Security Risk Assessment & Risk Treatment Plan

| **Project Details** | | | |
| --- | --- | --- | --- |
| **Project ID** |  | | |
| **Project Name** |  | | |
| **Prepared by** |  | **Version** |  |

Contents

[2 Scope & Context 2](#_Toc12977988)

[3 Initial Risk Assessment 2](#_Toc12977989)

[4 Identified Security Risks and Recommended Controls 3](#_Toc12977990)

[5 Risk Analysis and Recommended Controls 4](#_Toc12977991)

[6 Risk Treatment Plan and Residual Risk Assessment 5](#_Toc12977992)

[Appendix – Risk Matrix 6](#_Toc12977993)

[7 Approvals 8](#_Toc12977994)

[8 Document Administration 9](#_Toc12977995)

[8.1 Document Location 9](#_Toc12977996)

[8.2 Document References 9](#_Toc12977997)

[8.3 Amendment History 9](#_Toc12977998)

# Scope & Context

Agency risk assessments are based upon the *AS/NZS ISO 31000:2009, ISO 27005:2011 Risk Management - Principles and Guidelines,* and *Standards Australia HB 231:2004. Information security risk management guidelines.*

[Refer to the *Security Risk Management* guide in the Agency *Information Security Standards and Guidelines* for information on completing the assessment. For a high level assessment, not all detail may be required.]

[Briefly describe the context:

* What functionality is to be provided or supported;
* Who will be using the functionality;
* Any external service provider(s) involved;
* Any current technology providing the functionality;
* Any proposed changes;
* The reason / or request prompting the risk assessment.]

[Summarise the information used or processed and its sensitivity, as well as any current controls.

Briefly summarise any noted risks and their severity]

[REMOVE this guidance information.]

# Initial Risk Assessment

The following relevant security risks were identified in the initial risk assessment;

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Risk Level** | **Risk Rating** | **Action Required** | **Adequate Controls required to be in place** | **Number of Identified Security Risks** |
| 1 – 5 | Low | Risk impact is minimised through routine procedures. | Standard security controls are sufficient. |  |
| 6 – 9 | Medium | Risk impact is minimised through a combination of management attention and defined response procedures. | Risk specific security controls must be maintained and regularly reviewed. |  |
| 10 – 20 | High | Senior management attention needed to minimise potential impact. | Targeted specialist security controls must be applied and sustained for lengthy periods. |  |
| 20 - 30 | Extreme | An immediate response is required to minimise impact | Security controls cannot not be sustained in the long term. |  |
| Total | | | |  |

[Firstly complete the identified risks and recommended controls on the following page before completing this table.]

# Identified Security Risks and Recommended Controls

The following table shows the risk ratings for the identified security risks based on existing documented controls, together with additional recommended controls to reduce any potentially unacceptable risks.

[Remove or add rows as required.]

| **ID** | **Risk** | **Cause(s) and Impact(s)** | **Recommended Controls** | **Residual Risk Assessment** | | | **Area Impacted** | **Date** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Likelihood** | **Business Impact** | **Rating** |
| R1 |  |  |  | 2-Unlikely | 2-Minor | 1-5 Low |  |  |
| R2 |  |  |  | 2-Unlikely | 1-Insignificant | 1-5 Low |  |  |
| R3 |  |  |  | 3-Moderate | 3-Moderate | 6-9 Medium |  |  |
| R4 |  |  |  | 4-Likely | 2-Minor | 6-9 Medium |  |  |
| R5 |  |  |  | 4-Likely | 3-Moderate | 10-14 High |  |  |
| R6 |  |  |  | 3-Moderate | 4-Major | 10-14 High |  |  |

# Risk Analysis and Recommended Controls

[Explain how the identified risks were determined and priorities risk treatments and recommended controls]

# Risk Treatment Plan and Residual Risk Assessment

The risk treatment plan recommends additional controls or improvements to existing controls to reduce the risk to acceptable levels.

| **ID** | **Risk** | **Initial Risk Rating** | **Recommended Controls** | **Residual Risk Assessment** | | | **Area Impacted** | **Date** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Likelihood** | **Business Impact** | **Rating** |
| R3 | [Repeat risks rated above LOW from section 4.  Repeat the initial risk rating in the next column] | **MEDIUM** | [Repeat the recommended controls]  [Show the residual risk assessment in the following columns] | 2-Unlikely | 2-Minor | 1-5 Low |  |  |

# Appendix – Risk Matrix

The first table presents guidance on assessing the impact or consequences of a realised threat against WA Police operations.

| **Business Impact** | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Level** | **Rating** | **A**  **Injuries** | **B**  **Financial** | **C**  **Unauthorised Disclosure of Sensitive or Personal Information[[1]](#footnote-1)** | **D**  **Interruption to Services** | **E**  **Reputation Image** | **F**  **Operational Efficiency** | **G**  **Breach of Procedure/ Order/ Law** |
| 1 | Insignificant | Nil | Loss of less than $50,000 | The information is in the public record | < 1 hour | Little or no loss of confidence in the agency | Little or no damage to WA Police operations | Managerial Intervention Model |
| 2 | Minor | Injuries that are not serious or life threatening | loss of $50,000 to $250,000 | Identity theft or threat to personal safety of individuals is unlikely;  No impact on ongoing investigations | 1 hour – 1 day | Substantiated, low impact | Inconvenient delays | Substandard Performance Management |
| 3 | Moderate | Medical treatment required | Loss of $250,000 to $3 million | A Notifiable Data Breach (NDB)[[2]](#footnote-2);  Possible identity theft, threat to personal safety;  Compromised investigations | 1 day – 1 week | Substantiated, public embarrassment, moderate impact | Delays in major deliverables | Disciplinary charge |
| 4 | Major | Extensive injuries, could lead to loss of life | Loss of $3m to $10m | Long-term impairment to investigate serious organised crime | 1 week – 1 month | Substantiated, public embarrassment, high impact & high news profile, 3rd party actions | Non-achievement of major deliverables | Statutory charge |
| 5 | Catastrophic | Multiple deaths & casualties | Loss greater than $10 million | Grave damage to extremely valuable security or intelligence operations | > 1 month | Exceptionally grave damage to community relations | Non-achievement of major key objectives | Dismissal, Commissioner’s loss of confidence |

The table below may be used to calculate the likelihood of a threat event occurring:

| **Likelihood/Probability** | | | | |
| --- | --- | --- | --- | --- |
| **Level** | **Rating** | **Operational Likelihood** | | **% Chance** |
| 1 | Rare | * Event may occur in exceptional circumstances | * Less than once in five years | ≤5% |
| 2 | Unlikely | * Event could occur at some time | * At least once in three years | 6-30% |
| 3 | Moderate | * Event should occur at some time | * At least once a year | 31-60% |
| 4 | Likely | * Event will probably occur in most circumstances | * At least once in six months | 61-90% |
| 5 | Almost Certain | * Event is expected to occur in most circumstances | * More than once in quarter | ≥91% |

| **Risk Analysis Matrix** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Business Impact** | | **Likelihood** | | | | |
| **1** | **2** | **3** | **4** | **5** |
| **Rare** | **Unlikely** | **Moderate** | **Likely** | **Almost Certain** |
| **1** | **Minor** |  |  |  |  |  |
| **2** | **Moderate** |  |  |  |  |  |
| **3** | **Major** |  |  |  |  |  |
| **4** | **Extreme** |  |  |  |  |  |
| **5** | **Catastrophic** |  |  |  |  |  |

Risk is calculated on the basis of (Likelihood) X (Business Impact). See the tables below:

|  |  |
| --- | --- |
| Risk Rating | Legend |
| Low | 1-5 |
| Medium | 6-9 |
| High | 10-14 |
| Extreme | 15-25 |

# Approvals

This document requires the following review, endorsement and approval process.

| **Position** | **Name** | **Sign off Type** | **Version Reviewed** | **Sign off Method** | **Sign off Date** |
| --- | --- | --- | --- | --- | --- |
| <Document Creator> |  | Review |  | Email |  |
| <Line Manager> |  | Review |  | Email |  |
| Chief Information Security Officer |  | Endorse |  | Email |  |
| Senior Responsible Officer (SRO) |  | Approve |  | Email |  |

*Rows assigned for endorsement are not to be removed.*

| **Approval Outcome** |
| --- |
| Approval of this document constitutes acceptance that   * The assessment has correctly identified the relevant security risks and recommended reasonable controls. * Recommendations are approved for project implementation/action.   Note: Additional project costs/schedule impacts are to be managed by the project Request for Change process |

# Document Administration

## Document Location

| **Location of approved document.** |
| --- |
|  |

## Document References

The following documents have been referred to in the development of this document:

| **Document Name** | **Version** | **Description** |
| --- | --- | --- |
| Security Risk Management | 1.0 | WA Police Information Security Standards & Guidelines |
| Security planning and risk management - PSPF | 2018.1 | Protective Security Policy Framework issued by Australian Government Attorney-General’s Department |
|  |  |  |

## Amendment History

This document has the following amendment history:

| **Date** | **Version** | **Author** | **Nature of Amendment** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1. See the Western Australia Police Force Privacy Statement: <https://www.police.wa.gov.au/Privacy> [↑](#footnote-ref-1)
2. Under the Notifiable Data Breaches(NDB) scheme of Part IIIC of the *Privacy Act 1988.* <https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme>

   The NDB scheme does not apply to the WA Police, but the reporting criteria are relevant to assessing risk – unauthorised disclosure likely to cause harm that cannot be prevented by remedial action: <https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/identifying-eligible-data-breaches> [↑](#footnote-ref-2)