Australian Government

Department of Infrastructure, Transport,
Regional Development and Local Government

GUIDANCE PAPER:
TRANSPORT SECURITY RISK ASSESSMENT for

Operators of Prescribed Air Services and Security Controlled Airports

Contents:

This Transport Security Risk Assessment Guidance Material has been prepared to assist aircraft and airport operators construct a Security Risk Assessment.

Disclaimer: This document is designed to provide general guidance to prescribed air service operators, operating under arrangements according to the Aviation Transport Security Act 2004 (the ATSA) and Aviation Transport Security Regulations 2005 (the ATSR) in developing Transport Security Programs (TSPs) for submission to the Secretary of the Department of Infrastructure, Transport, Regional Development and Local Government (The Department) for approval. This guide should not be used by prescribed air service operators as a substitute for obtaining independent professional advice (including legal advice) regarding their TSP and the TSP's compliance with the requirements of the ATSA and the ATSR. This document is subject to change. The Department is not responsible for the consequence of the use of any outdated version of this guide.

Table of Contents

1

2 INTRODUCTION

This paper provides guidance for aircraft and airport operators (operators) conducting Security Risk Assessments (SRAs) of their people, assets, infrastructure and operations. The approach taken in the guide recognises that, in the Australian context, operators are best placed to determine risks to their own people, assets, infrastructure and operations as well as identify appropriate preventative security measures and procedures for inclusion in Transport Security Programs (TSPs).

The purpose of a SRA is to provide a sound risk based approach to the implementation of security planning. SRAs ensure that a systematic and analytical process is conducted with the aim of identifying security measures and/or procedures that reduce the probability of acts of unlawful interference with aviation and/or minimise harm to people, assets and operations should unlawful interference occur. Operators should also have security risk information available to them in order to make well-informed decisions regarding the implementation of preventative security arrangements directed at reducing acts of unlawful interference with aviation and ensuring public confidence in aviation security arrangements.

3 GENERAL GUIDANCE

Operators are encouraged to use the combined Australian/New Zealand standard and handbook HB 436:2004 Risk Management Guidelines (a companion to AS/NZS 4360:2004 Risk Management) to complete their SRAs. These guidelines provide guidance in conducting a SRA using the risk management guidelines.

SRAs should identify security risks to all operations, demonstrate that the risks have been adequately analysed and evaluated, and determine appropriate preventative and mitigative security strategies to control unacceptable or intolerable risks.

At all times SRAs should be protected from unauthorised access, amendment or disclosure, due to the sensitive nature of their contents.

SRAs should be drafted in an easy to read plain English format ensuring that the key elements of the risk management process adopted are clearly identifiable. If SRAs are not presented in an easy to read format, DOTAR's assessment and review processes of TSPs may be delayed.

Key definitions used in this document are described in Part 9.

4 REQUIREMENTS OF SECURITY RISK ASSESSMENTS

SRAs should include:
The date when the assessment was completed or reviewed;
The scope of the assessment, including the people, assets, infrastructure and aircraft operations assessed;
A summary of how the assessment was conducted, including details of the risk management process adopted;
Identification and evaluation of strategically important assets, infrastructure and operations that need to be protected;
Identification and assessment of possible security risks to people, assets, infrastructure and operations, and the likelihood and consequences of their occurrence;
Identification of existing current security measures, procedures and operations; and
Identification, selection and prioritisation of risk treatments (for example, counter-measures and procedural changes that need to be implemented) and their effectiveness in reducing risk levels.

Operators should consider the following when deciding on the scope of their SRA:
The location and nature of the operations, services or facilities to be covered. For example, operating to and/or from remote areas will have advantages and disadvantages different from those when operating from densely populated urban areas.
Those who have responsibility for the security of the operations, and services to be covered by the SRA. Those responsible for security, and those who have an impact on security, should be adequately consulted during the SRA process.

5 THE SECURITY ASSESSMENT PROCESS

This guidance paper sets out an indicative process for SRAs based on the standard, AS/NZS 4360:2004 Risk Management. However, operators may wish to use different risk assessment tools based on the AS/NZS 4360:2004 which have been developed for their individual circumstances. References to the AS/NZS HB 436:2004 Risk Management Guidelines are mentioned throughout this document as footnotes to the text.

The main elements of the risk assessment process set out in AS/NZS HB 436:2004 Risk Management Guidelines are:

Communicate and Consult[1]
This is an ongoing process that occurs before, during and after the risk assessment to gather information, keep stakeholders informed and to disseminate the findings of the risk assessment to those who need to administer risk treatments.

Establish the Context[2]
This part sets the context of the risk assessments in terms of the external context, the internal context, the risk management context and the context of existing risk controls. This step also includes developing the risk criteria and defining the process for the remainder of the process.

Risk Identification[3]
This part determines who and what is at risk and the sources of harm (hazards) with the potential to harm assets. Consider what can happen, when and where. Consider why and how it can happen.

Analyse Risks[4]
This part analyses existing controls and estimate likelihood and consequence in the context of existing controls.

Evaluate Risks[5]
This part evaluates and rate the identified risks based on likelihood and consequences and an agreed risk rating scale and set risk priorities.

Treat Risks[6]
This part identifies the range of options for the treatment of risks assessed to be intolerable or unacceptable and determine the cost effective risk control strategies available to reduce likelihood and/or consequences and develop treatment plans.

Monitor and Review Risks[7]
This part provides guidance for monitoring risks and risk treatments for effectiveness allowing the adjustment of risk treatments to maintain the desired level of risk control.

Recording the Risk Management Process[8]
This part sets our guidelines for recording and reporting the process in a manner allowing for auditing and review of the process and compliance with good corporate governance guidelines.

Establishing Effective Risk Management[9]
This part sets out guidelines for effective risk management and whilst placed in the latter parts of the guidelines it should be considered at the start of the process.

[1] Refer to HB 436:2004 Risk Management Guidelines – page 19 - 25 *Part 3 Communicate and consultation*
[2] Refer to HB 436:2004 Risk Management Guidelines – page 27 - 36 *Part 4 Establish the context*
[3] Refer to HB 436:2004 Risk Management Guidelines – page 37 - 41 *Part 5 Risk identification*
[4] Refer to HB 436:2004 Risk Management Guidelines – page 43 - 61 *Part 6 Risk Analysis*
[5] Refer to HB 436:2004 Risk Management Guidelines – page 63 – 67 *Part 7 Risk evaluation*
[6] Refer to HB 436:2004 Risk Management Guidelines – page 69 – 86 *Part 8 Risk treatment*
[7] Refer to HB 436:2004 Risk Management Guidelines – page 87 - 93 *Part 9 Monitoring and review*
[8] Refer to HB 436:2004 Risk Management Guidelines – page 95 - 102 *Part 10 recording the RM process*
[9] Refer to HB 436:2004 Risk Management Guidelines – page 103 - 111 *Part 11 Establishing effective RM*

6 THE AS/NZS 4360 RISK ASSESSMENT PROCESS

7 ESTABLISHING THE CONTEXT

7.1 General

This part determines the external (strategic), internal (organisational) and risk management context of SRAs to be undertaken[10]. Key external and internal stakeholders should also be identified to assist in the SRA process. It sets out the individual, local and unique circumstances including geographical, seasonal and operational factors operators should consider when determining the scope of the assessment to be undertaken. The SRA should outline its scope and be conducted in the context of existing security measures.

7.2 The External Context

This part defines the external environment in which operators conduct business. It also defines the relationship between the operator and the external environment. Defining the external context includes consideration of the following factors:

Environmental and Geographical;
Business and Operational;
Statutory and Regulatory;
Social and Cultural;
Competitive;
Political; and
Financial.

It is particularly important to take into account the perceptions and values of external stakeholders and establish policies for communication with these parties.

Establishing the external context is important to ensure that external stakeholders and their objectives are considered when developing risk management criteria and that externally generated threats and opportunities are taken into account.

7.3 The Internal (Organisational) Context

This part defines the internal or organisational context. Before a SRA is undertaken it is necessary to understand the organisation. Key areas include:
The organisational culture;
Internal stakeholders;
Organisational structure;
Capabilities in terms of resources such as people, systems, processes, capital; and
Goals and objectives and the strategies that are in place to achieve them.

Establishing the internal context is important because:
Risk management takes place in the context of the goals and objectives of the organisation;
The major risk for most organisations is that they fail to achieve their strategic, business or project objectives;
The organisational policy and goals and interests help define the organisation's risk policy; and
Specific objectives and criteria of aircraft operation and associated activity must be considered in the light of objectives of the organisation as a whole.

Establishing the internal context for a SRA will also require consideration of the following:
Critical Assets and Resources;
Critical functions and business activities;
Operational capabilities;
Risk management capabilities (or lack thereof);
Activities and Programs (a summary of passenger, charter, cargo, training operations);
Existing risk controls;
Risk tolerance level or position;
Limitations on risk treatments including budget constraints.

[10] Refer to HB 436:2004 Risk Management Guidelines – page 27 – 36 *Part 4 Establish the context*

7.4 The Risk Management Context

The goals, objectives, strategies, scope and parameters of the activity, or part of the organisation to which the risk management process is being applied, should be established. The process should be undertaken with full consideration of the need to balance costs, benefits and opportunities. The resources required and the records to be kept should also be specified. Setting the scope and boundaries of an application of risk management involves:

Defining the organisation operations, processes, project or activity and establishing goals and objectives;
Specifying the nature of the decisions that have to be made;
Defining the extent of the project activity or function in terms of time and location;
Identifying any scoping or framing studies needed and their scope, objectives and the resources required; and
Defining the depth and breadth of the risk management activities to be carried out, including specific inclusions and exclusions.

Specific issues that may also need to be considered include:
The roles and responsibilities of various parts of the organisation participating in the risk management process; and
Relationships between the project or activity and other projects or parts of the organisation.

Defining the risk management context for SRAs pertaining to operations also includes:
The aviation transport security risk context;
Determining the resources and expertise required;
Defining the risk reporting criteria;
Defining the Impact (Consequence) criteria;
Defining the Likelihood (Probability or Frequency) criteria;
Defining the Risk Rating criteria; and
Outlining the local security risk context of your operations.

7.5 Defining the Risk Criteria

This involves defining the criteria against which risks are to be evaluated. Decisions concerning whether or not risk treatment is required may be based on operational, technical, financial, legal, social, environmental, humanitarian or other criteria. The criteria should reflect the context defined in the parts above.

The following criterion has been developed by the Department of Infrastructure, Transport, Regional Development and Local Government. It is similar to the criterion set out in the HB 436:2004 Risk Management Guidelines.

7.6 Likelihood Estimate Criteria – example

The example likelihood criteria set out in the table below has been selected because it follows the example provided in AS/NZS HB 436:2004. Further, those making the assessments may need to rely heavily on those with corporate memory. Accordingly, it uses a simple scale that is designed to help people recall the frequency of security incidents in terms of so many per year.

	LIKELIHOOD	DEFINITION
A	Almost Certain	Is expected to occur in most circumstances. (100/year)
B	Likely	Will probably occur in most circumstances. (10/year)
C	Possible	Might occur at some time. (1/year)
D	Unlikely	Could occur at some time. (1/10 years)
E	Rare	May occur only in exceptional circumstances. (1/100 years)

7.7

7.8 Consequence Estimate Criteria – example

The example consequence criteria set out in the table below has been selected because it follows the examples provided in AS/NZS HB 436:2004. Consequence definitions should be considered in the context of the operator, and possibly the communities served by the operations. The scale should reflect the extremes of what is insignificant and what is catastrophic in the organisational context with the intermediate ratings spread between. Care should be taken not to understate or overstate the definitions.

	CONSEQUENCE	DEFINITION
1	Insignificant	Risk impact would be negligible or no risk impact can be identified to community or business.
2	Minor	Risk impact would result in few consequences, such as minor disruption to community and/or business, but of limited overall consequence.
3	Moderate	Risk impact would result in some consequences, such as short-term disruption to community and/or business.
4	Major	Risk impact would result in serious consequences, such as medium-term disruption to community and/or business.
5	Catastrophic	Risk impact would result in disastrous consequences, such as long-term disruption to community and/or business. *The worst case outcome for the community and/or business.*

7.9

7.10 Risk Rating Criteria – example matrix

The example risk rating criteria has been selected because it follows the example provided in AS/NZS HB 436:2004. The matrix allows inputs of likelihood and consequence for each risk or risk category assessed and provides a risk rating. The numerical notations have been added to provide further refinement when assessing risks within a rating range. For example an extreme risk could range from 10^7 to 10^9. The notation helps refine the range so that small shifts in risk rating can be determined.

	INSIGNIFICANT 10^3	MINOR 10^4	MODERATE 10^5	MAJOR 10^6	CATASTROPHIC 10^7
ALMOST CERTAIN 10^2 ~ 100/Year	High 10^5	High 10^6	Extreme 10^7	Extreme 10^8	Extreme 10^9
LIKELY 10^1 ~ 10/Year	Moderate 10^4	High 10^5	High 10^6	Extreme 10^7	Extreme 10^8
POSSIBLE 10^0 ~ 1/Year	Moderate 10^3	Moderate 10^4	High 10^5	High 10^6	Extreme 10^7
UNLIKELY 10^{-1} ~ 1/10Year	Low 10^2	Moderate 10^3	Moderate 10^4	High 10^5	High 10^6
RARE 10^{-2} ~ 1/100Year	Low 10^1	Low 10^2	Moderate 10^3	Moderate 10^4	High 10^5

Specific risk treatment options and actions should be adopted for all Extreme and High risks identified and adequately documented in subsequent security planning processes. A generic treatment action criterion follows:

Extreme (or Very High[11]) and High Risk – immediate executive management attention needed, action plans and management responsibility specified.
Medium Risk - Manage by specific monitoring or response procedures, with management responsibility specified.
Low Risk - Manage by routine procedures, unlikely to need specific application of additional resources.

8 IDENTIFYING SECURITY RISKS

8.1 What can Happen and How it can Happen[12]

Security risks are defined as those risks where the perpetrator carries out a deliberate act designed to cause harm to their target (victim) or to gain a benefit for the perpetrator or both. In the aviation context it is – the risk of "acts of unlawful interference with aviation" that must be the focus of all security risk considerations.

[11] HB 436:2004 Risk Management Guidelines use the term Very High Risk in lieu of Extreme Risk
[12] Refer to HB 436:2004 Risk Management Guidelines – page 37 - 41 *Part 5 Risk identification*

Risk identification should consider potential risks arising from the general public, passengers and vehicles, regulated cargo operations, including the receipt, storage, land transport and handling, screening and loading of cargo onto aircraft.

This Part generates a list of generic security risks, (what can happen) and considers possible causes and scenarios (how it can happen). The exercise is to determine possible risks that if realised could harm people, assets, infrastructure or operations, as well as considering how the identified risks could be realised (e.g. how terrorist acts could be perpetrated), to evaluate areas of exposure and vulnerability and to subsequently establish and prioritise security planning requirements.

8.2 Assets at Risk

The identification of people and assets, including critical infrastructure and operations at risk is fundamental to the identification of risks. People may include the public, pilots, air and ground crew and administrative and support staff. Important infrastructure may include aircraft, terminal facilities, loading facilities, refuelling and fuel storage areas, transport storage areas and/or hangar facilities.

An analysis of the criticality of people, assets, infrastructure and operations at risk is essential for the assessment of possible consequences should the risk/s be realised.

8.3 Risk Assessment for Operators

SRAs should focus on the identification and evaluation of the risks to people, assets, infrastructure, operations and aviation transport. Consideration should be given to risks that if realised may result in:
Unlawful interference with aviation; and/or
Significantly reducing public confidence in using aviation transport services.

8.4 The Current Security Environment

Generally, SRAs should be made in the context of the current security environment. For more information about the National Counter-Terrorism Alert Level go to www.nationalsecurity.gov.au When conducting a SRA, all contemporary security risks should be considered, including terrorism in all its potential forms. This approach enables consideration of actual and potential risks to aviation transport operations and the travelling public.

8.5 Risk Categories and Sources of Harm (Hazards)

The template which assists in identifying risks to your operations also refers to six (6) security risk categories. The categories arise from potential sources of harm, or hazards shown in *italics* that should be considered when conducting a SRA.
When identifying risks, consideration should be given to risks and associated sources of harm (*hazards*) and possible outcomes according to the six identified risk categories:

Vandalism – *vandals* damaging aircraft, support equipment, infrastructure, systems or facilities;
Public interference - *troublemakers* (including drunks, persons in custody and emotionally disturbed persons) disrupting operations causing harm, delays and inconvenience or offence to other travellers;
Insider Interference - *disgruntled insiders* engaging in inappropriate behaviour causing losses, disruptions or damage and includes sabotage.
Group interference - *Violence prone groups* (politically motivated or otherwise) – disrupting normal operations causing a high degree of interference, inconvenience, delay and or offence to other travellers;
Crime - *criminals* engaging in crime to gain advantage for themselves such as in theft, sabotage or other criminal behaviour; and
Terrorism – *terrorists* engaging in acts of terror and destruction by way of bombings, sabotage, hijacking, kidnapping, shootings and sieges.

8.6 Risk Scenarios

Risk scenarios should be developed to determine how various risks might be realised and unfold. Previous security incidents (security history) should be used to make informed decisions about possible security risks of the future. Security history must be viewed in the context of the security measures and other pertinent factors that existed at the time of the incidents. Operators should consider their own particular risk scenarios for their particular operations. Having identified a list of risks it is then necessary to consider possible risk scenarios to determine how the risk may be initiated and realised. It is important that significant risk causes and scenarios are identified.[13]

[13] Refer to HB 436:2004 Risk Management Guidelines – page 37 - 41 *Part 5 Risk identification*

Operators conducting SRAs should endeavour to capture key risk scenarios. It is expected that consideration will be given to the identification of risk scenarios that identify security exposures and/or vulnerabilities in physical protection, personnel protection systems, processes and other areas that may lead to a security incident. However, most lists of potential risk scenarios will not be exhaustive, as it is not practical to document all potential situations that could cause loss. It is also not necessary to record excessive numbers of similar risk scenarios. However, risk scenarios should be investigated and recorded where people, assets, infrastructure and/or operations are considered exposed or vulnerable to acts of unlawful interference with aviation or where there is a need to ensure greater public confidence in security arrangements.

When identifying security risks, past experiences and history can be of great assistance. However, security hazards (criminals and especially terrorists) have the ability to assess existing security measures and be creative. Accordingly, it is important to explore beyond what has occurred in the past and consider what the foreseeable risks may be.

Some example risk scenarios are contained in the template to illustrate how risks could occur.

9 ANALYSING RISKS

9.1 Determine Likelihood and Consequence[14]

This Part determines the effectiveness of existing controls - their implementation and analyses in terms of consequence and likelihood, in the context of existing controls.

9.2 Determine Existing Controls

When estimating the consequences and likelihood of a risk, consideration should be given to the presence of existing preventative security measures provided, including those provided by airport operators at security controlled airports, such as perimeter fences, access control, security awareness, security patrols and procedures. Risks must be examined in the context of these controls. It is recommended that security surveys and inspections or audits of existing security control arrangements be conducted to determine their strengths and weaknesses prior to an analysis of the risks identified. It is also important to closely evaluate how rigorously management and staff use and maintain existing controls in order to fully assess their effectiveness.

9.3 Methods of Risk Analysis

A number of methodologies have been developed to analyse risks depending on the risk information and data available. Qualitative, quantitative or semi-quantitative risk analysis (or a combination of these) can be conducted under the AS/NZS 4360 standard, which provides examples of qualitative and quantitative methods at page 53 of HB 436 Risk Management Guidelines. However, qualitative risk analyses are considered sufficient for aviation SRA purposes as they provide satisfactory indicators of risk levels.

9.4 Likelihood

When estimating the likelihood[15] element of risk, consideration should be given to the exposure of people, aircraft and operations, to acts of unlawful interference with aviation and public confidence in aviation through the exploitation of security weaknesses in operations. The intent and capability of potential sources of harm to conduct criminal acts may also be relevant factors to consider in determining the likelihood of a risk event. The frequency of past security incidents is a good guide to general criminal behaviour but must be assessed in the context of controls that exist now – not those that existed at the time of the past incident or incidents.

9.5 Consequence

A qualitative rating or score of consequence[16] for each risk identified should be determined. Example Risk Consequence Ratings that could be used to determine a consequence rating for a particular risk are included in the template. Individual risks may have different scores for the different risk categories identified. These individual scores should be considered together prior to determining an overall consequence score for a particular risk. The table can be used or modified by operators completing SRAs to suit their own circumstances.

[14] Refer to HB 436:2004 Risk Management Guidelines – page 43 - 61 *Part 6 Risk analysis*
[15] Refer to HB 436:2004 Risk Management Guidelines – page 54 *Part 6 Risk analysis*
[16] Refer to HB 436:2004 Risk Management Guidelines – page 53 *Part 6 Risk analysis*

10 EVALUATING RISKS

10.1 Identify Risk Priorities

Risk evaluation[17] requires a comparison of identified risk levels to predetermined risk assessment criteria established for the SRA. The Risk Rating Matrix provides an example assessment table for combining the estimated likelihood of a risk being realised with the estimated consequence to determine a risk rating.

Estimates for consequence and likelihood for each risk identified during the SRA may be recorded in the Risk Rating Template.

The risk evaluation should result in separating the minor acceptable or tolerable risks from the higher risks allowing management action to be focused on the latter.

11 TREATING RISKS

11.1 Determining and Implementing Risk Controls[18]

The treatment of risks involves the identification of options for treating risks that are not acceptable or tolerable and implementing risk controls. Risk treatments may be implemented to reduce the likelihood or consequence of a risk or both.

Decisions by operators concerning the treatment or tolerance of risks should be based upon consideration of risk assessment criteria as well as the need to balance costs, benefits and opportunities. Risks identified that impact on operators but are outside the control or responsibility of the individual operator should be noted and discussed with the appropriate owner or operator. Specific risk treatment options and actions should be adopted for all Extreme and High risks identified and adequately documented in subsequent security planning processes.

A list of preventative and mitigative security measures and procedures should be identified for all intolerable risks identified. The objective is to ensure that the most effective security measures are employed to reduce the exposure and/or vulnerability of people and aviation operations, services and facilities to potential risks. All risk treatment options should be considered in the local context by operators on the basis of their likely effectiveness in risk reduction, practicality of implementation, overall cost and benefits derived. In many cases, it is unlikely that one risk treatment option will provide a complete treatment for a particular risk. Conversely, one risk treatment may have a significant reduction effect on a number of risks.

Whilst specific risk treatment strategies should be outlined for all Extreme and High risks, it is also realistic to assume that some risks may need to be tolerated on the basis that security measures are not feasible or cost effective. For example, it may not be practicable to significantly reduce the potential of some risks to some aviation transport assets due to local circumstances. However, it may be practicable for some security measures to be put in place, such as aircraft wheel locks or other anti-theft devices. Moderate and Low risk may be treated by general risk treatments.

However, preventative security planning procedures and practices should be monitored, reviewed and tested to determine whether or not the risks have been adequately treated.

11.2 Risk Treatment Planning

Following the selection of preferred risk treatment options a schedule for implementation should be prepared. The schedule, which should be authorised at executive management or the aircraft operations management level, should identify:
the risk category to be treated by the security measures or procedures;
the desired security outcome;
the security measure or procedure (i.e. the risk treatment);
the estimated cost of the treatment (both initial and ongoing costs);
the person responsible for the risk treatment actions;
the target date and/or schedules for implementation of new security measures or procedures;
a description of what additional risk treatments will be deployed in the event of a heightened security alert level being declared (e.g. High or Extreme national security alert).

[17] Refer to HB 436:2004 Risk Management Guidelines – page 63 – 67 *Part 7 Risk evaluation*.
[18] Refer to HB 436:2004 Risk Management Guidelines – page 69 - 86 *Part 8 Risk treatment*

.

It should be noted that some risk treatments may be effective security measures and procedures but may not significantly alter the risk rating if implemented. These risk treatments should be assessed and adopted on the basis of their contribution to the overall desired risk treatment package.

11.3 National Security Alert Levels

National security alert levels provide guidance of the assessed likelihood of a terrorist attack in Australia. Alert levels are subject to change. Therefore, operators should plan security measures for expedient deployment in the event that the alert levels should rise to a high or extreme. The alert levels are defined as follows:

Extreme - A terrorist attack is imminent or has occurred.
High - High risk of terrorist attack in Australia.
Medium - Medium risk of terrorist attack in Australia.
Low - No information to suggest a terrorist attack in Australia.

11.4 Treatments for Higher National Security Alert Levels

Appropriate security measures for High alert include those that could be deployed quickly such as additional security procedures, precautions and additional staff or changed security priorities.

Appropriate security measures for Extreme alert include those that could be deployed immediately such as additional or changed security procedures, precautions, changed security priorities and the temporary halt of high risk activities.

11.5 Documenting Risk Treatments

A template with an example of a Risk Treatment Implementation Schedule is included in the Templates document.

Once risk treatments have been identified there is an additional template which provides a table for allocating post treatment risk ratings to each of the risk categories.

12 MONITORING AND REVIEW[19]

12.1 An Ongoing Process

It is necessary to monitor and review security risks and the effectiveness of treatments to ensure that they remain relevant to the security environment. Regular monitoring and reviewing is required to ensure that risks identified are consistent with the evolving risk context, that risk treatments are effective, remain appropriate and are properly implemented. It can also help to identify alternative and potentially more effective risk treatment solutions. SRAs should also be reviewed and updated when major changes to your operations or assets occur.

It may also be necessary for operators to review their SRAs after changes in Aviation Transport Security Legislation, or distribution of new security information by the Department of Infrastructure, Transport, Regional Development and Local Government.

13 COMMUNICATION AND CONSULTATION[20]

13.1 An Ongoing Process

Communication and consultation with internal and external stakeholders is required throughout the SRA process. Executive management should be part of the SRA process if they are to make well-informed decisions regarding the implementation of preventative security measures to counter acts of unlawful interference with aviation and ensure public confidence in aviation.

The sharing of information, within acceptable bounds of confidentiality, between operators is encouraged to promote a common understanding of local risks and to foster the exchange of best practice security measures and procedures between aviation industry participants.

[19] Refer to HB 436:2004 Risk Management Guidelines – page 87 - 93 *Part 9 Monitoring and review*
[20] Refer to HB 436:2004 Risk Management Guidelines – page 19 - 25 *Part 3 Communication and consultation*

The SRA process for operators will need to involve consultation with relevant owners and authorities overseeing airport facilities and other infrastructure used by the operator.

13.2 Further Guidance

A list of information resources is provided at Part 10 of this document.

14 TEMPLATES

Templates have been developed to simplify and standardise the SRA process for operators.

To conduct a SRA in accordance with this guide, operators should complete the templates, keeping in mind the context of their operations and the scope of the assessment.

The security risk and hazard (sources of harm) categories provided in the templates have been distilled down to six (6) following consultation at regional aviation SRA workshops. Risk and risk scenarios based on these six risk and hazard categories should be determined. Where you need to record more detail about your security concerns, use the risk scenario sections of the templates.

Words in *italics* are provided as examples only and should be deleted or amended to reflect your circumstances before submitting the completed templates as part of your SRA to the Department of Infrastructure, Transport, Regional Development and Local Government for review.

15 KEY DEFINITIONS

Consequence – the outcomes of an event expressed qualitatively or quantitatively, being loss, injury, disadvantage or gain. There may be a range of possible outcomes associated with an event – eg, loss of life or public injury, damage to critical infrastructure, loss of business continuity, police or other investigation etc.

Control – any existing process, policy, device, practice, procedure or measure that acts to minimise negative risk or to enhance positive opportunities.

Criticality – part of the consequence assessment to determine how critical the various people, assets and resources at risk are to the business and/or community.

Event – occurrence of a particular set of circumstances.

Exposure – Being open to a hazard. The degree to which assets are unprotected.

Frequency - is the rate of occurrence of an event or outcome. The measure of the number of occurrences per unit of time.

Hazard – a source of potential danger or harm, including a situation with the potential to cause commercial loss. The potential of a hazard to cause harm may be further determined by treat assessments.

Likelihood – used as a general description of probability or frequency. Because there is an element of chance associated with risk likelihood is expressed qualitatively in the range 'almost certain' to 'rare' or in the case of AS/NZS HB 436:2004 page 54 'almost incredible'

Loss – any negative or adverse consequence.

Probability – a measure of the chance of occurrence expressed as a number between 0 (impossible) and 1 (certain). Probability is the ratio actual outcomes to the number of possible outcomes. Frequency of likelihood may be used in describing risk.

Regular Public Transport (RPT) – means the operation of an aircraft for the purpose of an air service that:
(a) is provided for a fee payable by persons using the service; and
(b) is conducted in accordance with fixed schedules to or from fixed terminals over specific routes; and
(c) is available to the general public on a regular basis.

Realised Risk/s – the occurrence of a set of circumstances constituting a risk event.

Risk - the chance of something happening that will have an impact upon objectives. It is measured in terms of consequences and likelihood.

Security Committee – means a body formed for the oversight, communication and coordination of security arrangements.

Security Manager – a suitably qualified/experienced person responsible for the development, implementation, review and maintenance of a TSP.

Security risk – means a risk involving deliberate illegal acts designed to establish a benefit for the perpetrator or to inflict a loss or injury on a victim or target asset. Safety risk may also have a human act at their source but differ in that the actions may be careless or negligent but are not deliberate.

Security Risk Assessment (SRA) – means the part of a transport security program that identifies, analyses, evaluates and treats risks to aviation security. SRAs consider the manner in which hazards contribute to risk. The assessment of consequences and likelihood together are used to estimate the risk levels.

Threat - a declaration of an intention to cause harm or the determination (or assessment) that a hazard may cause harm. This document refers to security threats only - not other forms of threats such as natural disasters or global economic downturns and other non security incidents.

Treatment – the process of selection and implementation of measures (and procedures or actions) to modify risk.

Vulnerability – a measure of the susceptibility to harm. Vulnerability should be considered when assessing consequences.

16 RESOURCE LIST

16.1 Risk Assessment and Management Resources

AS/NZS HB 4360:2004 Risk Management
This combined Standard and guideline provides a generic guide for the establishment and implementation of the risk management process involving the identification, analysis, evaluation, treatment and ongoing monitoring of risks. www.standards.com.au

AS/NZS HB 231:2000
Information Security Risk Management Guidelines
This Handbook provides a generic guide for the establishment and implementation of a risk management process for information security risks.

Critical Infrastructure Emergency Risk Management and Assurance Manual
The handbook is an additional resource to complement AS/NZS 4360:1999 Risk Management standard which will be continually refined to become a repository of collective knowledge and wisdom of the emergency risk managers in the infrastructure sector.
http://www.ema.gov.au/ema/emainternet.nsf/HeadingPagesDisplay/Research?OpenDocument#ermmanual

Securing Queensland's Critical Infrastructure: guidelines for owners/participants
A general critical infrastructure protection document produced by the Queensland Government on issues which should be considered when attempting to secure critical infrastructure.
http://www.premiers.qld.gov.au/library/pdf/infopackweb.pdf

Risk Management Process
Draft Guidance Manual for Infrastructure Participants
Tasmanian Counter Terror Review Team, Jan 2003

ANAO – Australian Government Audit Office

Business Continuity Management Guide
This guide presents a structured approach to business continuity management. The approach involves identifying preventative treatments for continuity risks that can be routinely managed, and developing an organisation- wide business continuity program-to deal with the consequences should the preventative treatments fail.
http://www.anao.gov.au/WebSite.nsf/Publications

16.2 Transport Security Resources

Australian Government's National Security Website
www.nationalsecurity.gov.au

Current National Counter-Terrorism Alert Level
www.nationalsecurity.gov.au

Department of Infrastructure, Transport, Regional Development and Local Government - *Transport Security*
http://www.infrastructure.gov.au/transsec/index.asp