|  |
| --- |
| **Enterprise Security Risk Assessment**  Relating to the Territory and Municipal Services (TAMS) Estate |
| **Prepared by**: Agilient Pty Ltd **For**: TAMS **Date of Issue**: XXX 2015 |

|  |
| --- |
| **Agilient Pty Ltd**  Level 4, 655 Pacific Highway  ST LEONARDS NSW 2065  Australia |
| **ACN**: 157 911 441  **ABN**: 37 157 911 441 |
| **Phone**: (02) 9751 0112  **Fax**: (02) 9751 0195 |
| [konrad@agilient.com.au](mailto:konrad@agilient.com.au)  [www.agilient.com.au](http://www.agilient.com.au) |

# DISCLAIMER AND CONFIDENTIALITY

This document is based on information gathered from Territory and Municipal Services’ (TAMS) and other personnel, site visits and inspection processes, and a review of documentation provided to the assessor.

Observations and recommendations are based upon the assumption that documented and other information provided to the assessor was complete, factual, accurate and relevant in the circumstances, and that performance levels observed during visits were indicative of regular practice.

Agilient Pty Ltd, its officers, assessors, consultants and/or contractors involved or engaged in this project shall not be held liable for any direct, indirect or consequential loss or damage (whether for loss of profit, loss of business, loss of life, depletion of goodwill or otherwise), costs/expenses, or other claims for compensation whatsoever, which may arise as a result of any planning or dependence upon the results of the assessment process and this report.

The intent of this document is to provide an independent view of in-scope security risk observations and recommendations and must be reviewed by TAMS management to ensure that recommendations are suitable for the organisation.

# GLOSSARY

|  |  |
| --- | --- |
| **Acronym/Abbreviation** | **Definition** |
| XXX | XXX |
| XXX | XXX |
| ESRA | XXX |
| XXX | XXX |
| XXX | XXX |
| XXX | XXX |
| XXX | XXX |
| SRA | XXX |
| TAMS | XXX |
| XXX | XXX |

# TABLE OF CONTENTS

[DISCLAIMER AND CONFIDENTIALITY 2](#_Toc418263318)

[GLOSSARY 3](#_Toc418263319)

[TABLE OF CONTENTS 4](#_Toc418263320)

[EXECUTIVE SUMMARY 5](#_Toc418263321)

[Key Security Risk Observations and Recommendations 5](#_Toc418263322)

[Key Security Administration Observations and Recommendations 5](#_Toc418263323)

[Purpose 5](#_Toc418263324)

[Scope, Constraints and Exclusions 5](#_Toc418263325)

[METHODOLOGIES 6](#_Toc418263326)

[Consulting Methodology 6](#_Toc418263327)

[Security Risk Methodology 6](#_Toc418263328)

[ASSESSMENT CONTEXT 10](#_Toc418263329)

[External/Operational Context 10](#_Toc418263330)

[Internal/Operational Context 10](#_Toc418263331)

[Security Risk Context 11](#_Toc418263332)

[Vulnerability 15](#_Toc418263333)

[SOURCE DOCUMENTS AND REFERENCES 16](#_Toc418263334)

[ANNEX XXX: VULNERABILITY ASSESSMENT 17](#_Toc418263335)

[ANNEX XXX: SECURITY RISK REGISTER AND TREATMENT RECOMMENDATIONS 22](#_Toc418263336)

[ANNEX XXX: GENERAL ADMINISTRATIVE RECOMMENDATIONS 24](#_Toc418263337)

[ANNEX XXX: SAMPLE TREATMENT PLAN TEMPLATE 26](#_Toc418263338)

# EXECUTIVE SUMMARY

## Key Security Risk Observations and Recommendations

|  |
| --- |
| * **XXX**. XXX. |

1. XXX.

## Purpose

1. XXX.

## Scope, Constraints and Exclusions

1. XXX.

# METHODOLOGIES

## Consulting Methodology

1. The stakeholder engagement process was a critical element of the assignment, providing the opportunity to elicit contextual information for review and risk identification processes. Stakeholders consulted during visit and general review processes are listed below (in no particular order):
2. XXX, XXX | TAMS.
3. XXX, XXX | TAMS.
4. XXX, XXX | TAMS.
5. XXX, XXX | TAMS.
6. XXX, XXX | XXX.
7. In addition, TAMS and other documents examined, and site visit processes included:
8. XXX.
9. XXX.
10. XXX.
11. XXX.
12. XXX.
13. XXX.

## Security Risk Methodology

1. The recognised International Standard for assessing risks is ‘AS/NZS ISO 31000:2009 Risk management – Principles and guidelines’. Standards Australia’s ‘HB 167:2006 – Security risk management’ serves to extend on this ‘function agnostic’ methodology to account for subject matter specific factors when assessing security risks. In particular, the Handbook articulates the manner in which critical assets, security threats and levels of vulnerability should be taken into account initially and throughout the security risk management continuum, among other considerations.
2. Upon reviewing contextual arrangements, risks were identified through an iterative process of:
3. considering assets requiring protection and their level of criticality and subsequent prioritisation in the risk assessment process;
4. examining sources and levels of threat/potential harm to TAMS’ critical assets;
5. examining vulnerabilities arising from procedural and/or tangible control weaknesses;
6. reviewing open source and restricted access reports and material from ASIO, AFP and other sources and accounting for inputs in an appropriate manner;
7. observing operational settings and reviewing relevant internal documentation.

**Critical Assets**

1. The criticality assessment involved identification of critical assets that may be exposed to, or harmed by threats through reference to Criticality Criteria at Table XXX below. This process was a vital step in the identification of risks, as it provided the starting point for a consideration of pertinent threats and TAMS’ vulnerability to those threats[[1]](#footnote-1).

|  |  |
| --- | --- |
| **Criticality Rating** | **Criteria**[[2]](#footnote-2) |
| **Vital** | * Alternative services and/or facilities cannot be provided by State or Federal agencies. * Loss or compromise will result in abandonment or long-term cessation of the functions or core business practices. * Loss or compromise will have a severe impact on the economic and social well-being of the community. |
| **High** | * If services and/or facilities are disrupted, major restrictions to core business practices will result. * Service/facility will require extensive assistance from State or Federal agency resources. * Loss or compromise will have a significant impact on the economic and social well-being of the community. |
| **Significant** | * Services and/or facilities will be available, but with some restrictions to core business practices. * Reduced responsiveness and/or capacity compared to normal operations. * Maintaining a level of service may require assistance from State agencies from other jurisdictions. * Loss or compromise will result in medium term disruption of the functions or core business practices. * Minimal impact on the economic and social well-being of the community. |
| **Low** | * Normal services and/or facilities can be provided by State or Federal resources located within the region. * Loss or compromise will have very limited effect on the functions or core business practices. * Loss or compromise of functionality will have no impact on the economic and social well-being of the community. |
| **Very Low** | * Normal services and/or facilities can be provided by resources located within the region. * Loss or compromise will have no effect on the functions or core business practices. * Loss or compromise of functionality will have no impact on the economic and social well-being of the community. |

Table XXX: Criticality Criteria

**Threat Analysis**

1. A threat is generally regarded as anything that has the potential to prevent or hinder the achievement of objectives or disrupt the processes that support them. The aim of the threat analysis is to clearly identify realistic and significant threats arising from both external and internal environments. Such threats were considered with regard to capability and intent, using rating and tolerance matrices shown in Tables XXX and XXX below to assess relevance to the assessment. Threat ‘opportunity’ was also considered, but as an influencing factor in assessing vulnerability within the following stage (Vulnerability Assessment).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | **Motivation and Intent** | | |
|  |  | **Little** | **Expressed** | **Determined** |
| **Capability** | **Extensive** | Medium | High | High |
| **Moderate** | Low | Medium | High |
| **Low** | Low | Low | Medium |

Table XXX: Threat Rating Matrix

|  |  |
| --- | --- |
| **High** | Must be considered in risk assessment. |
| **Medium** | Consider including in risk assessment if threat act warrants. |
| **Low** | Monitor changes to threat level. |

Table XXX: Threat Tolerance Matrix

1. A range of threats and specific acts were considered through the course of analysis, with those ranked as ‘Medium’ included in the final risk assessment; ‘Low’ level threats were also considered for inclusion where a noted Threat Act warranted particular consideration.

**Vulnerability Assessment**

1. General vulnerabilities associated with TAMS’ locations and operations are noted within the Security Risk Context section of this report. Critical asset control vulnerabilities were identified through an assessment of current controls/methods of protection from identified threat sources using the criteria in Table XXX below.

| **Vulnerability Rating** | **Criteria** |
| --- | --- |
| **VERY HIGH** | * Security controls are non-existent. * It is almost certain that security controls will be breached or will fail. * There is recent evidence of widespread security control failures. * There are no contingencies in place; severe disruptions to operations are likely. |
| **HIGH** | * Security controls are largely ineffective. * There is an increasing probability of the security controls being breached. * There is recent evidence of significant numbers of security controls being breached. * Few contingencies are in place and significant disruptions to operations are likely. |
| **MODERATE** | * The majority of controls are functioning as intended but are not fit for purpose. * There is moderate probability of the security controls being breached. * There is recent evidence of small number of security controls being breached. * Contingencies are in place for only a few key areas of operations to manage potential disruptions. |
| **LOW** | * Security controls are effective, but small improvements could be made. * There is low probability of the security controls being breached in the future. * There are no recent examples of security controls being breached. * Contingencies are in place for key areas of operations to manage potential disruptions. |
| **VERY LOW** | * Security controls are optimum and sustainable. * There is an extremely low probability of the security controls being breached in the future. * There are no previous incidents of the security controls being breached. * Comprehensive contingencies are in place to manage most potential disruptions to operations. |

**Table XXX:** Vulnerability Assessment Criteria

1. Once identified, risks were assessed using the Risk Assessment Matrix below; risk criteria were derived from the ‘*TAMS* *Risk Management Framework’*. Assessed likelihood ratings were informed by a review of the level of individual threats and an examination of inherent vulnerability to those threats; consequence ratings were largely influenced by the assessed degree of asset criticality.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | |  | **Increasing Consequences 🡪** | | | | | |
|  | |  | XXX | XXX | XXX | XXX | XXX | XXX |
|  | |  | XXX | XXX | XXX | XXX | XXX | XXX |
|  | |  | XXX | XXX | XXX | XXX | XXX | XXX |
|  | |  | XXX | XXX | XXX | XXX | XXX | XXX |
|  | |  | XXX | XXX | XXX | XXX | XXX | XXX |
|  | XXX | XXX | XXX | XXX | XXX | XXX |
| **Increasing Likelihood 🡪** | **Qualitative Likelihood** | **Quantitative Likelihood** |  | XXX | XXX | XXX | XXX | XXX |
| XXX | XXX | XXX |  |  |  |  |  |
| XXX | XXX | XXX |  |  |  |  |  |
| XXX | XXX | XXX |  |  |  |  |  |
| XXX | XXX | XXX |  |  |  |  |  |
| XXX | XXX | XXX |  |  |  |  |  |

**Table XXX**: Risk Assessment Matrix (TAMS Aligned)

|  |  |
| --- | --- |
| **Risk Rating** | **Risk Treatment Requirements** |
| XXX | XXX |
| XXX | XXX |
| XXX | XXX |
| XXX | XXX |

**Table XXX:** Risk Tolerance Matrix (TAMS Aligned)

# ASSESSMENT CONTEXT

## External/Operational Context

1. XXX.

## Internal/Operational Context

**Business Strategies and Security Risk Objectives**

1. XXX.

**Resource Limitations**

1. XXX.

**Key Processes**

1. **Employee screening and separation processes**. XXX.
2. **Fraud management**. XXX.
3. **Guard force operations**. XXX.
4. **Enterprise risk management**. XXX.
5. **Security risk management**. XXX.
6. **Security compliance management.** XXX.
7. **Incident Response**. XXX.
8. **Security training**. XXX.
9. **Internal audit**. XXX.
10. **XXX**. XXX.

**Locations**

1. XXX.

**Security Culture and Values**

1. XXX.

## Security Risk Context

**Incident History**

1. XXX.

**Crime Statistics**

1. XXX.

**Critical Assets**

1. An assessment of significant TAMS assets appears below.

| **Asset Category** | **Details of Asset** | **Criticality** |
| --- | --- | --- |
| XXX | XXX | XXX |
| XXX | XXX | XXX |
| XXX | XXX | XXX |
| XXX | XXX | XXX |
| XXX | XXX | XXX |
| XXX | XXX | XXX |

**Table XXX:** Critical Assets

1. Despite the categorisation of critical assets as such, arrangements for other assets, such as information/data, personal items etc. were observed and considered in the preparation of this report. Identifying and drawing attention to those assets considered to be of the highest criticality is designed purely to sharpen attention and assist in maintaining a consistent focus during the review process.

**Threats**

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

|  |  |
| --- | --- |
| 1. Trusted Insiders; 2. Petty Criminals; 3. Issue Motivated Groups; | 1. Outlaw Motorcycle Gangs; 2. Organised Criminals; and 3. Terrorists. |

1. 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 an insider also being classed a petty criminal etc. Nonetheless and when risks derived from each group are considered holistically, this limitation tends to be largely mitigated.
2. A summary of assessed threats and Threat Acts appears within Table XXX at the end of this section.
3. **Trusted 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. A detailed UK study into the trusted insider threat[[3]](#footnote-3) found that there was “…clear link between an insider act taking place and exploitable weaknesses in an employer’s protective security and management processes…” Organisational-level factors that most enable an environment for trusted insider threats included:

|  |  |
| --- | --- |
| 1. Poor management practices; 2. Poor use of auditing functions; 3. Lack of protective security controls; 4. Poor security culture; 5. Lack of adequate, role-based, personnel security risk assessment; | 1. Poor pre-employment screening; 2. Poor communication between business areas; 3. Lack of awareness of people risk at a senior level; and 4. Inadequate corporate governance. 5. Poor information Management |

1. Trusted insider acts may include forms of sabotage, fraud, theft, workplace violence and manipulation of records, among other things. The trusted insider may be a dedicated, loyal worker one day, but dispositional changes can occur quickly if a real or perceived cause to feel aggrieved arises, when personal circumstances deteriorate causing financial stress and/or when the desire for motivation for personal gain outweighs obligations to ethical conduct.
2. 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.
3. [Insert comments specific to TAMS].
4. **Petty Criminals**. For the purposes of this assessment petty crime types include:

|  |  |
| --- | --- |
| 1. vandalism; 2. theft from person; 3. opportunistic assault; | 1. malicious damage; and 2. theft of retail goods. |

1. [Insert comments specific to TAMS].
2. **Issue Motivated Groups.** XXX.
3. Aside from cyber-security attacks, IMGs usually seek to present in numbers at physical, highly visible locations to draw attention to a cause.
4. [Insert comments specific to TAMS].
5. **Outlaw Motorcycle Gangs**. In some contexts, OMGs 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 TAMS, OMGs are not assessed as posing a unique threat to the organisation.
6. 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 ‘Organised Criminals’.
7. **Organised Criminals**. Despite its generic tag and clear overlap with some other threat categories, the ‘criminal’ threat is considered in the context of serious, organised crime, and for the purposes of this assessment excluding terrorism-related events. Organised criminal threats include kidnap for ransom, extortion, armed robbery, high-end burglary and other, relatively more sophisticated offences.
8. Organised crime in Australia has been estimated to cost at least $10 Billion/year and is responsible for much of the nation’s serious crime. The most successful groups operate across many sectors and crime types but are typically involved in some form of financial crime or money laundering. They will also have some connection with the illicit drugs market and may be involved in crimes such as people or firearms trafficking, kidnapping for ransom, fraud or high tech crime[[4]](#footnote-4).
9. [Insert comments specific to TAMS].
10. **Terrorists**. On the 23 Feb 15 the Prime Minister of Australia delivered a statement on the rise of the terrorism threat both at home and abroad. Core issues included the fact that the (hostile) potential of home grown terrorists is rising, an assertion that suggests that more sophisticated attacks are likely in the future. In a contrasting message, terror acts in the spirit of exhortations made by ISIL require little more than “…a camera-phone, a knife and a victim.”
11. A range of planned terrorist attacks in Australia have been disrupted in recent years, including plots to attack electricity supplies, a Grand Final at the MCG and Holsworthy Army Barracks in 2009. Two men were arrested in February 2015 in Sydney, after each had recorded a pre-attack video message in preparation for the beheading of a random person on the street of Sydney. Moreover, ASIO presently has more than 400 high-priority investigations underway into the terrorism threat - no doubt a significant portion of which have connections to geographical locations where ABS Regional offices are situated.
12. Perhaps of some concern is that the results of the investigation into the recent Martin Place Siege recently revealed that there were no major failings of intelligence or process in the lead up to the event. Risk-based consideration suggests that there are quite probably further individuals of the same disposition to the perpetrator Man Haron Honis, who was, according to investigation findings, beyond the immediate focus of ASIO, the AFP and NSWPOL.
13. It is informative to note these matters and more broadly the evolution of the terror threat to Australia over the past decade. In 2004 Jemaah Islamiyah was identified as presenting the greatest terrorist threat to Australia through its interest in attacking ‘soft targets’, such as the ABS. Other reports suggest that Al Qaeda, through its globally decentralised network of terror cells, was the greater risk to Australian interests. This was highlighted when an image of the Sydney Opera House appeared on the front cover of the organisation’s ‘Inspire’ magazine. Since then ISIL has emerged as an inspiration for the Martin Place siege, a knife attack on two VICPOL detectives and various other defeated attempts to commit terrorism within the Australian community.
14. ISIL is considered somewhat more pervasive in regards to its ability to draw in potential recruits through its savvy use of online social platforms and indeed through demonstrative military successes in Syria and Iraq. It also maintains awareness of its horrific deeds through a coordinated and continuous media campaign, in much the same way that any organisation seeks to market itself to attract the support of its audience.
15. Moreover, it is evident that Australian jihadist recruits have returned or are likely to return home from fighting in war zones in the Middle East, in support of ISIL and others. Much like returning Australian military service personnel, individuals will, in some cases, suffer a form of post-traumatic stress, or worse a solid belief that they are returning to bring the war to Australian soil. It is noteworthy that, at the time of writing this report, several Australian participants in Middle Easter conflicts were seeking to negotiate with the Government to return to Australia. Regardless of the cause, capable and experienced jihadists will likely live among our community, or indeed already do; this is a problem that will inevitably escalate as conflict in the Middle East continues and more fighters return to the country.
16. The modus operandi of the various current terrorist threats to Australia could vary significantly. Vehicle or person borne improvised explosive devices, 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.
17. The likelihood of these types of events occurring falls largely to both the ability of Australian intelligence community to disrupt planned attacks, and indeed the measure of capability, motivation and intent of would be attackers.
18. As such and at least for the short term, it is more probable that lower levels of capability will restrain terrorists to more simplistic attacks, such as the Lindt Café and the alleged attack planned for ANZAC Day 2015[[5]](#footnote-5).
19. [Insert comments specific to TAMS and potential attraction to attacking the organisation or whether it is more likely to be a victim by happenstance, if at all].

| **Threat Sources** | **Threat Acts** | **Critical Assets at Risk and Rating** | **Threat Rating** |
| --- | --- | --- | --- |
| **Trusted Insiders** Persons with privileged access to critical assets e.g. employees and some contractors | Financial or other forms of fraud | XXX (XXX) | XXX |
| Theft of personal or Organisational assets | XXX (XXX) | XXX |
| Workplace violence, intimidation or bullying | XXX (XXX) | XXX |
| Tampering with/leaking of sensitive information | XXX (XXX) | XXX |
| Sabotage of critical equipment | XXX (XXX) | XXX |
| **Petty Criminals**  Criminals who perpetrate opportunistic criminal acts. | Graffiti vandalism | XXX (XXX) | XXX |
| Theft from person | XXX (XXX) | XXX |
| Opportunistic assault on person | XXX (XXX) | XXX |
| Malicious damage to property | XXX (XXX) | XXX |
| Theft of retail goods | XXX (XXX) | XXX |
| **Issue Motivated Groups** Protestors who take violent or non-violent action to bring attention to a particular cause. | Non-violent protest blocking access to a building | XXX (XXX) | XXX |
| Violent protest blocking access, injuring people | XXX (XXX) | XXX |
| Cyber security attack on ICT systems | XXX (XXX) | XXX |
| Hate crime assault on person(s) | XXX (XXX) | XXX |
| **Organised Criminals**  Criminals who plan, coordinate and conduct crime on a continuing basis. | Break, enter and steal | XXX (XXX) | XXX |
| Cyber security attack on ICT systems | XXX (XXX) | XXX |
| Armed robbery | XXX (XXX) | XXX |
| Major fraud (including arson) | XXX (XXX) | XXX |
| Large scale drug offences | XXX (XXX) | XXX |
| **Terrorists**  Criminals who act or threaten to act in a manner intended to advance a political, ideological or religious cause by coercing or intimidating an Australian or foreign government or the public. | Vehicle born improvised explosive device | XXX (XXX) | XXX |
| Person born improvised explosive device | XXX (XXX) | XXX |
| Armed attack using firearm | XXX (XXX) | XXX |
| Armed attack using sharp edged weapon | XXX (XXX) | XXX |
| Sabotage/arson | XXX (XXX) | XXX |
| Chemical, biological or radiological attack | XXX (XXX) | XXX |
| Parcel or letter bomb | XXX (XXX) | XXX |
| Hostage taking and/or siege | XXX (XXX) | XXX |
| Food/drink contamination | XXX (XXX) | XXX |

Table XXX: Threat Sources, Acts and Ratings

## Vulnerability

1. An assessment of security control vulnerabilities common across the organisation appears at Annex XXX.

# SOURCE DOCUMENTS AND REFERENCES

1. XXX.
2. HB 167:2006 – Security risk management.
3. ISO AS/NZS 31000:2009 – Risk management principles and guidelines.
4. [Privacy Act 1988](http://www.comlaw.gov.au/Series/C2004A03712) and [Privacy Amendment (Enhancing Privacy Protection) Act 2012](http://www.comlaw.gov.au/Series/C2012A00197).
5. ACT Protective Security Policy Framework.
6. XXX.

# ANNEX XXX: ENTERPRISE VULNERABILITY ASSESSMENT

| **Security Controls** | | **Strengths** | | **Weaknesses** | **Vulnerability Rating** |
| --- | --- | --- | --- | --- | --- |
|  | **Security Governance** | | | | |
| Management support. | | | * XXX. |  |  |
| Security policies & procedures. | | | * XXX. |  |  |
| Security risk assessments & threat assessments. | | | * XXX. |  |  |
| Review of previous incidents & risk assessments. | | | * XXX. |  |  |
| Inventory control systems. | | | * XXX. |  |  |
| Housekeeping. | | | * XXX. |  |  |
| Evacuation arrangements. | | | * XXX. |  |  |
| Emergency planning arrangements. | | | * XXX. |  |  |
| Incident planning arrangements. | | | * XXX. |  |  |
| Business continuity arrangements. | | | * XXX. |  |  |
| Interaction with Emergency Services. | | | * XXX. |  |  |
| Organisational culture & management support for security. | | | * XXX. |  |  |
| Clear roles & responsibilities. | | | * XXX. |  |  |
| Reporting arrangements. | | | * XXX. |  |  |
| Communicating with staff & stakeholders. | | | * XXX. |  |  |
| Disciplinary arrangements. | | | * XXX. |  |  |
| Testing & audit arrangements. | | | * XXX. |  |  |
| Bomb threat procedures. | | | * XXX. |  |  |
|  | **Physical Security** | | | | |
| Lock-key practices. | | | * XXX. |  |  |
| Physical access controls & reviews. | | | * XXX. | XXX. |  |
| Mail screening. | | | * XXX. | XXX. |  |
| Security signage. | | | * XXX. | XXX. |  |
| Perimeter security (buildings & area). | | | * XXX. | XXX. |  |
| Security guard force (including covert security & static & mobile patrols). | | | * XXX. | XXX. |  |
| Local traffic proximity. | | | * XXX. | XXX. |  |
| Crime Prevention Through Environmental Design (CPTED) | | | * XXX. | XXX. |  |
| Security lighting. | | | * XXX. | XXX. |  |
| Entry, egress & building/area design. | | | * XXX. | XXX. |  |
| Vehicle controls points. | | | * XXX. | XXX. |  |
| Buffer & designated security zones. | | | * XXX. | XXX. |  |
| Search & detain arrangements. | | | * XXX. |  |  |
| Car parking. | | | * XXX. |  |  |
| Front of house arrangements. | | | * XXX. |  |  |
| Asset management, maintenance & repair. | | | * XXX. |  |  |
| Proximity to attractive targets/organisations/ buildings. | | | * XXX. |  |  |
| Personnel screening. | | | * XXX. |  |  |
| CCTV & monitoring. | | | * XXX. |  |  |
|  | **Personnel Security** | | | | |
| Pre-employment/ contracting vetting/ checking. | | | * XXX. |  |  |
| Training and awareness arrangements. | | | * XXX. |  |  |
| Employment termination procedures. | | | * XXX. |  |  |
| Whistle-blower procedures. | | | * XXX. |  |  |
| Identification arrangements. | | | * XXX. |  |  |
| Visitor and contractor arrangements. | | | * XXX. |  |  |
| Public access to venues/ areas. | | | * XXX. |  |  |
| Challenging strangers in security controlled areas. | | | * XXX. |  |  |
| Travel security. | | | * XXX. |  |  |
| Intruder/trespasser procedures. | | | * XXX. |  |  |
|  | **Information Security** | | | | |
| XXX | | |  |  |  |
| XXX | | |  |  |  |
| XXX | | |  |  |  |
| XXX | | |  |  |  |
| XXX | | |  |  |  |
| XXX | | |  |  |  |

# ANNEX XXX: ENTERPRISE SECURITY RISK REGISTER

| **ID** | **Threats and Ratings** | **Critical Assets and Ratings** | **Area(s) of Vulnerability** | **Assessed Risks** | **Inherent Risk** | **Recommended Treatments** | **Residual Risk** | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Rating | Likelihood | Consequence | Rating |
|  | Terrorist  (HIGH) | Personnel +  (VITAL) | Intelligence | Lorem ipsum dolor sit amet, ligula suspendisse nulla pretium, rhoncus tempor fermentum, enim integer ad vestibulum volutpat. Nisl rhoncus turpis est, vel elit, congue wisi enim nunc ultricies sit, magna tincidunt. | Likelihood: Low  Consequence: Low  **Rating: Low** | * XXX. | XXX | XXX | XXX |
| Mail Screening |
| Security Signage |
| Perimeter |
| + Add More |
|  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  | * XXX. |  |  |  |

# ANNEX XXX: XXX SECURITY RISK REGISTER

| **ID** | **Threats and Ratings** | **Critical Assets and Ratings** | **Area(s) of Vulnerability** | **Assessed Risks** | **Inherent Risk** | | | **Recommended Treatments** | **Residual Risk** | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Likelihood | Consequence | Rating | Likelihood | Consequence | Rating |
|  | Terrorist  (HIGH) | Multiple  (VITAL) | Intelligence | XXX | XXX | XXX | XXX | * XXX. | XXX | XXX | XXX |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |

# ANNEX XXX: XXX SECURITY RISK REGISTER

| **ID** | **Threats and Ratings** | **Critical Assets and Ratings** | **Area(s) of Vulnerability** | **Assessed Risks** | **Inherent Risk** | | | **Recommended Treatments** | **Residual Risk** | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Likelihood | Consequence | Rating | Likelihood | Consequence | Rating |
|  | Terrorist  (HIGH) | Multiple  (VITAL) | Intelligence | XXX | XXX | XXX | XXX | * XXX. | XXX | XXX | XXX |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |

# ANNEX XXX: XXX SECURITY RISK REGISTER

| **ID** | **Threats and Ratings** | **Critical Assets and Ratings** | **Area(s) of Vulnerability** | **Assessed Risks** | **Inherent Risk** | | | **Recommended Treatments** | **Residual Risk** | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Likelihood | Consequence | Rating | Likelihood | Consequence | Rating |
|  | Terrorist  (HIGH) | Multiple  (VITAL) | Intelligence | XXX | XXX | XXX | XXX | * XXX. | XXX | XXX | XXX |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |

# ANNEX XXX: XXX SECURITY RISK REGISTER

| **ID** | **Threats and Ratings** | **Critical Assets and Ratings** | **Area(s) of Vulnerability** | **Assessed Risks** | **Inherent Risk** | | | **Recommended Treatments** | **Residual Risk** | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Likelihood | Consequence | Rating | Likelihood | Consequence | Rating |
|  | Terrorist  (HIGH) | Multiple  (VITAL) | Intelligence | XXX | XXX | XXX | XXX | * XXX. | XXX | XXX | XXX |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |

# ANNEX XXX: XXX SECURITY RISK REGISTER

| **ID** | **Threats and Ratings** | **Critical Assets and Ratings** | **Area(s) of Vulnerability** | **Assessed Risks** | **Inherent Risk** | | | **Recommended Treatments** | **Residual Risk** | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Likelihood | Consequence | Rating | Likelihood | Consequence | Rating |
|  | Terrorist  (HIGH) | Multiple  (VITAL) | Intelligence | XXX | XXX | XXX | XXX | * XXX. | XXX | XXX | XXX |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |

# ANNEX XXX: XXX SECURITY RISK REGISTER

| **ID** | **Threats and Ratings** | **Critical Assets and Ratings** | **Area(s) of Vulnerability** | **Assessed Risks** | **Inherent Risk** | | | **Recommended Treatments** | **Residual Risk** | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Likelihood | Consequence | Rating | Likelihood | Consequence | Rating |
|  | Terrorist  (HIGH) | Multiple  (VITAL) | Intelligence | XXX | XXX | XXX | XXX | * XXX. | XXX | XXX | XXX |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |

# ANNEX XXX: XXX SECURITY RISK REGISTER

| **ID** | **Threats and Ratings** | **Critical Assets and Ratings** | **Area(s) of Vulnerability** | **Assessed Risks** | **Inherent Risk** | | | **Recommended Treatments** | **Residual Risk** | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Likelihood | Consequence | Rating | Likelihood | Consequence | Rating |
|  | Terrorist  (HIGH) | Multiple  (VITAL) | Intelligence | XXX | XXX | XXX | XXX | * XXX. | XXX | XXX | XXX |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |

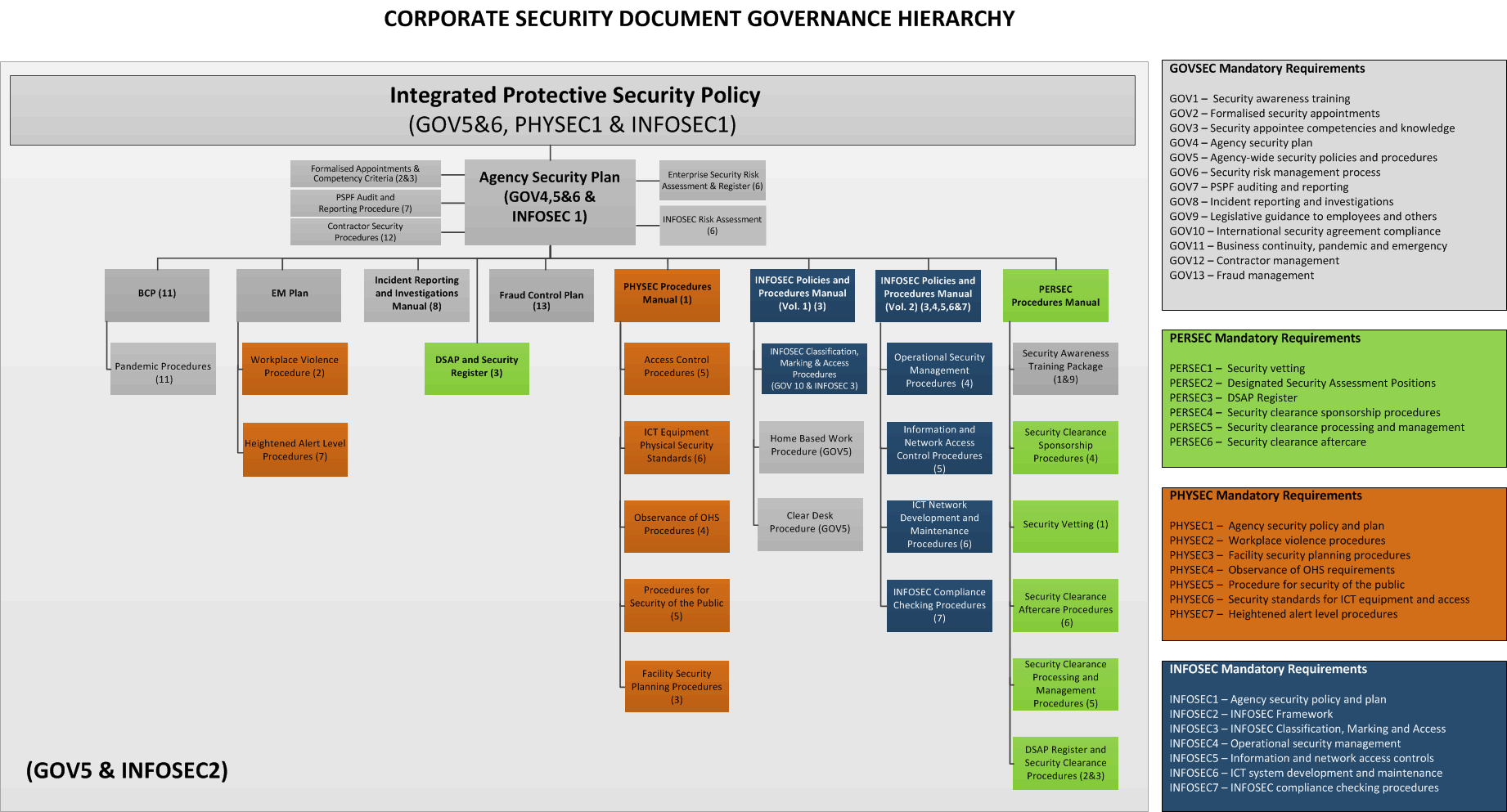
# ANNEX XXX: XXX SECURITY RISK REGISTER

| **ID** | **Threats and Ratings** | **Critical Assets and Ratings** | **Area(s) of Vulnerability** | **Assessed Risks** | **Inherent Risk** | | | **Recommended Treatments** | **Residual Risk** | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Likelihood | Consequence | Rating | Likelihood | Consequence | Rating |
|  | Terrorist  (HIGH) | Multiple  (VITAL) | Intelligence | XXX | XXX | XXX | XXX | * XXX. | XXX | XXX | XXX |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |
|  |  |  |  |  |  |  |  | * XXX. |  |  |  |

# ANNEX XXX: ENTERPRISE GOVERNANCE RECOMMENDATIONS

1. The following general enterprise recommendations are provided in the context of continual improvement and it is usually of tenuous value to present these in the context of security risks, rather than as issues of governance:
2. Consider developing an illustrated corporate document hierarchy (an example appears at page at -XXX2-) to clearly articulate the internal documentary governance environment, making it easier to understand and thus comply with embedded requirements[[6]](#footnote-6). This will also serve to assist in clearly demonstrating compliance with ACT PSPF GOVSEC-5, and highlight areas of redundancy that currently exist.
3. XXX.

-**XXX2**-

****

# ANNEX XXX: SAMPLE TREATMENT PLAN TEMPLATE

| **ID** | **Risk(s) Addressed** | **Accepted Treatment Actions** | **Intended Effect of Treatment on Threat Vector** | **Resource Requirements** | **Responsibilities** | **Due Date** | **Reporting and Monitoring Requirements** | **Key Performance Indicators** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |





Level 4, 655 Pacific Highway  
ST LEONARDS NSW 2065

**Phone**: 02 9751 0112

**Fax**: 02 9751 0195

enquiries@agilient.com.au

www.agilient.com.au

1. For the purposes of this assessment, only those assets categorised as ‘Significant’ and higher were considered in risk identification and analysis processes, unless an associated threat was assessed as ‘High’. [↑](#footnote-ref-1)
2. **Short-term:** Pertaining to the near or immediate future; usually less than 1 year. **Medium term:** Usually between 1 and 3 years. **Long-term:** Extending over a relatively long time period; usually more than 3 years. [↑](#footnote-ref-2)
3. http://www.cpni.gov.uk/Documents/Publications/2013/2013003-insider\_data\_collection\_study.pdf [↑](#footnote-ref-3)
4. http://www.aic.gov.au/crime\_types/transnational/networks.html [↑](#footnote-ref-4)
5. http://www.theaustralian.com.au/news/nation/two-held-after-terror-raids-allegedly-linked-to-anzac-day/story-e6frg6nf-1227310072957. [↑](#footnote-ref-5)
6. Note: This is a dated model of the Commonwealth PSPF based on the previous regime of 33 Mandatory Requirements and is shown for demonstrative purposes only. [↑](#footnote-ref-6)