

Security Sensitive Biological Agents Regulatory Scheme

Security Risk Assessment and Risk Management Plan

In confidence once completed

September 2022

Entity name: Enter the name of the entity

Facility name: Enter the name of the facility

Approvals

Prepared by: Enter name

Date: Click or tap to enter a date.

Accepted by: Enter name
 Enter position

Date: Click or tap to enter a date.

Accepted by: Enter name
 Enter position

Date: Click or tap to enter a date.

Review

Version	Date revised	Section revised	Revision by
Enter version number	Click or tap to enter a date.	Enter details of the section revised	Enter the name of the person who revised

Contents

- Introduction4
- 1. Context.....7
 - 1.1 Internal context.....7
 - 1.1.1 Structure7
 - 1.1.2 Resources.....7
 - 1.1.3 Future change.....8
 - 1.1.4 Constraints.....8
 - 1.1.5 Assumptions.....8
 - 1.2 External context8
 - 1.3 Security risk context8
 - 1.3.1 Culture8
 - 1.3.2 Type of SSBAs.....9
 - 1.3.3 Legislation.....9
 - 1.3.4 Facilities9
- 2 Stakeholder communication and consultation.....10
 - 2.1 Objectives10
 - 2.2 Internal and external stakeholders.....10
 - Internal stakeholders10
 - External stakeholders.....10
- 3. Identifying and analysing risk.....11
 - 3.1 Assets11
 - 3.2 Identification of risk.....11
 - 3.3 Analysis of risk12
 - 3.4 Risk acceptance level.....12
 - Example13

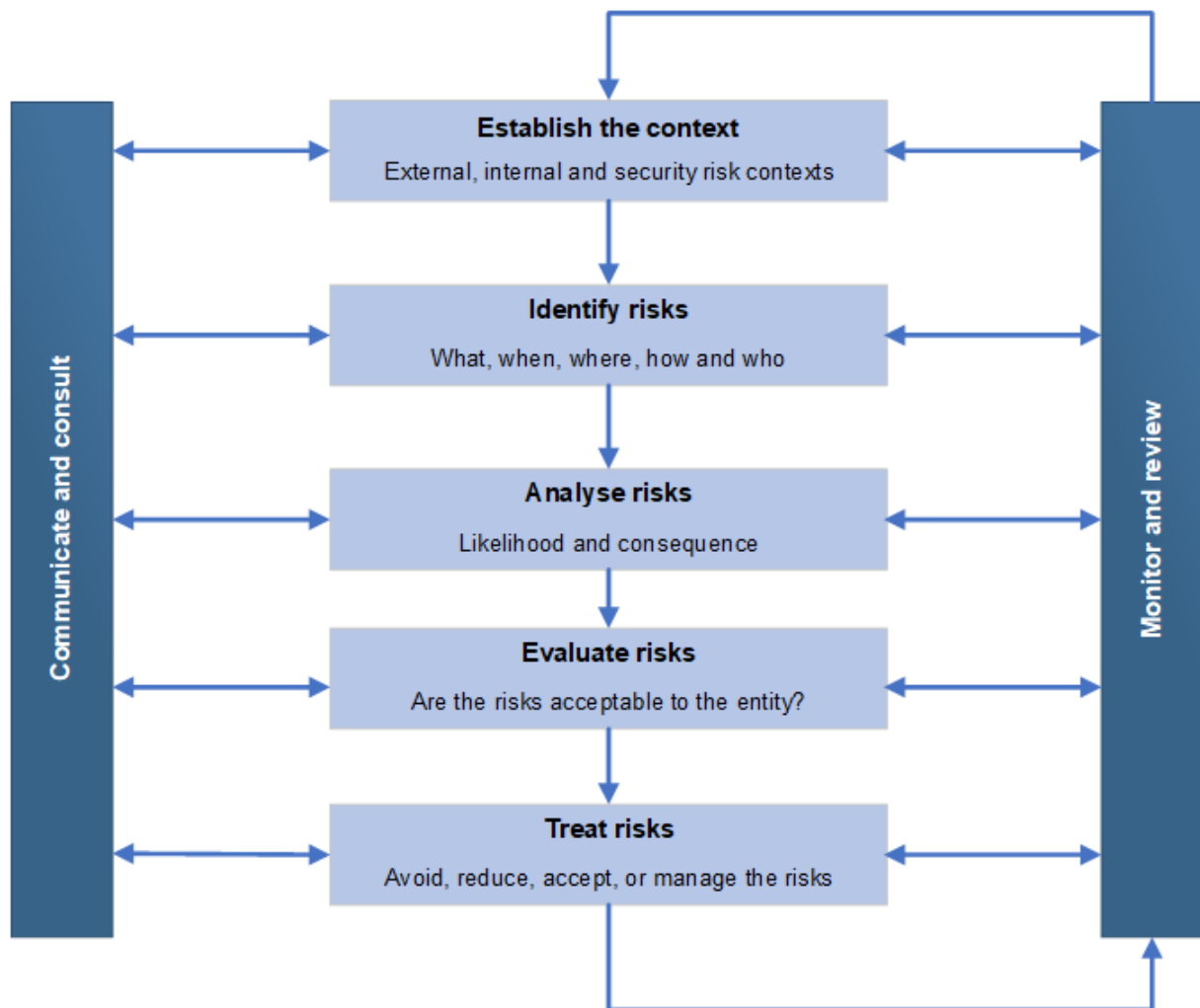
3.5	Risk assessment table.....	14
3.6	Risk treatment action plan	15
3.7	Vulnerability analysis.....	16
4	Budget.....	16
5	Monitoring	17
6	Review	18
	Attachment A – Sample risk matrix tables	19
	Risk consequence rating table	19
	Effectiveness of controls	20
	Risk likelihood table	21
	Risk Consequence Table	21
	Risk analysis matrix	22
	Acceptability table	22

Introduction

Security risk assessments provide an approach to support the identification, assessment and management of security risks relating to the physical environment, personnel, sensitive information and incident management. Security risk assessments also provide opportunities for education and awareness raising amongst personnel.

Under Part 2 of the Security Sensitive Biological Agent (SSBA) Standards, entities handling SSBA are required to undertake a risk assessment and develop a risk management plan. The security risk assessment process assists entities to identify, understand, communicate and mitigate security related risks and threats. Risk analysis plans are critical for managing the security requirements in the SSBA Standards.

The following diagram depicts the risk assessment and risk management process.



Process

A risk is the chance of something happening that has an impact on the objective, in this case the **biosecurity** of the SSBA. Security risks may be identified by looking at potential sources of risk and when, where, why and how the risks may occur. Risks may be determined through consultation with stakeholders, persons or organisations with previous experience in handling SSBA information or from security experts. It should be noted that while external advice may assist during the risk assessment and risk management process, the entity should balance the need for this advice against the need to keep the details of SSBA information restricted to those who have a need to know.

Once the security risks are identified, they should be analysed by determining the likely consequences of the risk occurring, the likelihood of that event and determining what controls or mitigation strategies are already in place. From this, the initial level of risk can be determined and the entity can then decide if:

- the risks are controlled at a level where no further management is required; or
- additional controls need to be developed to reduce the risk.

In treating risks, the options for further control of the risk need to be identified and assessed. From this, treatment and implementation plans are prepared. The risk is analysed and assessed with these new treatment options in place, and a decision made on if the risk is:

- now controlled by the elimination or minimisation of the risk to acceptable levels; or
- not controlled and it is therefore not secure to proceed.

Review of the Risk Assessment and Risk Management Plan

Under the SSBA Standards, a review of the Risk Assessment and Risk Management Plan must be undertaken at least annually for facilities handling Tier 1 SSBA information and every two years for facilities handling Tier 2 SSBA information. A section has been provided in this template for determination of when a review will take place and what may trigger a review outside the timeframes mentioned above.

Purpose

This template is designed to assist entities in identifying potential security risks and development of appropriate mitigation strategies. It has been aligned with the requirements of the SSBA Standards.

Completing this document

The document is broken down into a number of sections with each section including instructional text on what information may be required (this text can be deleted upon completion of each section). The section on risk assessment and risk management includes a number of risk tables that should assist in identifying the risk, the source of the risk, the consequences and controls, and will help to determine the risk rating. Other tables deal with the risk mitigation strategies and look at the current risk ratings, the identified target risk ratings and the strategies that can help achieve this. A number of risk matrix tables have also been included in this document to assist in determining risk levels.

The risk assessment and risk management plans do not need to be long and complex documents. It is acceptable to use dot points and tables if these get the message across in a clearer and more concise form.

This template is only a tool and its use is not compulsory. Entities may use another risk assessment and risk management template if desired.

Sensitive information considerations

The risk assessment and risk management plan, once completed, is considered to be sensitive information under the SSBA Regulatory Scheme and is subject to the requirements of Part 5 of the SSBA Standards, including a requirement for entities to restrict access to sensitive information to those who have a need to know.

1. Context

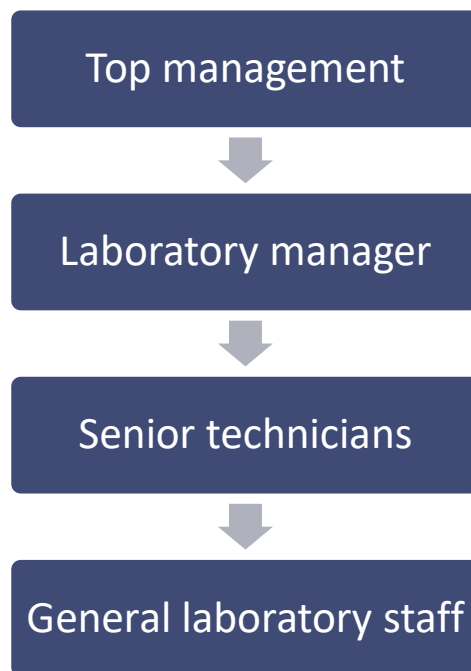
1.1 Internal context

This section should document the key aspects of the business, including defining the governance structure of the entity, resourcing issues, any upcoming significant changes (for example new facilities) and the assumptions and constraints that the entity works under (in relation to SSBAs).

1.1.1 Structure

What is the internal structure of the entity for the purposes of this assessment?

For example:



The risk assessment and risk management plan should identify who is defined as Top Management (see clause 8.3.1 of the SSBA Standards) as well as any other positions where necessary. It is recommended that you use position titles in the document rather than individual names.

1.1.2 Resources

What resources are available to undertake security risk management? Resources may include staff, budget, knowledge and the working environment.

1.1.3 Future change

What changes are expected in the short, medium or long term that may affect the security risk environment? For example, new facilities, new management, mergers with other organisations or changes to legislation.

1.1.4 Constraints

What are the constraints on the security risk process?

For example:

- Legislation or regulation that governs the handling of SSBA
- Specific requirements for handling (such as the SSBA Standards, local transport requirements, AQIS requirements, etc)
- Internal constraints such as specific policies or procedures
- Financial issues

1.1.5 Assumptions

What assumptions can be made about the security risk process?

For example:

- Biosafety requirements for handling SSBA are covered under other standards and regulatory schemes

1.2 External context

The external context for the purposes of the risk assessment includes the consideration of the external environment in which the entity operates, such as the general regulatory environment, and understanding the relationship between the environment, external stakeholders and the entity.

1.3 Security risk context

The security risk context relates to defining what influences the security environment in the entity. This may include the security culture present in the entity, type of SSBA held, legislation that governs handling of SSBA (i.e. the NHS Act, NHS Regulations and SSBA Standards) and the type and location of the facilities handling the SSBA.

1.3.1 Culture

What is the current security culture of the entity?

1.3.2 Type of SSBAs

The entity does not have to list the specific SSBAs held but should indicate if Tier 1 SSBAs, Tier 2 SSBAs or both are handled.

1.3.3 Legislation

In addition to the legislation governing SSBAs under the NHS Act, is there any other legislation that may affect the security of the SSBAs (for example transport regulations and dangerous goods codes)?

1.3.4 Facilities

How many facilities are covered by this assessment? Where are they located? Are they located in a private building or a multi-tenancy building?

2 Stakeholder communication and consultation

2.1 Objectives

What are the objectives of the communication?

2.2 Internal and external stakeholders

Stakeholders are defined as those who may affect or be affected by the risk process.

The internal stakeholders are those who have a direct impact on, or are directly affected by, the scheme – for example facility staff and management, contractors, clients or the SSBA Regulatory Scheme.

Internal stakeholders

Internal stakeholders	Information to be communicated	Communication methods	Timeframes
Enter stakeholder name	Enter information to be communicated	Enter communication methods	Enter timeframes
Enter stakeholder name	Enter information to be communicated	Enter communication methods	Enter timeframes

External stakeholders

External stakeholders	Information to be communicated	Communication methods	Timeframes
Enter stakeholder name	Enter information to be communicated	Enter communication methods	Enter timeframes
Enter stakeholder name	Enter information to be communicated	Enter communication methods	Enter timeframes

3. Identifying and analysing risk

3.1 Assets

What are the assets of the entity? An asset for the purposes of this assessment is something that the entity values and is important to the handling of the SSBAs. Assets may include such things as the facility and corporate infrastructure, knowledge, staff, equipment etc.

3.2 Identification of risk

The identification of risks is a critical step in the risk management process. The SSBA Standards define risk as ‘the chance of something happening that will have an impact on objectives’. The SSBA Standards¹ identifies the minimum risks to be assessed as including the following:

- determination of the potential for, and possible causes of, an incident, including those listed as reportable events
- human behavioural risks
- periods of reduced staff availability (for example, during weekends and holiday periods)
- identifying potential emergency situations involving SSBAs to:
 - prepare for their occurrence and to limit possible illness or other damage that may be associated with them;
 - ensure an appropriate emergency response can be activated during and outside normal working hours, including the control of emergency access as appropriate and emergency exit routes to avoid evacuating personnel through areas of higher risk; and
 - identify risks surrounding the safe removal, transport, treatment and accommodation of contaminated people or objects.

¹ Part 2 of the SSBA Standards covers the risk and incident management processes, including the risk assessment and risk management plans, required by the SSBA Regulatory Scheme.

3.3 Analysis of risk

The analysis of the risk involves considering the likelihood and impact of the risk in light of controls already in place. At the end of the analysis the risk should be given an initial risk rating. This assists in determining if further controls are needed and provides a baseline for evaluation of any further controls to reduce the risk.

The SSBA Standards state that the analysis of the risks must include:

- If action is needed to prevent the occurrence of incidents;
- effectiveness of physical security controls (see Part 4 of the SSBA Standards);
- effectiveness of the processes for decontamination/inactivation of contaminated and potentially contaminated items (see part 7 of the SSBA Standards);
- identification of those responsible for devising, implementing and testing control measures.

A table to record the risks identified and to determine the effectiveness of controls, likelihood and consequence can be found in this document at section 3.5 – Risk Tables. The first part of the table uses the following headings:

- **Category:** What broad category does this risk fall under (e.g. operational, staffing, facilities, IT, legislation etc)? Use of broad categories allows you to group risks together for more effective analysis and treatment.
- **Risk:** What can happen?
- **Source:** How can the risk occur?
- **Consequence:** What is the consequence of the risk occurring?
- **Controls:** What controls are currently in place?

Once the risks have been identified and the consequences determined, the second part of the table can be filled in to determine the current risk level. These columns can be filled in using the risk matrices at Appendix A. A decision is then made as to whether the risk is acceptable or unacceptable according to the risk acceptance level set by the entity (see 3.4).

3.4 Risk acceptance level

Prior to determining the risk ratings, the entity should determine what level of risk is acceptable. For example, the entity may decide that a risk level of *Medium* is acceptable and that any risks at this level or below will be monitored. Any risks identified as being higher than medium will then be treated with further controls.

Example

A risk acceptance level of **Medium** was determined as tolerable. Risks that are deemed to be **Low** require no action at this time and will be monitored to ensure the risk rating does not become higher. Risks determined to be **Medium** currently have adequate control measures in place but will be managed and monitored to ensure the controls continue to maintain the risk level. Risks with a rating of **High or Extreme** will undergo further risk management to reduce the risk to an acceptable level.

3.5 Risk assessment table

Category	Risk <i>What can happen?</i>	Source <i>How can this happen?</i>	Consequence <i>What is the consequence on entity if it does happen.</i>	Controls <i>What is currently in place to stop it happening or reduce the level of consequence.</i>	Effectiveness of controls	Likelihood	Consequence	Current risk rating	Acceptable or unacceptable

3.6 Risk treatment action plan

A risk treatment plan for all risks identified under section 3.5 that had a risk rating of <risk level> or higher.

Category	Risk	Current Risk Rating	Target Risk Rating <i>What rating can be effectively achieved.</i>	Risk Treatment <i>What can be done to reduce the chance of the risk happening or the level of consequence if it does.</i>	Risk Treatment Owner	Expected Completion date

3.7 Vulnerability analysis

A vulnerability analysis must be performed for all entities handling Tier 1 SSBAs. In risk management terms, a vulnerability is defined as any weakness that can be exploited to make an asset susceptible to change. A vulnerability analysis is the determination of how each credible threat can be realised against a critical asset. Critical assets (in this case the SSBA and the sensitive information relating to the SSBA) are usually protected by several layers of security. Multiple layers of control are aimed at preventing access if one layer fails. The layers might be physical security controls, access controls, staff selection and vetting, standard operating procedures, secure record controls, auditing and incident investigation and other layers of controls.

The vulnerability analysis looks at weaknesses in each of these layers and works out how they can be exploited, to identify gaps that need to be addressed. The vulnerability assessment does not look at the consequences of the attack, as this is conducted in the risk assessment. Vulnerability assessments should look at the most credible worst case scenario, not the absolute worst case scenario.

The Australian Standards Handbook HB167:2006 – Security Risk Management may assist when performing a vulnerability analysis.

4 Budget

This should include any finances for monitoring and review as well as any funding to deal with any risk management strategies.

5 Monitoring

A monitoring plan should be put in place for all risks that were deemed tolerable. The plan should include how risks will be monitored and timeframes for monitoring.

Category	Risk	Monitoring plan	Owner	Timeframes

6 Review

When will the risk assessment and risk management plan be reviewed? Under the SSBA Standards, it is mandatory that a review of the risk assessment and risk management plan is undertaken at least annually for facilities handling Tier 1 SSBAs and every two years for facilities handling Tier 2 SSBAs.

The risk assessment and risk management plan should also detail what else may prompt a review. For example:

- an incident (which may or may not be a Reportable Incident under the SSBA Regulatory Scheme);
- changes in the SSBAs handled;
- changes in procedures;
- change to the national threat level; or
- following a request to do so by the Department of Health and Aged Care.

Attachment A – Sample risk matrix tables

It is not mandatory to use these tables and tables may be altered to reflect the business of the entity.

Risk consequence rating table


Consequence					
Criteria	Insignificant	Minor	Moderate	Major	Catastrophic
Impact on organisational outcomes	Little or no impact, no financial loss	Inconvenient project delay, financial loss of >5% to net revenue or assets	Material project delays, under achievement of target performances, financial loss of >10% to net revenue or assets	Significant project delays, performance significantly under target, financial loss of >20% to net revenue or assets	Non achievement of objective, performance failures, financial loss of >30% to net revenue or assets
Critical services disruptions	No material disruptions	Short term backlog or suspensions of work	Medium term backlog or suspensions of work	Prolonged backlog or suspensions of work, additional resources required	Indefinite backlog or suspension of work, significant additional resources required
Health and safety	Ailments not requiring medical treatment or first aid only, no lost time or occupational illness	Minor injury, medical treatment required	Serious injury causing hospitalisation or multiple minor injuries, lost time or recoverable occupational illness	Life threatening injury or multiple serious injuries causing hospitalisation, potential for permanent disability	Deaths or multiple life threatening Injuries

Consequence					
Criteria	Insignificant	Minor	Moderate	Major	Catastrophic
Reputation	Little or no impact, not at fault, unlikely to be widely broadcast or known	Potential media interest (non-headline exposure), concerns raised	Media interest (headline exposure at local level) over short term, criticism by local community and government, damage to reputation over short term	Strong media interest with potential national coverage over short to medium term, adverse public attention	Maximum exposure with national coverage. Intense media interest over long term, serious public outcry, loss of credibility
Non-compliances with regulation	Little impact, no breach	Breach of internal procedures and guidelines, performance reviews possible	Breach of non-legislative regulatory requirements. Performance reviews required	Breach of legislative requirements. Formal investigations and disciplinary actions	Deliberate breach, criminal negligence or act Potential for prosecution Loss of registration



Effectiveness of controls

Adequate	A control or set of controls that should be effective in managing the risk and is well applied (implemented, documented, communicated and monitored.) An adequate control implies that the risk is well managed and no further treatments are required.
Marginally Effective	A control or set of controls that manage a part of the risk, or are not completely applied. A marginally effective control implies that a treatment is necessary however this may depend on the level of risk. Low or Medium risks may not warrant the additional costs.
Inadequate	A control or set of controls that ineffectively manage the risk or are not or partially applied. An inadequate control implies that treatments are necessary.

Risk likelihood table

 Likelihood	Expected in most circumstances. Has occurred on an annual basis in the past or circumstances are in train that will cause it to happen.	Almost certain
	Has occurred in the last few years or has occurred recently, circumstances have occurred that will cause it to happen in the short term.	Likely
	Has occurred at least once in the history of the organisation or is considered to have a 5% chance of occurring in the current planning cycle or term of the project.	Possible
	Has never occurred in the organisation but has occurred infrequently in other similar organisations or is considered to have around a 1% chance of occurring in the current planning cycle or term of the project.	Unlikely
	Exceptional circumstances only. Is possible but has not occurred to date in any similar organisation and is considered to have very much less than a 1% chance of occurring in the current planning cycle or term of the project.	Rare

Risk Consequence Table

 Consequence 					
Rating	Insignificant	Minor	Moderate	Major	Catastrophic
Outcomes	Project is delayed. Impact limited to project only. Minor errors in system requiring corrective action. Self improvement review required.	Project does not meet objectives. Impact predominantly limited to the project only. Minor delay without impact on overall schedule or services do not fully meet needs. Scrutiny by internal committee or audits to prevent escalation.	Project failure. One or more performance indicators not met. Impact on the reputation of the Branch. External committee or department scrutiny.	Project failure. Major Impact on organisation outcomes and over 10% of performance indicators not met. Impact on the reputation of the organisation. Intense public, political or media scrutiny.	Project failure. Significant impact on organisational outcome and over 30% of performance indicators not met. Critical impact on the reputation of the organisation, through system failure, bad policy advice or ongoing non-compliance. Potential for significant legal consequences.

Risk analysis matrix

		Consequences				
		Insignificant	Minor	Moderate	Major	Catastrophic
Likelihood	Almost certain	Low	Medium	High	Extreme	Extreme
	Likely	Low	Medium	High	High	Extreme
	Possible	Low	Medium	Medium	High	Extreme
	Unlikely	Low	Low	Medium	Medium	High
	Rare	Low	Low	Medium	Medium	Medium

Acceptability table

Extreme (E)	Unacceptable	Must be given immediate Executive attention
High (H)	Active management	Must have considerable management to reduce to as low as reasonably practicable
Medium (M)	Tolerable	Risks should be managed and monitored to reduce to as low as reasonably practicable
Low (L)	No action required	Manage and monitor with normal operational management practices