENT 13](#_Toc6)

[ANNEX B: THREAT / HAZARD ASSESSMENT 14](#_Toc7)

[ANNEX C: CONTROLS ASSESSMENT 15](#_Toc8)

[ANNEX D: RISK REGISTER 20](#_Toc9)

[ANNEX E: ASSESSMENT METHODOLOGY 23](#_Toc10)

[Asset Criticality Assessment 23](#_Toc11)

[Threat Assessment 24](#_Toc12)

[Hazard Assessment 25](#_Toc13)

[Controls Assessment 26](#_Toc14)

[Risk Assessment 27](#_Toc15)

# EXECUTIVE SUMMARY

POPULATE OR DELETE THIS SECTION IF IT IS NOT REQUIRED.

# SCOPE, CONTEXT AND CRITERIA

## Scope

The scope of the assessment encompasses security and workplace/occupational health and safety (WHS/OHS) in relation to the site and primary catchment area. In doing so it considers requirements detailed within the Security of Critical Infrastructure Act (2018) and Model WHS Laws.

## Context

### Legislation

As an entity that falls under the Security of Critical Infrastructure Act (2018), and per the Government's Critical Infrastructure Centre website, "Foreign involvement in our critical infrastructure, including through investment, third party contractual arrangements and supply chains, is essential to ensure that the country harnesses global skills and capabilities. These arrangements, however, can provide malicious actors with unique levels of access to and control of critical infrastructure assets, which in turn can be used to facilitate espionage, sabotage or exert coercive influence contrary to our national interests and in a way that can be very difficult to detect or attribute.

"While the more extreme manifestations of sabotage are unlikely to occur in the current geopolitical context, the level of access and control can facilitate pre-positioning for strategic advantage.

The Security of Critical Infrastructure Act 2018 is designed to manage these national security risks from foreign involvement in the country's critical infrastructure in the electricity, gas, water and ports sectors. In addition, the Security of Critical Infrastructure Rules 2018 specify thresholds for electricity generation stations and gas transmission pipelines, prescribe critical infrastructure assets and provide further information requirements for reporting.

The Act aligns with the government-business partnership-approach that underpins the country's Critical Infrastructure Resilience Strategy. This strategy recognises that in most cases neither business nor government in isolation have access to all the information they need to understand and appropriately mitigate risks to the continuity and integrity of services.

This Act ensures that Government has all the necessary information to conduct national security risk assessments as well as the ability to enforce risk mitigations if they cannot be addressed through other means.

To ensure this is the case, the Act introduced three measures:

* an asset register, provides the Government visibility of who owns and controls the assets, enabling better targeting of our risk assessments
* the ability to obtain more detailed information from owners and operators of assets in certain circumstances to support the work of the Centre
* the ability to intervene and issue directions in cases where there are significant national security concerns that cannot be addressed through other means.

The measures contained in the Act apply to both domestic and foreign owned critical infrastructure and take account of the country’s trade agreements and other international obligations.

The powers in this Act enable government to better assess the extent of vulnerability across...high priority assets, and work collaboratively with industry to address the kinds of vulnerabilities identified, while maintaining open economic settings and imposing only a minimal and targeted regulatory burden."

Separately, the national Model WHS Laws (Act and Regulations) provide for a balanced and nationally consistent framework to secure the health and safety of workers and workplaces. It does this by:

* underpinning mechanisms for the protection of workers and other persons from harm by requiring duty holders to eliminate or minimise risk;
* providing for fair and effective representation, consultation and cooperation;
* encouraging unions and employer organisations to take a constructive role in promoting improvements in WHS practices;
* promoting the provision of advice, information, education and training for WHS;
* securing compliance with the Act through effective and appropriate compliance and enforcement measures;
* ensuring appropriate scrutiny and review of actions taken by persons with powers or functions under the Act;
* providing a framework for continuous improvement; and
* maintaining and strengthening national harmonisation of WHS laws and facilitating a consistent national approach to WHS.

### Organisational Structure

Among other accountabilities, the Chief Risk Officer (CRO) retains responsibility for Health, Safety and Security risk management practices. The CRO reports directly to the CEO, and also to a Sub-Committee of the Board, which is designed to ensure direct Board oversight of organisational risk and compliance functions, especially in relation to matters of security and safety.

Reporting to the CRO are several full time staff, with two specifically focused on day to day management of saftey and security. Informed by those personnel, the CRO also has the primary reporting role that reports notifiable incidents to the organisation's regulators.

Working to the security manager, a single security guard is stationed at the operations building 24x7.

### Geographical

The site is located at Boondearwah, which is 250km north-east of Tombilins. It is located adjacent to PGM's electricity generation plant, and shares an access road with it.

The dam helped drive the economic development of areas surrounding the catchment area as a major food producing region. Today the dam continues to support agriculture across the 830,000km2 of the Neidal Irrigation Area centred around the towns of Boolinds and Equenti. It also supplies stock and household needs for landholders and towns along the Timerool River, environmental flows, flood mitigation and hydroelectricity. The large lake has become a popular sport and recreation destination.

**Image 1**: The Dam

### Security and Safety Budget and Resourcing

In relation to security and safety, the budget of the CRO meets the needs of forecast CAPEX and OPEX requirements for the 12-month forward period. Senior management are sympathetic to budget revision, especially in view of new legislation, and accompanying expertise required to address function-related vulnerabilities. In previous years the budget has been adequate to cover needs, and incident history demonstrates that an effective risk-based approach, balancing functional and financial imperatives, has been taken.

### Asset Criticality

In the absence of an asset (or indeed a threat), it is problematic to assert that a risk can exist. Per the scope of the assessment, the underlying philosophy in this risk assessment, therefore, is/was to identify assets at risk from threats and hazards, and to determine how critical they are to the organisation in performing its functions. Doing so provides the basis from which to examine the effectiveness of related risk controls, and to consider and prioritise risk mitigations.

The site has several sub-assets that are critical to the effective operation of the dam, while numerous others play a supporting role. This assessment documents those that are most critical, and assigns an Asset Criticality Rating to each; this is presented within at stage 2 of the assessment, or at Annex A (Asset Criticality Assessment) where the assessment has been printed.

### Threat Summary

Generally speaking, security threats, as distinct from safety hazards, tend to be derived from human sources, rather than those arising from the natural or built environment. As such and for the purposes of risk planning, it has been typical of benchmark entities to categorise human-derived threats generally within the following groups:

* Insiders;
* Outlaw Motorcycle Gangs (OMCGs);
* Petty Criminals;
* Issue Motivated Groups (IMGs);
* Serious & Organised Criminals (S&OCs);
* Cyber Criminals;
* Terrorists; and
* Foreign Intelligence Services (FISs).

There is however an acknowledged limitation in the process of seeking to definitively categorise threat sources, as individuals and groups typically demonstrate characteristics of multiple types of threat. Examples may include an organised criminal being considered a form of terrorist and a trusted insider also being classified as a petty criminal etc.

Nonetheless and when risks derived from each group are considered holistically, this limitation tends to be largely mitigated, and a tabulated summary of assessed threats appears within Annex B (the Threat Assessment).

#### Insiders

A trusted insider is considered anyone who has been granted approval to access an organisation’s systems, facilities, information and/or other assets. This threat category includes past and present employees and contractors and visitors, in the context of both while they are directly involved with an organisation, and following this through retention of confidential knowledge that may facilitate a future illegal act. Studies of the threat posed by insiders show the majority of insiders do not act for terrorist or espionage purposes, but rather for motives of financial gain, disgruntlement or revenge.

It bears mentioning in view that trusted individuals do not necessarily require to be predisposed to criminal undertakings; opportunism, compounded by circumstance, may turn an otherwise trustworthy person into someone who seeks to deliberately steal or harm an organisation and/or its assets.

Rogue and/or disgruntled ex-employees who take advantage of their insider knowledge may commit a range of crimes. This may include: low-end acts such as stealing office equipment such as computers, phones, corporate credit cards or other transactional items; unauthorised sharing or leaking of sensitive information, including information on ongoing or high profile legal cases; and serious crimes such as assault or threat of assault on company personnel.

Disgruntled employees (current or previous) may be particularly vulnerable to assisting organised criminal, petty criminal, and issue motivated group interests, or in extreme cases, terrorist interests via the provision of company information (e.g. confidential documents), access to information (e.g. intranet password), and/or access to physical assets (art pieces, production equipment etc.). A rogue employee or contractor may also act on their own accord for financial gain, commonly to hack systems and provide information to a competitor.

In summary, the likelihood of a trusted insider attack may be largely precipitated by any combination of these factors. Furthermore, vigilance by the organisation is warranted with regards to outgoing and ex-employees who have previously come to the attention of HR for behavioural and/or other misconduct issues (in addition to regular personnel security practices, such as reporting/noting change of circumstances, suspicious or unusual behaviour, etc.)

#### Outlaw Motorcycle Gangs

In some contexts, OMCGs pose a specific and credible threat to personnel and other assets, demonstrated by multiple documented criminal events and enterprises in recent years. However, and in the absence of any specific threats or other information to suggest that such entities and individuals hold a specific interest in the site/entity, OMCGs are not assessed as posing a unique threat to the organisation.

It was however considered judicious to reflect that such organisations are widely recognised as criminal enterprises, and as such have been considered within the context of Serious & Organised Criminals’.

#### Petty Criminals

Incidents of property crime and theft from person in most major cities have been in overall decline over the past five years. However, there are exceptions to these trends, with certain pockets in some cities and regional hubs showing small increases in these types of crime. Although Aginkert was deemed the world’s most liveable city in various recent years, petty crime was a key area where the city did not perform well.

The threat of opportunistic theft at commercial and/or infrastructure sites is an ongoing concern for most organisations in the country. However, this crime is often under-reported or not reported at all and accurate statistics are difficult to obtain.

Buildings with external public access and internal public/private access across the region have been subject to a broad spectrum of petty crimes ranging in seriousness from public nuisance or graffiti vandalism incidents to theft of personal possessions and/or company assets to violent assaults. These may be carried out by employees, contractors, or members of the public, and they may be targeted or random incidents.

#### Issue Motivated Groups (IMGs)

Lawful advocacy, protest and dissent are part of the country's political culture. Most IMGs engage in these activities peacefully and the significant majority of them do not support or participate in violent protest activity. However, a small minority of protesters have previously employed violent and/or confrontational tactics during protests and will continue to occasionally do so.

Each time a similar event occurs, it has the potential to attract copycat protestors and others through the exposure that the site attracts. This is especially true in relation to environmental protestors.

#### Serious and Organised Criminals (S&OCs)

Despite its generic tag and clear overlap with some other threat categories, this ‘criminal’ threat is considered in the context of serious, organised crime, excluding terrorism-related events.

S&OCs typically operate in multiple sectors across the licit, grey, and black markets, in both formal and shadow economies. S&OC illegal activities include: kidnap for ransom; extortion; armed robbery; high-end burglary; drugs trafficking/sale; firearms trafficking; fraud; money laundering; financial crime; and cyber-crime . Art theft is also considered a serious and organised crime by FBI and other law enforcement agencies.

While this assessment identified minor cases of theft, there were no examples or evidence identified that suggested a threat from this Threat Actor.

#### Cyber Criminals

All industries are at risk of becoming a victim of cybercrime (as part of serious and organised crime, and to some extent terrorism) in its various forms. Per the Cyber Security Centre’s 2015 Threat Report, the country's Signals Directorate responded to 1,131 cyber-security threat incidents in 2014.

This was a 20% increase on the previous year when the number of incidents was 940, and in 2011 it was just 313. The theft of intellectual property and/or commercially sensitive information is the most significant problem for businesses who have been the subject of a cyber-attack.

Indeed, the entity is custodian to sensitive information and intellectual property from multiple stakeholder groups that may be vulnerable to a cyber-attack. Also, a concern for cyber security is the entity's commercial information, including financial and personal details of customers in addition to payment card details.

The modus operandi of cybercriminals can be as diverse as their motivations. Perpetrator profiles include rogue employees, the environmental lobby and politically-motivated and other malicious attackers. The reach and subsequent impact of successful cyber-attacks has increased dramatically worldwide over the past five years.

Organised crime groups are reportedly “using sophisticated malware to improve their success and avoid detection in gaining unauthorised access to computer systems”. A significant case in the energy industry involved executives who “were regularly using a common website that had been turned into a "watering hole’” (a site with embedded malware).

#### Terrorists

At the time of writing, the National Terrorism Threat Level remains at PROBABLE (“Credible intelligence, assessed to represent a plausible scenario, indicates an intention and capability to attack...”), as detailed under the National Terrorism Threat Advisory System.

The February 2015 national security statement made salient the significant breadth of the modus operandi of terrorists; from simply orchestrated acts undertaken in the spirit of ISIS’ exhortations (that require “little more than a camera-phone, a knife, and a victim” ) to sophisticated/complex potential future attacks (as suggested by the reported rising number of potential home grown terrorists). In 2015, the country's intelligence agency reported more than 400 high-priority investigations underway into the terrorism threat; notably, the perpetrator of the Lindt Café siege was not on this list, indicating that more than 400 extremists are present within the country.

Currently, the most likely type of terrorist attack is one with low levels of coordination and basic resourcing. Vehicle or person borne improvised explosive devices (IEDs), an armed attack on employees or visitors, suicide or stand-off attacks, individuals or a group of offenders are all variables in a range of possible terrorism scenarios. Moreover, a lone wolf style attack should not be discounted, such attacks are far more difficult for the authorities to identify in their planning phase than a coordinated attack involving multiple participants and/or locations, as they require limited, if no communication, and are often simplistic in their execution (although their outcome may be violent and devastating).

A highly-coordinated attack with sophisticated weaponry is less likely, however, not impossible. Also, relevant to some extent is a cyber-attack or terrorism related hoax, such as the recent spate of threats made against schools. The latter issue has been a significant cause in community disruption and rising angst among students and parents, which is a generally stated terrorist objective.

From a global perspective, the country remains a target of high profile terrorist groups including al-Qaeda and more recently ISIS. In 2015, senior ISIS propagandist Abu Mohammad al-Adnani promised violence “worse and more bitter” than Paris in several Western countries. Located closer to home, ISIS is reportedly building its presence throughout the Philippines and Indonesia by establishing training camps.

In January 2016, it is believed that ISIS announced the unification of four battalions in the Philippines. The training camps will likely seek to attract recruits from Southeast Asia and Australia. Members of Jemaah Islamiyah (JI), who found infamy following the 2002 Bali bombings, remain somewhat of a threat, with an interest in ‘soft targets’. However, JI has lost much of its potency over the past decade, due to external disruptions by security and intelligence agencies and internal disputes resulting in its splintering into smaller factions.

#### Foreign Intelligence Services

As reported by the country's intelligence agency, "Espionage and foreign interference targeting national interests remains pervasive and enduring. The agency has observed increased targeting of national interests within the country and abroad through a variety of methods against an array of sectors. The country is a target of hostile foreign intelligence services as a result of:

* strategic alliances and the defence relationship we share with other countries;
* a desire to gain privileged insights into our strategic interests and positions on international diplomatic, economic and military issues;
* a desire to gain commercial advantage on matters including our energy and mineral resources;
* a desire to gain access to our innovations in science and technology;
* a desire to shape the actions of decision-makers and public opinion in favour of the adversary; and
* the reach of online technologies enabling hostile cyber activities.

A range of countries continue to conduct espionage against vital national interests. The range, scale and sophistication of foreign powers engaged in hostile cyber espionage activity against Government and private sector systems continues to increase, as does the threat from malicious insiders. An increasing number of countries are pursuing a cyber espionage program as this offers high returns for relatively low cost and plausible deniability. The continued evolution of technology increases the sophistication and complexity of attacks, while also becoming increasingly accessible.

The harm caused by hostile intelligence activity can undermine national security and sovereignty. It can damage international reputation and degrade our diplomatic and trade relations. Both espionage and foreign interference can inflict economic damage, degrade or compromise nationally vital assets and critical infrastructure, and threaten the safety of the populace. One of the most insidious features of both espionage and foreign interference is that even a small level of activity can have severe consequences which take years to be realised."

### Hazard Summary

With regards to issues of safety, hazards are taken to be situations or things that have the potential to harm a person; "Things' in this context are taken to not be persons or groups (i.e. human derived).

Hazards can appear in many occupational circumstances. Some hazards are acute and pose an immediate danger to the health and physical integrity of the worker or guests on the premises. Others take a longer time to materialize and may have a cumulative effect, as is the case for certain chemicals, vapors, dusts, and radiation that may lead to chronic medical conditions following repeat or prolonged exposure. Examples include:

* **Physical Environment**: These are the most common hazards and they include extremes of temperature,  radiation, excessive noise, electrical exposure, working from heights, and machinery.
* **Mechanical Items**: These are usually created by machinery, often with protruding and moving parts.
* **Chemicals & Gasses**: These appear when a worker is exposed to chemicals in the workplace. Some are safer than others, but for workers who are more sensitive to chemicals, even common solutions can cause illness, skin irritation, or breathing problems.
* **Biological Agents**: These include the viruses, bacteria, fungus, parasites, and any living organism that can infect or transmit diseases to human beings.
* **Ergonomic Factors**: Including considerations of the total physiological demands of the job upon the worker, even beyond productivity, health, and safety.

### Risk Controls Effectiveness

The existence, and indeed effectiveness of, controls that reduce risk levels associated with assets is a critical measure in determining the organisation's risk profile, and consequently its ongoing level of risk exposure. Absent, or poorly designed/implemented or operated risk controls inhibit the ability to manage such risks, and weaknesses must be remedied in order to address areas of vulnerability.

Within this assessment relevant risk controls, details on their current status, and effectiveness ratings, are presented within stage 4 of this assessment, or within Annex C (Risk Control Effectiveness Assessment) where it has been printed.

Criteria

Risk and evaluation criteria was derived from the BME Energy Enterprise Risk Management Framework (ERMF).

# ANNEX A: ASSET CRITICALITY ASSESSMENT

The following assets were identified as falling within the scope of the assessment. The categorization and criticality of each was also assessed to inform risk identification and treatment processes.

| **Asset Details**  | **Asset Category**  | **Criticality**  |
| --- | --- | --- |
| Ops IT Network | Systems | VITAL |
| Sensitive Data | Information | VITAL |
| Operations Building | Infrastructure | VITAL |
| Essential Functions | Systems | VITAL |
| Employees | People | KEY |
| Intellectual Property | Intangible | KEY |
| SCADA Systems | Systems | KEY |
| Public Confidence | Intangible | KEY |
| Cash & Finances | Intangibles | KEY |

**Table:** Asset Criticality Assessment

# ANNEX B: THREAT / HAZARD ASSESSMENT

The following sources of risk were assessed in support of risk identification and analysis.

| **Type** | **Actor / Hazard** | **Act / Event** | **Primary assets at Risk** | **Rating** |
| --- | --- | --- | --- | --- |
| Threat | **Terrorists** | PBIED attack | EmployeesOperations Building | **Significant**ImpliedDeveloped |
| Armed shooter attack | Employees | **Medium**NoneAdvanced |
| Vehicle ramming attack | Employees | **Low**ExpressedUndeveloped |
| Threat | **Cybercriminals** | Hacking | Intellectual PropertySCADA SystemsSensitive Data | **Extreme**DedicatedAdvanced |
| Threat | **Foreign Intelligence Services** | Espionage | Intellectual PropertySCADA SystemsSensitive DataPublic Confidence | **Extreme**CommittedAdvanced |
| Coercion | Sensitive Data | **High**ExpressedAdvanced |
| Hazard | **Chemicals & Gasses** | Inhalation of dangerous gases | Employees | **Critical** |
| Hazard | **Physical Environment** | Slip, trip or fall | Employees | **Emerging** |
| Hazard | **Mechanical Items** | Equipment malfunction | Employees | **Emerging** |

**Table:** Threat / Hazard Assessment

# ANNEX C: CONTROLS ASSESSMENT

Areas of vulnerability and the effectiveness of related risk controls were examined within the Controls Assessment stage; findings are documented within the table below, accompanied by Control Effectiveness ratings for each assessed control.

| **Controls** | **Control Comments** | **Rating** |
| --- | --- | --- |
| **Security Governance** |
| General Security Policies | The organisation has developed a range of general security policies, but all are out of date and require review to ensure currency. They are also not integrated with other security-domain policies, and overall the program lacks coordination. | INADEQUATE |
| Emergency Management Program | A robust 3745:2010 conforming emergency program has been established, along with a requisite Dam Safety Plan, which incorporates emergenacy procedures for the dam itself. | ADEQUATE |
| Crisis Management | An effective crisis framework exists and is tested annually. | ADEQUATE |
| Reporting/Investigations | Security reporting and investigations are demonstrative of best practice and align with Commonwealth standard defined within the PSPF. | ADEQUATE |
| Lockdown Procedures | Lockdown procedures have been developed and are incorporated within the site Emergency Plan. These involve utilising the reinforced pump room, which is adjacent the Operations Building, as a safe haven. | ADEQUATE |
| Contractor management | Contractors are drawn from a close community and trusted suppliers are used in favour of new organisations. Individuals who work onsite are required to be subjected to the same pre-employement vetting as our own staff are, or they are not issued an access pass to get on site. | ADEQUATE |
| Audit processes | Audit processes are in place but Internal Audit functions focus strictly on cybersecurity and not the broader program that protects people, infrastructure and other assets. | MODERATE |
| Security culture | Security culture is not particularly well developed across the organisation, with inadquate, visual senior management support, and a lack of enabling activities, such as security-specific induction training, performance KPIs and awards for good security perfromance. | MODERATE |
| Induction training | Induction training is generic and focused on business and operational issues, not security. | MODERATE |
| **Personnel Security** |
| Pre-employment vetting | Vetting is outsourced to our recruitment partner, Vilexines Pty Limited. Designated positions require greater levels of vetting according to the authority and role that the position entails. | ADEQUATE |
| Security clearances | Security clearances are issued according to the DSAP register. Reviews and revalidations are conducted by the Government Security Vetting AGency (GSVA) and its contracted entities. | ADEQUATE |
| Awareness training | There is a lack of security-focused induction training material and ongoing awareness reminders. | MODERATE |
| PERSEC policies | PERSEC policies are owned and managed by People and Culture, with input provided by security. With an increase in obligatory security requirements arising, this is not ideal. | MODERATE |
| **Information Security** |
| Application patching | This is conducted consistent with ASD's Top 4 Mitigation Strategies. | ADEQUATE |
| Application hardening | This is conducted consistent with ASD's Top 8 and 35 Mitigation Strategies. | ADEQUATE |
| Backup & Recovery | Backups are maintained offsite and include a RPO of 10 minutes. | ADEQUATE |
| INFOSEC policies | INFOSEC policies are managed by the CISO, consistent with ISO 27001 and ASD's Top 35 Mitigation Strategies, especially those in the Top 4 and 8. | ADEQUATE |
| IT access controls | Access controls are similarly managed consistent with ASD Top 4 mitigations. | ADEQUATE |
| **Physical Security** |
| Perimeter security | The perimeter is porous and mesh fencing is in need of repair in multiple locations. | INADEQUATE |
| CCTV | Newer IP-based CCTV cameras have been installed are monitored offsite in real-time. They are also equipped with event-detection software, increasing awareness of pre-defined conditions. | ADEQUATE |
| CPTED | CPTED has been effectively implemented throughout the site. | ADEQUATE |
| Access controls | Access controls are accommodated through dual-factor card swipe and PIN arrangements at all access points. Mechanical locks and keys are minimised, but where they exist they are controlled through a masterkey system. | ADEQUATE |
| Duress system | Duress points/buttons have not been installed, which limits the ability for individuals in distress to call for help quickly. | MODERATE |
| Guard force | A single security guard is stationed within the vicinity of the Operations Building 24x7. | MODERATE |
| Lighting | Illumination within the carpark is adequate, but improvements could be made along the pathway leading to the operations building. | MODERATE |
| **WHS/OHS Program** |
| Policies & Governance | * Health and safety is notated as a key priority in the company's vision statement and WHS Policy.
* A procedure is in place for workers to report injuries, illnesses, incidents (including near misses/close calls), hazards, and safety and health concerns.
* Workplace inspections are conducted with workers, and they are trained how to identify and control hazards.
* Roles and responsibilities are noted within a WHS Management System.
* Arrangements exist to report 'notifiable incidents' within stipulated timeframes.
 | ADEQUATE |
| **WHS/OHS Procedures** |
| General Housekeeping | * The workplace is clean, orderly, and sanitary.
* Workplace floors are maintained in a dry condition.
* Where wet processes are used, drainage is maintained and false floors, platforms, mats, or other dry standing places are provided, where practicable, or workers use appropriate footwear.
* Appropriate precautions are taken to maintain exits, and protect workers during construction, renovation, and repair operations.
* Combustible scrap, debris and waste materials (oily rags, etc.) are stored in covered metal receptacles and promptly removed from the site.
 | ADEQUATE |
| Vermin Control | Enclosed workplaces are maintained to prevent the entrance of rodents, insects, and other vermin; and a continuing and effective extermination program is instituted where their presence is detected. | ADEQUATE |
| Compressed Gas Management | * Cylinders are clearly marked to identify their contents.
* Cylinders are regularly examined for obvious signs of defects, deep rusting, and leakage.
* Liquefied gases are stored and shipped valve end up with valve-protection caps in place.
 | ADEQUATE |
| Ventillation | In most areas, general dilution or local exhaust ventilation systems are used to control dusts, vapors, gases, fumes, smoke, solvents, or mists generated in the workplace. Some storage areas have not been equipped with ventilation, however, requiring procedural arrangements to be implemented for manual air circulation. | MODERATE |
| Fire Protection | * Fire extinguishers are not visually inspected monthly, and the inspections are not presently recorded.
* Workers expected to use fire extinguishers are provided with initial training in their use and annually thereafter.
* Fire extinguisher discharge nozzles are free from obstructions or blockage.
* The fire alarm system has been certified, is in proper working condition, and is tested annually.
 | MODERATE |
| Preventative Maintenance | * An equipment inspection and testing regime has been implemented.
* Log records are not being maintained effectively, however.
 | MODERATE |

**Table:** Controls Assessment

# ANNEX D: RISK REGISTER

| **ID** | **Threats / Hazards** | **Primary Assets** | **Current Controls** | **Risk Description** | **Current Risk** | **Recommended Treatments** | **Residual Risk** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | Threat:**Cybercriminals**Hacking(Extreme) | Intellectual Property (KEY). SCADA Systems (KEY). Sensitive Data (VITAL). | INFOSEC policies. Application patching. IT access controls. Induction training. Security culture.  | A cybercriminal uses social engineering to solicit information to launch an attack on the operations network, resulting in loss of sensitive information and compromising essential functions. | **High**LikelyMajor | Add security KPIs to all employee performance reviews.Arrange for the CEO to visibly promote security as a priority.Include an information security component to online induction training. | **Medium**UnlikelyModerate |
| 2 | Threat:**Foreign Intelligence Services**Coercion(High) | Sensitive Data (VITAL). | Reporting/Investigations. General Security Policies. Awareness training.  | A FIS operative coerces an employee to provide access to sensitive data, resulting in loss of IP and compromising continuity. | **High**PossibleMajor | Review the existing GOVSEC policy suite for currency and efficacy.Include this risk within induction and awareness training. | **Low**UnlikelyMinor |
| 3 | Hazard:**Chemicals & Gasses**Inhalation of dangerous gases(Critical) | Employees (KEY). | Compressed Gas Management. Ventillation. Policies & Governance.  | Poor chemical/gas management practices result in dangerous conditions (e.g. a leak), resulting in serious injury to employees. | **High**PossibleMajor | Install automated ventilation mechanisms for storage areas A, B and C.Install gas leak detection alarms in all gas storage areas. | **Low**UnlikelyMinor |
| 4 | Hazard:**Mechanical Items**Equipment malfunction(Emerging) | Employees (KEY). | Preventative Maintenance. Policies & Governance.  | Equipment fails due to a lack of maintenance/inspection, resulting in major injury(s) to operators and/or others nearby. | **High**PossibleMajor | Review log record keeping practices to ensure that maintenance is conducted per OEM specifications. | **Medium**UnlikelyModerate |
| 5 | Threat:**Terrorists**Armed shooter attack(Medium) | Employees (KEY). | Guard force. Emergency Management Program. Perimeter security.  | An armed terrorist gains access to the site and severely wounds personnel with a firearm. | **Medium**RareCatastrophic | Consider repairing perimeter fence to limit access.Risk is otherwise within tolerances - monitor and review. | **Medium**RareCatastrophic |
| 6 | Threat:**Terrorists**PBIED attack(Significant) | Employees (KEY). Operations Building (VITAL). | Emergency Management Program. CCTV. Perimeter security.  | A terrorist gains access to the site by foot and detonates an explosive device at a critical location, resulting in compromise of the dam wall, or major impacts on the ops building and people. | **Medium**RareMajor | Consider repairing perimeter fence to limit access.Risk is otherwise within tolerances - monitor and review. | **Medium**RareMajor |
| 7 | Threat:**Foreign Intelligence Services**Espionage(Extreme) | Intellectual Property (KEY). SCADA Systems (KEY). Sensitive Data (VITAL). Public Confidence (KEY). | Contractor management.  | An FIS operative employed by a third party use privileged information to access sensitive information, resulting in loss of IP and compromising continuity. | **Medium**RareMajor | Risk is within tolerances - monitor and review. | **Medium**RareMajor |
| 8 | Hazard:**Physical Environment**Slip, trip or fall(Emerging) | Employees (KEY). | General Housekeeping. Policies & Governance.  | A lack of cleanliness within the physical workplace environment causes injury to an employee, resulting in moderate injury(s). | **Low**UnlikelyMinor | Risk is within tolerances - monitor and review. | **Low**UnlikelyMinor |

**Table:** Risk Register

# ANNEX E: ASSESSMENT METHODOLOGY

The International Standard for assessing risks is ISO 31000:2018 Risk Management - Guidelines. Multiple standards extend on the generic methodology espoused within the standard when examining function-specific risks, such as those associated with health, safety and security. In particular, those standards articulate the manner in which assets, sources of risk (threats and hazards) and control effectiveness should be considered initially and throughout the risk management process.

The methodology applied in completing this assessment was consistent with both ISO 31000 and those other recognised standards, and the following criteria was applied during the assessment process.

## Asset Criticality Assessment

| **Criticality Rating** | **Criteria** |
| --- | --- |
| VITAL | * Alternative services and/or facilities cannot be provided if asset is lost or severely damaged.
* Loss or compromise will result in abandonment or long-term cessation of the functions or core business practices.
* Loss or compromise will have a debilitating impact on the reputation of the organisation (international, permanent).
 |
| KEY | * Major restrictions to core business practices will result if asset is lost or severely damaged.
* Loss or compromise will result in long-term cessation/disruption of core business.
* Loss or compromise will have a major, widespread impact on the organisation’s reputation (national, sustained).
 |
| IMPORTANT | * Some minor restrictions to core business practices will result if asset is lost or severely damaged.
* Loss or compromise will result in short-term cessation/disruption of core business.
* Loss or compromise may have an impact on the organisation’s reputation (regional, short-term).
 |
| SUPPORTING | * Business as usual services and/or facilities can be provided if asset is lost or severely damaged.
* Loss or compromise will not result in cessation/disruption of core business.
* Loss or compromise will have no discernible impact on the organisation’s reputation.
 |

**Table:** Asset Criticality Assessment Criteria

## Threat Assessment

|  | **Intent** |
| --- | --- |
|  | **None** | **Implied** | **Expressed** | **Committed** | **Dedicated** |
| **Capability** | **Advanced** | Medium | Significant | High | Extreme | Extreme |
| **Developed** | Medium | Significant | High | High | Extreme |
| **Developing** | Low | Medium | Significant | High | High |
| **Emerging** | Low | Low | Medium | Significant | High |
| **Undeveloped** | Low | Low | Low | Medium | Significant |

**Table:** Threat Assessment Criteria

No entries were made within the Risk Register in relation to ratings for ‘Threat Acts’ that were assessed less than the Threat Tolerance threshold below, but these remain documented for future review.

|  |  |  |
| --- | --- | --- |
|  | Extreme | Threat Acts rated at this level must appear within the Risk Register. |
|  | High | Threat Acts rated at this level (and higher) must appear within the Risk Register. |
|  | Significant | Threat Acts rated at this level (and higher) must appear within the Risk Register. |
| Selected | Medium | Threat Acts rated at this level (and higher) must appear within the Risk Register. |
|  | Low | Threat Acts rated at this level (and higher) must appear within the Risk Register. |

**Table:** Threat Tolerance Criteria

## Hazard Assessment

| **Hazard Rating** | **Criteria** |
| --- | --- |
| Critical | * Event would be of vigorous intensity.
* Event could materialise with minimal warning.
* Event would be prolonged.
* The event is within close proximity.
* The event would be highly volatile.
* The event would be highly persistent.
 |
| Emerging | * Event would be of moderate Intensity.
* Event could materialise with manageable warning.
* Event would be of moderate duration.
* The event is within intermediate proximity.
* The event would be of medium volatility.
* The event would be moderately persistent.
 |
| Benign | * Event would be of low Intensity.
* Could materialise with ample warning.
* Event would be short-term.
* The event is distant.
* The event would be of low volatility.
* The event would not be persistent.
 |

**Table:** Hazard Assessment Criteria

No entries were made within the Risk Register in relation to ratings for ‘Events’ that were assessed less than the Hazard Tolerance threshold below, but these remain documented for future review.

|  |  |  |
| --- | --- | --- |
|  | Critical | Critical for considered in risk assessment |
|  | Emerging | Must be considered in risk assessment |
| Selected | Benign | Should be considered in risk assessment |

**Table:** Hazard Tolerance Criteria

## Controls Assessment

Vulnerabilities were identified through assessing Control Effectiveness, using the criteria within the table below.

| **Rating** | **Criteria** |
| --- | --- |
| MODERATE | * Most control elements are designed correctly, in place and effective.
* Some more work should be considered to improve operating effectiveness.
* There may be doubts around operational effectiveness and reliability.
 |
| ADEQUATE | * Control elements are well designed to address threats.
* Nothing more to be done except review and monitor control elements.
* There are no doubts that the controls are the most appropriate for the task.
 |
| INADEQUATE | * Controls do not address threats effectively.
* There are significant control flaws or no credible controls at all.
* There are obvious doubts that the controls will work as intended.
 |

**Table:** Controls Assessment Criteria

## Risk Assessment

| Increasing Likelihood -> | **Likelihood Rating** | **Likelihood Descriptor** |
| --- | --- | --- |
| Certain | Occurs on an annual basis and will happen again in the short term. |
| Likely | Has occurred in last few years within the organisation or something has occurred that will cause it to happen in the short term. |
| Possible | Has occurred at least once within the organisation and is likely to occur again in the medium term. |
| Unlikely | Is possible but has not occurred to date and is considered to have less than a 1% chance of occurring within the organisation. |
| Rare | Has never occurred within the organisation but has occurred infrequently elsewhere and it is possible that it could occur in the medium term. |

**Table:** Risk Likelihood Criteria

|  | Increasing Consequence -> |
| --- | --- |
|  | Negligible | Minor | Moderate | Major | Catastrophic |
| People | Minor injury or first aid treatment. | Injury requiring treatment by medical practitioner and/or lost time from workplace | Major injury/hospitalisatzion | Single death or multiple major injuries | Multiple Deaths |
| Information | Compromise of information otherwise available in the public domain | Minor compromise of information sensitive to internal or sub unit interest | Compromise of information sensitive to organisation operation | Compromise of information sensitive to organisation interests | Compromise of information with significant ongoing impact |
| Economic | 1% of budget (organizational, division or project budget as relevant) | 2-5% of Annual Budget | 5-10% of Annual Budget | >10% of Budget | >30% of Project or organizational annual budget |
| Reputation | Local mention only. Quicky forgotten. Freedom to operate unaffected. Self-improvement review required | Scruttiny by excecutive, internal committees or internal audit to prevent escalation Short term local media concern. some impact on local level activities | Persistent national concern. Scrutiny required by external agencies. Long term "brand" impact. | Persistent intense national public, political and media scrutiny. Long term "brand" impact. Major operations severely restricted | International concern, goverment inquiry or sustained adverse national/international media. "Brand" significantly affect organization abilities |
| Capability  | Minor skills impact. Minimal impact on non-core operations. The impact can be dealt with by routine operations | Some impact on organization capability in terms of delays, systems quality but able to be dealt with at operational level | Impact on the organisation resulting in reduced performance such that targets are not met. Organisation existence is not threatened,but could be subject to significant review | Breakdown of key activities ect leading to reduction in business performance (e.g. service delays, revenue loss, client dissatisfaction, legislative breaches) | Protracted unavailability of critical skills/people. Critical failure(s) preventing core activities from being performed. Survival of the project/activity/organisation is threatened  |
| Property | Minor damage or vandalism to asset | Minor damage or loss of <5% of total assets | Damage or loss of <20% of Assets | Extensive damage or loss of <50% of assets | Destruction or complete loss of > 50% of assets |

**Table:** Risk Consequence Criteria

|  | Negligible | Minor | Moderate | Major | Catastrophic |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
| Certain | Medium | Medium | High | Extreme | Extreme |
| Likely | Low | Medium | High | High | Extreme |
| Possible | Low | Medium | Medium | High | High |
| Unlikely | Low | Low | Medium | Medium | Medium |
| Rare | Low | Low | Low | Medium | Medium |

**Table:** Risk Matrix

Once assessed, risks were then evaluated against thresholds within the table below and considered for treatment within the Risk Register.

| **Tolerance Level** | **Risk Rating** | **Risk Treatment Requirements** |
| --- | --- | --- |
|  | Extreme | Risk cannot be justified on any grounds - immediate risk treatment or avoidance is mandatory. |
|  | High | Risk exceeds the organisation’s tolerance threshold and must be reduced. |
| Selected | Medium | Risk should be reduced if cost effective to do so. If not monitoring arrangements must be established and the risk must be reviewed periodically. |
|  | Low | Risk is within acceptable tolerances and should be monitored and reviewed for changes. |

**Table:** Risk Tolerance Table