



# Recognition Assessment Workbook

**PSP51804**

## Diploma of Government (Security)

Last Name: \_\_\_\_\_

First Name: \_\_\_\_\_

Agency: \_\_\_\_\_

Agency Address: \_\_\_\_\_

\_\_\_\_\_

Work Email: \_\_\_\_\_

Work Phone: \_\_\_\_\_

Mobile: \_\_\_\_\_



Registered Training Organisation

# 88101

(Version 1.1 July 2011)



## Table of Contents

Introduction .....	3
PSP51804 Diploma of Government (Security).....	4
PSP51804 Diploma of Government (Security) program assessment strategy .....	4
Assignments .....	4
Units of competency.....	4
Academic transcripts .....	5
How does Assessment by National Recognition work? .....	5
Evidence to support your assessment .....	5
Types of evidence .....	6
What to expect when compiling your evidence .....	7
Who will have access to my portfolio? .....	8
Complaints and appeals.....	8
Student Handbook.....	8
Where to get help .....	9
Telephone number for Recognition enquiries: (02) 6141 3678.....	9
Part 1: Candidate's personal details .....	10
Part 2: Candidate's employment history .....	12
Part 3: Candidate's self-assessment summary.....	13
Part 4: Third Party Referee reports – Diploma of Government (Security) .....	14
Part 5: Units of competency .....	15
PSPETHC501B – Promote the values and ethos of public service (Required unit) .....	20
PSPGOV505A – Promote diversity (Required unit) .....	26
PSPGOV413A – Compose complex workplace documents (Required chosen elective unit) .....	31
PSPGOV504B – Undertake research and analysis (Required unit) .....	36
PSPSEC501A – Assess security risks (Required unit) .....	42
PSPSEC502A – Develop security risk management plans (Required unit) .....	46
PSPSEC503A – Implement and monitor security risk management plans (Required unit)....	51
PSPLEGN501B – Promote compliance with legislation in the public sector (Required unit) .	55
PSPGOV512A – Use complex workplace communication strategies (Required unit).....	60
PSPSEC504A – Coordinate protective security (Required unit).....	64
PSPSEC505A – Protect security classified information (Required chosen elective unit) .....	67
PSPSEC506A - Communicate security awareness (Required chosen elective unit) .....	72

## Introduction

Welcome to the PSP51804 Diploma of Government (Security) – Recognition Assessment workbook. The aim of this workbook is to:

- provide you with an understanding of the training delivery and assessment strategies for the qualification, and
- assist you to identify and gather evidence from your workplace to confirm your competence in the units of competency.

To be eligible for the award of the Diploma of Government (Security) you will need to demonstrate your competency in at least 11 units of competency of which 9 units are required and 2 units are chosen electives. In the Protective Security Training Centre qualification, you will obtain 12 units of competency.

Unit of competency	Assessment Strategy
PSPETHC501B - Promote the values and ethos of public service*  PSPGOV505A – Promote diversity*	Generalist units assessed by recognition of your knowledge and skills in the workplace and confirmed by third party referee reports.
PSPGOV413A – Compose complex workplace documents**  PSPGOV504B – Undertake research and analysis*  PSPSEC501A – Assess security risks*  PSPSEC502A – Develop security risk management plans*  PSPSEC503A – Implement and monitor security risk management plans*	Delivered and partially assessed through the Advanced Security Risk Management course and formally assessed through submission of a post-course workplace assignment, submission of verification letter from supervisor and statement of authenticity.
PSPLEGN501B – Promote compliance with legislation in the public sector*  PSPGOV512A – Use complex workplace communication strategies*  PSPSEC504A – Coordinate protective security*  PSPSEC505A – Protect security classified information**  PSPSEC506A – Communicate security awareness**	Delivered through the Managing Protective Security course and formally assessed through submission of a post-course workplace assignment, submission of verification letter from supervisor and statement of authenticity.

**Note:** Units marked with an asterisk (\*) are required. Units marked with double asterisk (\*\*) are the required chosen electives.

## **PSP51804 Diploma of Government (Security)**

**Pre-requisite courses [usually *Certificate IV in Government (Security)* or *Certificate IV in Government (Personnel Security)*] and/or suitable workplace experience as a security practitioner in a government agency are required for entry into the Diploma of Government (Security).**

The Diploma of Government (Security) training program is made up of the following two Protective Security Training Centre courses:

- Five day Managing Protective Security course
- Five day Advanced Security Risk Management course

## **PSP51804 Diploma of Government (Security) program assessment strategy**

This qualification is achieved through completion of two course modules and a recognition phase. The components are as follows:

- Managing Protective Security (MPS) course
- Advanced Security Risk Management (ASRM) course
- in-class exercises, tests and presentations
- post-course workplace assignments (including verification letter from supervisor and statement of authenticity)
- Recognition of prior learning / assessment in the workplace.

## **Assignments**

You will be briefed during the courses on the assignments for the competencies of this qualification. It is important that you complete the assignment as soon as possible. You have three months to complete your assignment after each course. Extensions can be negotiated in special cases. Qualified assessors at the Protective Security Training Centre will assess post-course assignments.

## **Units of competency**

Units of competency contain a **competency field** that covers the following industry sectors. The **generalist** units of competency are: Ethics and Accountability (ETH); Working in Government (GOV); and Legislation and Compliance (LEGN). The **specialist** units of competency are: Government Security Management (SEC).

For some of the generalist units, it is expected that students will have completed in-house training in OHS, code of conduct, equity and diversity within their agency. Students will need to produce evidence of completion of training and/or produce a third party referee report as part of the recognition assessment. If this pre-requisite training has not been completed then arrangements can be made with the Protective Security Training Centre to complete some distance training and assessment for these units.

## Academic transcripts

Successful completion of each unit of competency is recorded in the Protective Security Training Centre student record system (VETtrak). An official Academic Transcript listing all successfully completed Units of Competency is provided with all awards (Certificate / Diploma). Even if you do not complete sufficient units to achieve a full qualification, you can request a Statement of Attainment for those units that you have successfully completed.

## How does Assessment by National Recognition work?

National Recognition as defined in the Australian Quality Training Framework (AQTF) provides for recognition in the national training system at three levels:

- (a) Recognition by a Registered Training Organisation (RTO) of the AQF qualifications and statements of attainment issued by all other RTOs, thereby enabling national recognition of the qualification and statements of attainment issued to any person.
- (b) Recognition by each state and territory's registering body of the training organisations registered by any other state or territory's registering body and of its registration decisions.
- (c) Recognition by all state and territory course-accrediting bodies and registering bodies of all courses accredited by each state or territory's course-accrediting body and of its accredited decisions.

There are two pathways to assessment in a competency based framework:

- Recognition of competency – portfolio based evidence
- Workplace assessment – assessment on the job

In a Recognition of Prior Learning (RPL) or assessment only pathway, the candidate provides current, quality evidence of their competency against the relevant units of competency.

## Evidence to support your assessment

Using the portfolio pathway, you gather evidence from past and present workplace experiences or by engaging in development activities. Evidence plays a critical role in the assessment process. Assessment of evidence is a process of confirming you have achieved competency. The rules of evidence require that evidence used for assessment must be valid, authentic, consistent, sufficient, current and reliable. To be certain the final decision of competent / not yet competent is accurate, your evidence must be examined to ensure it meets the following six rules of evidence.

- 1 **Validity** – refers to the requirement that the evidence be relevant to the competencies being assessed and to current workplace practices.
- 2 **Authenticity** – evidence presented for assessment must be the candidate's own work.
- 3 **Consistency** – refers to the requirements that the portfolio shows a consistent standard over a period of time.
- 4 **Sufficient** – requires that there be sufficient recent evidence to cover all components of competency – task skills, task management skills, contingency skills and job/role environment skills – as well as to provide evidence of competent performance over time.

- 5 **Currency** – demands the assessor be confident that the candidate performs to the standard to demonstrate competency. This is based on performance at this time, so evidence must be provided from either the present or the very recent past.
- 6 **Reliability** – requires that the evidence has come from a reliable and verifiable source.

### Types of evidence

The following table summarises some types of evidence and examples of each. You need to provide several types of evidence for each unit of competency assessed or claimed to satisfy the assessor. You should discuss evidence required with your assessor.

Evidence Type	Explanation	Examples
Job experience	Details of work history and past and current job experience	Resume or Curriculum Vitae
Job duties	Details work responsibilities and the standard of performance of job tasks	Current and/or recent previous Job Descriptions or Duty Statements
Performance Management	Details standard and competence in the performance of job tasks	PPI, Performance Appraisals Reports, Performance Management Agreements
Work history	Documents that demonstrate completion of relevant workplace training and the capacity to apply the skills in the workplace	CV, current and/or previous Job Descriptions, membership of relevant professional associations, references/letters from previous employers or supervisors, industry awards.
Work product	Samples of work verified as authentic	Emails, memos, letters, reports etc
Third party reports	Report from a competent supervisor or colleague that confirms the candidate's level of knowledge and ability to apply skills in the workplace.	Reports from managers, supervisors and testimonials from clients
Accredited training program	<b>A qualification or statement of attainment including a transcript of units of competency awarded</b>	Statement of Attainment, Certificate or Diploma (Certified true copies or originals)
Other training programs	Documents that confirm attendance at a formal course of study	Non-accredited course or a University course

Evidence Type	Explanation	Examples
Interview / questioning / exams	Confirms the candidate's knowledge of the legislation policy and procedures that underpin the security assessing process	Responses to scenarios, knowledge of policy and processes
Workplace documents	Workplace documents that have been produced by the candidate that are relevant to his/her claim	Written communications
Practical demonstration	Observation by the assessor of the candidate actually performing the tasks in the workplace or in a simulated workplace environment	Conduct a simulated security assessing interview
Professional organisation memberships	Evidence of networks and continuous improvement and professional development	Membership of relevant professional associations

Your portfolio will be examined by an assessor, and if necessary, a subject matter expert (SME). The focus of the assessor will be *“can the candidate do this now?”* Additionally, the assessor will need to determine whether the evidence, as a whole, matches your claims. They will do this by comparing the documents with the competency standards. If there is something the assessor cannot reasonably infer from the evidence, they may request further documentary evidence be provided.

Although documentary evidence is the key to a portfolio assessment, you may also need to meet with the assessor. This provides an opportunity for you to expand the evidence you have presented and for the assessor and/or SME to be satisfied that the evidence provided meets the rules of evidence. You will usually be asked *“what if ...”* type questions by the assessor, so they can be sure you are able to apply your skills and knowledge to real life situations.

### What to expect when compiling your evidence

The length of a recognition process will vary depending on a number of factors, such as what is being assessed, the strategies being used to gather evidence, how many tasks you are being assessed against, the type of evidence you present, the availability of assessors and/or subject matter experts, etc.

During the course, an assessor will provide you with information about:

- the assessment strategy and recognition process;
- what is required in completing your Recognition Assessment Workbook, and
- the most appropriate way(s) of gathering evidence.

You will also be advised of the timeframe for compiling your evidence and submitting your portfolio for assessment.

As part of the assessment of the evidence provided in your portfolio, the recognition process may involve a follow-up meeting with the assessor and/or you may be

required to provide additional evidence to support your claims. You will be advised by an assessor if this is necessary.

### **Who will have access to my portfolio?**

In accordance with the AQTF standards for RTOs, the Protective Security Training Centre confirms your portfolio will be treated in confidence and only shown to individuals who have a genuine need to see the portfolio in order to conduct the assessment. Where you feel the need to use sensitive documents as evidence, it is recommended that you discuss this with the Protective Security Training Centre before you submit your portfolio of evidence.

### **Complaints and appeals**

Staff take complaints and appeals seriously and every effort will be made to resolve identified problems in a timely manner. If you have a complaint, in the first instance you should speak to your assessor who will endeavour to rectify the issue. If your issue concerns the workplace assessor and you feel uncomfortable speaking with the assessor contact another assessor or the Assistant Director: Training and Development. If your complaint is unresolved at this level, please refer the issue to the Training Centre Director who if unable to resolve the issue will arrange a panel or independent person to hear the complaint.

An independent person may be another officer of the Attorney General's Department removed from the Protective Security Training Centre, or a member of the Australian Public Service Commission (APSC). You may also choose to have an independent person with you for any hearing of the complaint. This person can be anyone of your choosing. For example: work colleague or another other course participant. Candidates will receive a written statement of the outcome of the complaint or appeal.

### **Student Handbook**

You should carefully read your rights and responsibilities outlined in the Student Handbook. This document is provided with the course joining instructions and can also be downloaded from:

<http://www.ag.gov.au/pstc>

## **Where to get help**

You will complete an initial session with a Protective Security Training Centre Assessor at which time you should ask questions if you are unsure of the process. Also, feel free to call the Protective Security Training Centre at any time if you are having difficulties.

The contact details are as follows:

**Telephone number for general enquires and course registrations:** (02) 6141 3699

**Telephone number for Recognition enquiries:** (02) 6141 3678

**Email address for Recognition enquiries:** [rpl.pstc@ag.gov.au](mailto:rpl.pstc@ag.gov.au)

### **Physical Address:**

#### **Protective Security Training Centre**

Kenneth Bailey Building  
71 State Circle  
YARRALUMLA ACT 2600

### **Postal Address:**

#### **Assistant Director, Training and Development**

Protective Security Training Centre  
Attorney-General's Department  
3 - 5 National Circuit  
BARTON ACT 2600

## Part 1: Candidate's personal details

1 Personal Details		
Last Name		
First Name		
Preferred Name		
Preferred Title (Mr, Mrs, Ms, Miss)		
Home Address		
Postal address if different from above		
Telephone Numbers	Home:	Work:
	Mobile:	Fax:
Date of Birth	/ /	
Gender	MALE <input type="checkbox"/> / FEMALE <input type="checkbox"/>	
Are you a permanent Resident of Australia	YES <input type="checkbox"/> / NO <input type="checkbox"/>	
2 Current Employment		
Are you currently employed?	YES <input type="checkbox"/> / NO <input type="checkbox"/>	
If Yes, in which occupation are you currently employed?	.....	
Who is your current employer/supervisor?	.....	
<b>Job Title</b>	.....	
3 Armed Forces details (If Applicable)		
Branch of Service		
Trade classification on discharge		
4 Further Training		
Have you undertaken any training courses related to the occupation and qualification?	YES <input type="checkbox"/> / NO <input type="checkbox"/>	
<b>If Yes</b>		
What occupation were you trained in?		
Training completion Date (month, year)		
Country where you trained		

Name of course and Institution (if applicable)	
<b>5 Is there any further information you wish to give in support of your application</b>	
<b>6 Professional Referees (relevant to work situation)</b>	
Name Position Organisation Phone Number Mobile Number Email Address	..... ..... ..... ..... ..... .....
Name Position Organisation Phone Number Mobile Number Email Address	..... ..... ..... ..... ..... .....

Part 2: Candidate's employment history

Name, Address and Phone number of Employer Organisation	Period of Employment (DD/MM/YYYY)		Position Held	Full Time Part-time Casual	Description of Major Duties
	From	To			
1					
2					
3					
4					

***Attach additional sheet if required***

If you are including documents in your application, please provide a brief description below:

**List of Candidate's Portfolio Attachments (documentary evidence):**  
**(For example, resume, photos, awards, PM KEYs record etc)**

- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
-

### Part 3: Candidate's self-assessment summary

Unit of competency	I have performed these tasks (please tick)		
	Frequently	Sometimes	Never
PSPETHC501B - Promote the values and ethos of public service*			
PSPGOV505A – Promote diversity*			
PSPGOV413A – Compose complex workplace documents**			
PSPGOV504B – Undertake research and analysis*			
PSPSEC501A – Assess security risks*			
PSPSEC502A – Develop security risk management plans*			
PSPSEC503A – Implement and monitor security risk management plans*			
PSPLEGN501B – Promote compliance with legislation in the public sector*			
PSPGOV512A – Use complex workplace communication strategies*			
PSPSEC504A – Coordinate protective security*			
PSPSEC505A – Protect security classified information**			
PSPSEC506A – Communicate security awareness**			

**Note:** Units marked with an asterisk (\*) are required. Units marked with double asterisk (\*\*) are the required chosen electives.

#### Candidate Declaration

I declare that the evidence detailed in the Recognition Workbook for the units of competency is true and correct and that the documents and statements supplied satisfy the rules of evidence for assessment.

**Candidate's Signature:** \_\_\_\_\_ **Date:** \_\_\_\_\_

#### Part 4: Third Party Referee reports – Diploma of Government (Security)

Third party reports can be completed by any member of staff who have worked with the candidate and can supply relevant examples of work performance. The referee needs to complete these attachments honestly and provide comments and examples that support and validate the candidate's claims. The person completing a third party report does not have to be an accredited workplace assessor. These are not statements of competence but are comments and examples of how the candidate conducts themselves in the workplace and therefore verifies the candidate's evidence of knowledge and skills.

These reports should include evidence of both knowledge and skills in regard to performance of the tasks in each of the units of competency. If the referee does not have first-hand knowledge please notate. The third party report should verify the statement of claims of the candidate against the units of competency and provide supporting examples.

**Check evidence guide for each unit, for the specific number of context examples required. Where possible both the candidate and the referee should include at least three brief examples in the comments section including the extent and currency of knowledge and skills. Information should also be included on any in-house courses, seminars or training completed by the candidate relating to each unit of competency.**

To be completed by the Third Party Referee after reading the above information and the supporting documents:

<b>Last Name of Candidate:</b>		<b>First Name of Candidate:</b>	
<b>Candidate's Organisation and Job Title:</b>			
<b>Last Name of Referee:</b>		<b>First Name of Referee:</b>	
<b>Referee's Organisation and Job Title:</b>			
<b>Referee's Contact Telephone No</b>			
<b>Referee's Contact Email</b>			
<b>Referee's Relationship to Candidate:</b>			
<b>Length of time the Referee has observed / supervised the Candidate:</b>			

#### Third Party Referee Declaration

I declare that I have read the supporting information and the candidate's claims against the units of competency. The comments I have supplied in the following unit of competency documents are true and correct and satisfy the rules of evidence for assessment.

**Third Party Referee's Signature:** \_\_\_\_\_ **Date:** \_\_\_\_\_

## Part 5: Units of competency

The following pages include the units of competency required to be assessed for the qualification: PSP51804 Diploma of Government (Security). For each unit there is a brief description of the unit and the elements for each unit (the essential outcomes of the unit) and performance criteria (the requirement for competent performance). Also included is a range statement (the context in which the unit of competency is carried out and a focus for assessment).

The information about the units comprising the qualification PSP51804 Diploma of Government (Security), is also detailed at the National Training Information Site (NTIS) website: <http://www.ntis.gov.au>

A summary of the employability skills developed through this qualification can be downloaded from: <http://employabilityskills.training.com.au/>

Candidates are required to complete the following forms for each competency. These forms are required to supplement the portfolio of evidence and to provide examples of the candidate's ability relating to the competency standards.

In compiling evidence, the candidate should detail evidence that confirms their:

- knowledge requirements of the unit
- skills requirements of the unit
- application of Employability Skills as they relate to the unit
- a range (3 or more) of contexts (or occasions, over time) to ensure the unit of competency is achieved and applied in different situations or environments.

A third party referee statement must also be obtained to validate the claims made by the candidate.

**Note: It is recommended that candidates keep a copy of the completed Recognition Assessment Workbook for their records.**

Additional information on generalist units can be located at the Australian Public Service Commission (APSC) website:

**Public Service Induction:** <http://www.apsc.gov.au/apsinduction/index.html>

**APS Values:** <http://www.apsc.gov.au/values/index.html>

**Legislation:** <http://www.apsc.gov.au/publications/legislation.htm>

**Employment Policy:** <http://www.apsc.gov.au/employmentpolicy/index.html>

**Code of Conduct:** <http://www.apsc.gov.au/conduct/index.html>

**Ethics:** [http://www.apsc.gov.au/ethics/introducing\\_the\\_eas.html](http://www.apsc.gov.au/ethics/introducing_the_eas.html)

Other sites that may be of interest regarding safety information include:

<http://www.actsafe.act.gov.au/business.cfm>

[http://www.comcare.gov.au/virtual\\_workplaces/virtual\\_office/reception](http://www.comcare.gov.au/virtual_workplaces/virtual_office/reception)

## PSPETHC501B – Promote the values and ethos public service

### Introduction

This is a required unit of competency in the PSP51804 Diploma of Government (Security) and covers the responsibility of those in public service to model and encourage in others the highest standards of ethical conduct. It includes promoting ethical standards, assisting staff to avoid conflicts of interest, and modelling and fostering integrity of conduct.

Being competent in this unit means being able to:

### Promote ethical standards

This element requires:

- Interpretation of ethical standards is discussed with senior staff to ensure common understanding of requirements
- The ethical obligations of public service and the **consequences of unethical conduct** are explained to others in a manner suited to their levels of understanding, experience and specific needs
- Conduct of self and others is assessed against **ethics standards, legislation and guidelines**, and feedback or assistance is timely, constructive, and consistent
- Impartial, culturally and politically neutral advice is provided in accordance with organisational procedures
- Resolution and/or **referral of ethical problems** identified in dealings with staff and the public are used as learning opportunities within the workgroup without compromising privacy and confidentiality considerations

### Assist staff to avoid conflicts of interest

This element requires:

- **Conflict of interest** requirements are explained to staff using language and supporting material suitable to their needs and the situations they are likely to experience
- Matters involving competing interests or conflicting views on appropriate action are discussed with staff, and resolved or referred in accordance with policy and guidelines

### Model and foster integrity of conduct

This element requires:

- Personal work practices are used to provide a consistent example of desired ethical conduct, and staff/team values are developed through collaboration and leadership
- Ethical, lawful and reasonable directions are provided to staff, and protection is provided from reprisals for refusing others' directions to act unethically

- The **principles of procedural fairness** are modelled and explained to others using strategies and language suited to their levels of understanding, experience and specific needs
- Decision making which upholds ethical standards is used, promoted and explained to others
- The risk of **unethical conduct** is assessed in accordance with organisational guidelines, and changes to policies or practices are recommended to improve outcomes
- The **reporting** of suspected unethical conduct is encouraged, dealt with in a confidential manner and acted on promptly, and in accordance with policy and procedures

### Range statement

The following information is taken from the Unit of Competency as outlined in the Public Sector Training Package (PSP04).

The range statement provides information about the context in which the unit of competency is carried out. The variables cater for differences between States and Territories and the Commonwealth, and between organisations and workplaces. They allow for different work requirements, work practices and knowledge. The range statement also provides a focus for assessment. It relates to the unit as a whole. Text in italics in the Performance Criteria is explained here.

<b><i>Consequences of unethical behaviour may include</i></b>	<ul style="list-style-type: none"> <li>• disciplinary action</li> <li>• transfer</li> <li>• demotion</li> <li>• dismissal</li> <li>• legal liability</li> <li>• that outlined in legislation, policy and/or guidelines</li> </ul>
<b><i>Ethics standards may include</i></b>	<ul style="list-style-type: none"> <li>• public sector standards</li> <li>• standards referred to in State/Territory/Commonwealth legislation</li> <li>• codes of ethics</li> <li>• organisational codes of conduct</li> <li>• organisational mission and values statements</li> <li>• organisational procedures/guidelines</li> <li>• government policy</li> <li>• professional standards</li> </ul>
<b><i>Legislation and guidelines may include</i></b>	<ul style="list-style-type: none"> <li>• legislation for public sector management</li> <li>• freedom of information legislation</li> <li>• privacy legislation</li> <li>• equal employment opportunity and anti-discrimination law</li> <li>• public sector standards</li> <li>• equity guidelines</li> <li>• workplace diversity guidelines</li> <li>• Ministerial directions</li> <li>• State/Territory/Commonwealth codes of ethics</li> <li>• organisational codes of conduct</li> </ul>

	<ul style="list-style-type: none"> <li>• organisational mission and values statements</li> <li>• organisational policy, procedures/guidelines</li> <li>• government policy</li> <li>• legal precedents</li> </ul>
<b>Referrals of ethical problems</b> may be made to	<ul style="list-style-type: none"> <li>• line management</li> <li>• human resources</li> <li>• workplace relations officer</li> <li>• grievance officer</li> <li>• chief executive officer</li> <li>• public service commissioner</li> <li>• public sector standards body</li> <li>• organisational ethics committee</li> <li>• internal grievance mechanisms</li> <li>• confidant programs (whistleblower protection programs)</li> <li>• organisational professional reporting procedures</li> <li>• unions and professional bodies</li> <li>• ombudsman</li> </ul>
<b>Ethical problems which may need to be referred rather than resolved at this level</b> may include	<ul style="list-style-type: none"> <li>• conflict between public sector standards and personal values</li> <li>• conflict between public sector standards and other standards such as professional standards</li> <li>• conflict between public sector standards and directions of a senior officer or Minister</li> <li>• tension between two 'rights' for example, the right to privacy versus the right to freedom of information</li> <li>• conflict regarding issues of personal and organisational intellectual property</li> </ul>
<b>Conflicts of interest</b> may include	<ul style="list-style-type: none"> <li>• perceived, potential and actual conflicts</li> <li>• bribery</li> <li>• improper use of official information</li> <li>• offers of gifts, entertainment</li> <li>• outside employment</li> <li>• intellectual property</li> <li>• favours for friends, relatives and others</li> <li>• memberships of organisations</li> <li>• political activity</li> <li>• pecuniary and non-pecuniary conflicts</li> <li>• conflicts relating to tendering and contracting</li> </ul>
<b>Principles of procedural fairness</b> may include	<ul style="list-style-type: none"> <li>• the right to be heard/put your case</li> <li>• the right to be informed of a complaint or case against you</li> <li>• the right to be advised of the outcome/recommendations of an investigation involving you</li> <li>• the right to know reasons for decisions affecting you</li> <li>• the right to privacy</li> <li>• the right to representation</li> <li>• the right to remain silent</li> <li>• the decision maker should not be a judge in</li> </ul>

	<p>his/her own cause</p> <ul style="list-style-type: none"> <li>• in accordance with the law</li> </ul>
<p><b><i>Unethical conduct may include</i></b></p>	<ul style="list-style-type: none"> <li>• fraud, corruption, maladministration and waste</li> <li>• unauthorised access to and use of information, money/finances, vehicles, equipment, resources</li> <li>• improper public comment on matters relating to the government and/or the organisation</li> <li>• falsifying records</li> <li>• giving false testimonials</li> <li>• dishonesty</li> <li>• improper use of telephones, credit cards, frequent flyer points, email and Internet</li> <li>• extravagant or wasteful practices</li> <li>• personal favours, preferential treatment</li> <li>• putting barriers in place, hindering, blocking action</li> <li>• compromising behaviour including sexual harassment</li> <li>• directing others to act unethically</li> <li>• oppressive/coercive management decisions</li> <li>• resorting to illegality to obtain evidence</li> </ul>
<p><b><i>Actions relating to the reporting of unethical conduct may include</i></b></p>	<ul style="list-style-type: none"> <li>• protection and support of those reporting unethical conduct</li> <li>• informal, low key investigation and evidence gathering to confirm allegations</li> <li>• referral to authority identified in guidelines</li> <li>• use of confidant programs such as whistleblower protection programs or organisational professional reporting procedures</li> </ul>

## Evidence Guide

Evidence must be gathered over time in a range of contexts to ensure the person can achieve the unit outcome and apply the competency in different situations or environments.

In relation to unit PSPETHC501B, candidates should provide evidence that confirms promotion of the values and ethos of public service in a range of (3 or more) contexts (or occasions, over time) where contexts include generalist or specialist work activities such as developing client services, coordinating financial resources, providing human resource services, conducting investigations, letting contracts etc.

<b>Do you consistently meet your organisation's performance standards for:</b>			
<b>PSPETHC501B – Promote the values and ethos of public service (Required unit)</b>	<b>Yes</b>	<b>Not Yet</b>	<b>Not able to comment</b>
Promoting ethical standards			
Assisting staff to avoid conflicts of interest			
Modelling and fostering integrity of conduct			
<p><b>Candidate's Comments and Attachment/s number as included in Portfolio of Evidence:</b>  Agency in-house courses completed</p>			
<p><b>Referee Comments:</b></p> <p><i>I have read the candidate's recognition application and documentation. I support the claims of the candidate to have met the knowledge and skill requirements in performing the tasks in this unit of competency.</i></p> <p><b>Signature of Referee:</b> _____ <b>Date:</b> _____</p> <p><i>I agree with the statements above and that I have met the knowledge and skill requirements in this unit of competency.</i></p> <p><b>Signature of Candidate:</b> _____ <b>Date:</b> _____</p>			

## PSPGOV505A – Promote diversity

### Introduction

This is a required unit of competency in the PSP51804 Diploma of Government (Security) and covers the implementation of workplace diversity strategies to promote diversity through the development of effective and inclusive work practices, the generation of new ideas, and to improve the organisation's responsiveness to the community.

Being competent in this unit means being able to:

### Provide diversity input to strategies, policies and plans

This element requires:

- **Quantitative and qualitative workplace diversity data** is collected, **analysed**, and used for planning strategies, policies and plans to achieve a more diverse workforce
- Workplace **diversity** data is compared with data on the diversity of the organisation's client base and the community it serves to ensure strategies, policies and plans are responsive to all stakeholders
- Diversity strategies are developed in consultation with stakeholders, including people from key equity groups and clients
- **Effectiveness measures** are developed to evaluate the effectiveness and outcomes of workplace strategies, policies and plans in relation to diversity
- Actions to address the implementation of workplace diversity objectives are included in workplace business plans in accordance with organisational requirements
- Reporting and feedback processes are incorporated into strategies and plans in accordance with organisational policy and procedures

### Attract, develop and promote a diverse workforce

This element requires:

- Diversity principles are integrated with and underpin **human resources policies and practices** in the work area in accordance with the organisation's diversity strategy
- Strategies to increase the recruitment and retention of equity groups and others who don't fit the dominant organisational paradigm are promoted and implemented in the workplace in accordance with **legislation, policies and procedures**
- Barriers that prevent the recruitment, retention and progression of staff from diverse backgrounds are identified, and strategies developed to address them
- **Development opportunities** are identified and tailored to address the needs of a diverse workforce in accordance with diversity objectives and resourcing constraints
- Individuals with the capacity to operate in a variety of business and cultural settings are identified and **mentored** to maximise their contribution to the

organisation and its clients in accordance with organisational procedures and diversity objectives

- A harmonious and supportive work environment is created by valuing and promoting the **benefits of a diverse workforce** to those working within the business unit and/or the organisation in accordance with diversity objectives

### Monitor diversity outcomes

This element requires:

- **Employee data** and feedback from staff or **interviews** are evaluated to identify changes and trends in diversity outcomes for the work area
- Progress against workplace diversity effectiveness measures and policy/legal obligations is regularly monitored, outcomes reported and adjustments made to the diversity strategy or objectives in accordance with organisational procedures, to ensure its continued relevance and success

### Range statement

The following information is taken from the Unit of Competency as outlined in the Public Sector Training Package (PSP04).

The range statement provides information about the context in which the unit of competency is carried out. The variables cater for differences between States and Territories and the Commonwealth, and between organisations and workplaces. They allow for different work requirements, work practices and knowledge. The range statement also provides a focus for assessment. It relates to the unit as a whole. Text in italics in the Performance Criteria is explained here.

<p><b>Quantitative and qualitative workplace diversity data</b> may include</p>	<ul style="list-style-type: none"> <li>• distribution of equity groups by public sector level (number and proportion)</li> <li>• barriers to progress illustrated by drop in numbers above a certain level in the hierarchy</li> <li>• employment status</li> <li>• changes over time in employment status</li> <li>• comparison with client base</li> <li>• representation of equity groups at senior executive level</li> <li>• comparison with the rest of the public sector</li> </ul>
<p><b>Analysis of data</b> may include</p>	<ul style="list-style-type: none"> <li>• comparison with historical data</li> <li>• desegregation and cross-referencing of data on the basis of gender, disability, ethnicity and age (to identify inter-sectionality)</li> </ul>
<p><b>Diversity</b> may include</p>	<ul style="list-style-type: none"> <li>• age</li> <li>• cultural background</li> <li>• educational level</li> <li>• ethnicity</li> <li>• expertise</li> <li>• family responsibilities</li> <li>• gender</li> <li>• interests</li> <li>• interpersonal approach</li> </ul>

	<ul style="list-style-type: none"> <li>• language</li> <li>• life experience</li> <li>• marital status</li> <li>• not fitting the dominant paradigm of the organisation</li> <li>• personality</li> <li>• physical ability</li> <li>• political orientation</li> <li>• religious belief</li> <li>• sexual orientation</li> <li>• socio-economic background</li> <li>• thinking/learning styles</li> <li>• work experience</li> <li>• working styles</li> </ul>
<b><i>Diversity effectiveness measures may include</i></b>	<ul style="list-style-type: none"> <li>• an increase in the proportion of equity group members in relation to the workforce as a whole</li> <li>• improved employment status</li> <li>• increased representation at higher salary levels</li> <li>• increased recruitment and retention of equity group members</li> <li>• removal of barriers to progression</li> <li>• reduction in complaints/grievances (eg harassment, racism)</li> <li>• reduction in requests for review of actions/grievances from equity group members</li> </ul>
<b><i>Human resource policies and practices may include</i></b>	<ul style="list-style-type: none"> <li>• planning</li> <li>• selection and recruitment</li> <li>• performance management</li> <li>• performance appraisal</li> <li>• training and development</li> <li>• occupational health and safety</li> <li>• workplace relations</li> <li>• anti-harassment strategies</li> <li>• diversity</li> <li>• workplace standards</li> </ul>
<b><i>Legislation, policies and procedures may include</i></b>	<ul style="list-style-type: none"> <li>• Commonwealth and State/Territory legislation addressing diversity issues for example: <ul style="list-style-type: none"> <li>• Racial Discrimination Act 1975</li> <li>• Sex Discrimination Act 1984</li> <li>• Disability Discrimination Act 1992</li> <li>• Workplace Relations Act 1996</li> <li>• Privacy Act 1988</li> <li>• Human Rights and Equal Opportunity Commission Act 1984</li> </ul> </li> <li>• public service/public sector management acts</li> <li>• organisational workplace diversity guidelines</li> <li>• national and international codes of practice and standards</li> <li>• the organisation's plans, strategies and policies relating to diversity</li> <li>• policies relating to language services</li> <li>• government policy mandating equal employment</li> </ul>

	<p>opportunity and/or workplace diversity requirements, such as:</p> <ul style="list-style-type: none"> <li>○ Managing diversity in the Western Australian public sector, August 1995</li> <li>○ Valuing cultural diversity, State of Victoria, 2002</li> <li>○ Public sector ethics/values/codes of conduct</li> <li>○ Public sector management standards (subordinate law)</li> <li>○ Commissioner's directions/instructions</li> <li>○ Community guidelines, policy and practices (such as those within Aboriginal and Torres Strait Islander communities)</li> </ul>
<b>Development opportunities may include</b>	<ul style="list-style-type: none"> <li>● mentoring</li> <li>● sponsorship</li> <li>● coaching</li> <li>● work trials</li> <li>● more challenging work</li> <li>● shadowing</li> <li>● demonstration</li> <li>● role modelling</li> <li>● acting opportunities</li> <li>● job rotation</li> <li>● formal study/training</li> <li>● scholarships</li> <li>● cadetships</li> <li>● self-accessed learning</li> </ul>
<b>Mentoring may include</b>	<ul style="list-style-type: none"> <li>● equity groups such as: <ul style="list-style-type: none"> <li>● women</li> <li>● people from culturally and linguistically diverse backgrounds</li> <li>● Aboriginal and Torres Strait Islander people</li> <li>● people with disabilities.</li> </ul> </li> <li>● current work skills development</li> <li>● literacy and numeracy development</li> <li>● personal development</li> <li>● career development</li> <li>● management talent development</li> </ul>
<b>Benefits of diversity may include</b>	<ul style="list-style-type: none"> <li>● improved client service – internal and external</li> <li>● improved service delivery</li> <li>● promotion of equity and fairness</li> <li>● improved access for clients from diverse backgrounds to government services and programs</li> <li>● improved relationship with the community</li> <li>● wider sources of recruitment</li> <li>● greater responsiveness to change</li> <li>● cultural enrichment/promotion of creativity</li> <li>● creation of a harmonious and supportive work environment</li> <li>● retention of staff</li> <li>● facilitation of attainment of organisation goals</li> </ul>

	<ul style="list-style-type: none"> <li>• increased skills and experience added to the workplace</li> <li>• a workforce representative of the client base</li> <li>• a balanced workforce in terms of age, gender, race and culture</li> </ul>
<b><i>Employee data may include</i></b>	<ul style="list-style-type: none"> <li>• employment status</li> <li>• position level</li> <li>• recruitment and retention patterns</li> <li>• take-up of training</li> <li>• flexible working arrangements</li> <li>• length of service</li> </ul>
<b><i>Interviews may include</i></b>	<ul style="list-style-type: none"> <li>• exit interviews</li> <li>• performance management interviews</li> <li>• grievances or complaints</li> <li>• manager interviews</li> </ul>

### **Evidence Guide**

Evidence must be gathered over time in a range of contexts to ensure the person can achieve the unit outcome and apply the competency in different situations or environments.

In relation to unit PSPGOV505A, candidates should provide evidence that confirms promotion of diversity in a range of (3 or more) contexts (or occasions, over time) such as promoting the values and ethos of public service, promoting compliance with legislation, providing leadership, developing client services, developing policy, coordinating career development.

**Do you consistently meet your organisation's performance standards for:**

<b>PSPGOV505A – Promote diversity (Required unit)</b>	<b>Yes</b>	<b>Not Yet</b>	<b>Not able to comment</b>
Providing input to strategies, policies and plans			
Attracting, developing and promoting a diverse workforce			
Monitoring diversity outcomes			

**Candidate's Comments and Attachment/s number as included in Portfolio of Evidence:**  
*Completes Agency in-house courses*

**Referee Comments:**

*I have read the candidate's recognition application and documentation. I support the claims of the candidate to have met the knowledge and skill requirements in performing the tasks in this unit of competency.*

**Signature of Referee:**

**Date:**

*I agree with the statements above and that I have met the knowledge and skill requirements in this unit of competency.*

**Signature of Candidate:**

**Date:**

## PSPGOV413A – Compose complex workplace documents

### Introduction

This is a required chosen elective unit of competency in the PSP51804 Diploma of Government (Security) and covers written communication involving the evaluation and composition of complex workplace documents. It includes interpreting and evaluating workplace information, composing complex written materials and editing

Being competent in this unit means being able to:

### Interpret and evaluate workplace information

This element requires:

- **Information** is sourced from inside and outside the organisation in accordance with organisational requirements and sources analysed for reliability
- Cultural context of the information is distinguished and used to aid in interpretation
- Information is analysed for relevance to own work and assistance is sought with interpretation of complex materials in accordance with organisational procedures
- Assumed prior knowledge underpinning workplace information is identified and additional information is gathered if necessary to allow interpretation
- Implications of information are passed on to relevant personnel in accordance with legislation, policy and procedures

### Compose complex written materials

This element requires:

- The **purpose**, objectives and format for the **materials** are determined in accordance with organisational requirements
- Information to inform the document is sourced, collated in a logical manner and assessed for relevance and inclusion
- **Content, structure and sequencing** of materials are determined in line with the purpose and intended audience
- Options/recommendations are considered for inclusion
- Possible impact on the target audience is assessed and potential criticism countered where necessary
- Written materials are composed, reviewed to confirm objectives, **organisational and legislative requirements** are met, and materials are submitted within required timeframes

### Edit written material

This element requires:

- Intent of the communication is confirmed
- Content is checked and proofread for grammar, spelling and punctuation

- Communication is assessed in light of the needs of the intended audience
- Recommendations for improvement are made if necessary and explained/recorded in a manner that provides a learning opportunity for the future
- Information is amended if required, and submitted for approval in accordance with organisational policy and procedures

<b>Range statement</b>
------------------------

The range statement provides information about the context in which the unit of competency is carried out. The variables cater for differences between States and Territories and the Commonwealth, and between organisations and workplaces. They allow for different work requirements, work practices and knowledge. The range statement also provides a focus for assessment. It relates to the unit as a whole. Text in italics in the Performance Criteria is explained here.

<b><i>Information for evaluation may include</i></b>	<ul style="list-style-type: none"> <li>● applications</li> <li>● briefing papers</li> <li>● discussion papers</li> <li>● expert opinion</li> <li>● literature</li> <li>● minutes</li> <li>● project briefs</li> <li>● reports</li> <li>● research</li> <li>● speeches</li> <li>● strategic and operational plans</li> <li>● submissions</li> <li>● web site information</li> </ul>
<b><i>Purpose may include</i></b>	<ul style="list-style-type: none"> <li>● to influence opinion</li> <li>● to report on achievement</li> <li>● to recommend options and corresponding actions</li> <li>● to meet regulatory requirements</li> <li>● to meet public sector reporting requirements</li> <li>● to develop policy</li> <li>● to document policy</li> <li>● to obtain funding</li> <li>● to provide briefing material</li> <li>● to provide or contribute to strategic planning</li> <li>● to respond to enquiries/complaints</li> </ul>
<b><i>Materials to be composed may include</i></b>	<ul style="list-style-type: none"> <li>● position papers</li> <li>● discussion papers</li> <li>● briefing materials</li> <li>● funding submissions</li> <li>● business cases</li> <li>● project briefs</li> <li>● reports</li> <li>● operational and other plans</li> </ul>
<b><i>Content, structure and sequencing may include</i></b>	<ul style="list-style-type: none"> <li>● facts and observations</li> <li>● case studies</li> <li>● critical analysis</li> <li>● opinion</li> </ul>

	<ul style="list-style-type: none"> <li>• creative ideas</li> <li>• recommendations and supporting arguments</li> <li>• anticipated arguments and rebuttals</li> <li>• conclusions</li> <li>• division into chapters or sections</li> <li>• tables of contents and indexes</li> <li>• glossaries</li> <li>• executive summary</li> <li>• précis</li> <li>• chronological structure</li> <li>• alphabetic structure</li> <li>• operating sequence</li> </ul>
<p><b><i>Organisational and legislative requirements may include</i></b></p>	<ul style="list-style-type: none"> <li>• use of plain English</li> <li>• style formats</li> <li>• acknowledgements</li> <li>• particular terminology to be used/not used:</li> <li>• acronyms and technical terms</li> <li>• bureaucratic language</li> <li>• abbreviations</li> <li>• requirements for minimising jargon in written materials</li> <li>• requirements for written material to take account of cultural, ethnic, religious or language differences, disabilities, etiquette</li> <li>• guidelines for illustrative items</li> <li>• standards for references, acknowledgements, citations, footnotes, endnotes, bibliographies</li> <li>• particular communication channels</li> <li>• State/Territory or Commonwealth legislation, regulations, policies, procedures and guidelines relating to the preparation and security of written information in the public sector, including freedom of information, copyright, privacy, confidentiality, equal employment opportunity, diversity, occupational health and safety</li> <li>• risk assessment</li> <li>• information security requirements</li> <li>• public sector standards</li> <li>• fraud control standards</li> <li>• codes of practice</li> <li>• codes of ethics</li> <li>• private or confidential materials</li> <li>• embargoed materials</li> <li>• security requirements</li> <li>• politically sensitive materials</li> <li>• security standards for government information</li> </ul>

<p><b>Information for evaluation</b> <i>may include</i></p>	<ul style="list-style-type: none"> <li>• applications</li> <li>• briefing papers</li> <li>• discussion papers</li> <li>• expert opinion</li> <li>• literature</li> <li>• minutes</li> <li>• project briefs</li> <li>• reports</li> <li>• research</li> <li>• speeches</li> <li>• strategic and operational plans</li> <li>• submissions</li> <li>• web site information</li> </ul>
---	--

### **Evidence Guide**

Evidence must be gathered over time in a range of contexts to ensure the person can achieve the unit outcome and apply the competency in different situations or environments.

In relation to unit PSPGOV413A, candidates should provide evidence that confirms advanced communication strategies used in a range of (3 or more) contexts (or occasions, over time).

**Do you consistently meet your organisation's performance standards for:**

PSPGOV413A – Compose complex workplace documents <b>(Required chosen elective unit)</b>	Yes	Not Yet	Not able to comment
Interpreting and evaluating workplace information			
Composing complex written materials			
Editing written material			

**Candidate's Comments and Attachment/s number as included in Portfolio of Evidence:**

**Referee Comments:**

*I have read the candidate's recognition application and documentation. I support the claims of the candidate to have met the knowledge and skill requirements in performing the tasks in this unit of competency.*

**Signature of Referee:**

**Date:**

*I agree with the statements above and that I have met the knowledge and skill requirements in this unit of competency.*

**Signature of Candidate:**

**Date:**

## PSPGOV504B – Undertake research and analysis

### Introduction

This is a required unit of competency in the PSP51804 Diploma of Government (Security) and covers research and analysis to develop advice and recommendations. It includes identifying and undertaking research, analysing information and applying the results of analysis, maintaining information systems, and compiling reports from information.

Being competent in this unit means being able to:

### Identify and undertake research

This element requires:

- Information needs are defined based on work objectives and client and organisation requirements
- Potential **sources of information** and the **format** in which they are presented are evaluated and selected in line with the purpose and audience for the research
- **Strategies** are developed to acquire required information in accordance with **legislation, policy and procedures**
- Information is researched in a timely and thorough way and within resource allocation
- Quantity, quality and relevance of initial search results are assessed and gaps filled using the same or adjusted research strategies
- The methods and outcomes of research, and the criteria used to make information decisions and choices are clearly communicated

### Analyse information and apply the results of analysis

This element requires:

- Information from various sources is examined, compared and evaluated for **content**, structure and logic
- Analytical techniques and processes are selected in line with defined objectives
- Information is collated, consolidated and **analysed** and outcomes are advised to senior staff in accordance with organisational policy and procedures
- Facts, issues, patterns, interrelationships and trends are identified through analysis in accordance with research aims
- Agreed project timelines are met, and the defined standards of the organisation are met for all work

### Maintain information systems

This element requires:

- **Information systems** are maintained, validated and reconciled so that data and system integrity are assured
- A range of standard and complex information systems and applications is maintained in accordance with organisation standards

- Information systems are reviewed and updated as necessary

### Compile reports from information systems

This element requires:

- The findings from analysing information are used to meet ***client/organisational needs and organisation standards***
- Content of reports is determined and organised in a manner that supports the purposes and format of the organisation and audience
- Reporting of results is sequenced logically, is concise and clear, and includes predictions, assumptions and constraints where relevant

### Range statement

The following information is taken from the Unit of Competency as outlined in the Public Sector Training Package (PSP04).

The range statement provides information about the context in which the unit of competency is carried out. The variables cater for differences between States and Territories and the Commonwealth, and between organisations and workplaces. They allow for different work requirements, work practices and knowledge. The range statement also provides a focus for assessment. It relates to the unit as a whole. Text in italics in the Performance Criteria is explained here.

<p><b><i>Sources of information may include</i></b></p>	<ul style="list-style-type: none"> <li>• organisation materials</li> <li>• client information</li> <li>• market trends</li> <li>• registries and file records</li> <li>• library materials</li> <li>• financial records</li> <li>• statistical information</li> <li>• personnel/human resource records</li> <li>• asset records</li> <li>• legislation</li> <li>• policies</li> </ul>
<p><b><i>Information format may include</i></b></p>	<ul style="list-style-type: none"> <li>• multimedia</li> <li>• database</li> <li>• web site</li> <li>• dataset</li> <li>• audio/visual</li> <li>• word processed documents</li> <li>• books</li> <li>• gazettes and other publications</li> <li>• reports</li> <li>• pivot tables</li> </ul>
<p><b><i>Strategies may include</i></b></p>	<ul style="list-style-type: none"> <li>• research plan</li> <li>• search strategy tailored to the information retrieval system selected:             <ul style="list-style-type: none"> <li>• using key concepts and terms</li> <li>• using classification schemes</li> <li>• using search engines</li> <li>• using analysis systems</li> </ul> </li> </ul>

	<ul style="list-style-type: none"> <li>• using data warehouse systems</li> <li>• using internal organisers such as indexes in books</li> </ul>
<b>Legislation, policy and procedures may include</b>	<ul style="list-style-type: none"> <li>• Commonwealth and State/Territory legislation, standards and guidelines especially relating to privacy, confidentiality, freedom of information, security, fraud control, copyright, intellectual property</li> <li>• government policy</li> <li>• public sector code of ethics</li> <li>• national standards</li> <li>• Australian standards such as records management, knowledge management, risk management</li> <li>• the organisation's policies and practices</li> <li>• organisational code of conduct</li> <li>• Internet etiquette (netiquette)</li> </ul>
<b>Evaluation of content may include</b>	<ul style="list-style-type: none"> <li>• reliability</li> <li>• validity</li> <li>• accuracy</li> <li>• authority</li> <li>• currency</li> <li>• point of view</li> <li>• bias</li> <li>• prejudice</li> <li>• deception</li> <li>• manipulation</li> <li>• supporting arguments</li> <li>• contradictions</li> <li>• different viewpoints</li> <li>• the cultural, physical or other context in which the information was created</li> <li>• the impact of context on interpretation of the information</li> <li>• comparison of new knowledge with prior knowledge</li> <li>• whether information contradicts or verifies information from other sources</li> </ul>
<b>Analysis may include</b>	<ul style="list-style-type: none"> <li>• application of statistical methods</li> <li>• mathematical calculations</li> <li>• critical analysis</li> <li>• problem solving</li> <li>• forecasting</li> </ul>
<b>Information systems may contain</b>	<ul style="list-style-type: none"> <li>• computers and networks</li> <li>• communication channels</li> <li>• records management guidelines</li> <li>• data</li> <li>• procedures</li> <li>• protocols</li> <li>• legislation, guidelines and awards</li> <li>• organisation, legal and policy materials</li> <li>• client information</li> </ul>

	<ul style="list-style-type: none"> <li>• market trends</li> <li>• registries and file records</li> <li>• library systems</li> <li>• financial records</li> <li>• basic statistical information</li> <li>• personnel records</li> </ul>
<b><i>Client/organisational needs may include</i></b>	<ul style="list-style-type: none"> <li>• provision of advice</li> <li>• input into policy development</li> <li>• solutions/options for action</li> <li>• forecasting</li> <li>• determining future outcomes</li> <li>• identifying strategies derived from analysis of information</li> </ul>

### **Evidence Guide**

Evidence must be gathered over time in a range of contexts to ensure the person can achieve the unit outcome and apply the competency in different situations or environments.

In relation to unit PSPGOV504B, candidates should provide evidence that confirms research and analysis undertaken in a range of (3 or more) contexts (or occasions, over time).

**Do you consistently meet your organisation's performance standards for:**

PSPGOV504B – Undertake research and analysis (Required unit)	Yes	Not Yet	Not able to comment
Identifying and undertaking research			
Analysing information and applying the results of analysis			
Maintaining information systems			
Compiling reports from information systems			

**Candidate's Comments and Attachment/s number as included in Portfolio of Evidence:**

**Referee Comments:**

*I have read the candidate's recognition application and documentation. I support the claims of the candidate to have met the knowledge and skill requirements in performing the tasks in this unit of competency.*

**Signature of Referee:**

**Date:**

*I agree with the statements above and that I have met the knowledge and skill requirements in this unit of competency.*

**Signature of Candidate:**

**Date:**

## PSPSEC501A – Assess security risks

### Introduction

This is a required unit of competency in the PSP51804 Diploma of Government (Security) and covers assessment of government security risks. It includes establishing the risk context, gathering and analysing information, identifying and analysing risks, and assessing and prioritising risks to underpin development of a security plan.

Being competent in this unit means being able to:

### Establish security risk context

This element requires:

- The scope of the risk assessment and its **strategic and organisational context** are identified in accordance with organisational requirements
- **Legislation, policies, procedures and guidelines** related to security risk management are identified and complied with
- **Stakeholders** are identified and their expectations and input are obtained in accordance with organisational policy and procedures
- **Security risk criteria** are identified in accordance with the organisation's security policy, **jurisdictional policies and legislation**
- A risk assessment **plan** is developed in accordance with organisational priorities, and endorsement is obtained

### Gather and analyse information

This element requires:

- Sources of **information** are identified and information is gathered in accordance with organisational policy and procedures
- Internal information including historical information is reviewed
- New information from internal/external sources is aggregated
- Information is contextualised to the organisational context
- Gaps in information are identified and addressed

### Identify security risks

This element requires:

- **Sources** of threat to the organisation's **resources** and functions are identified, and **threats/potential threats** are determined in accordance with organisational policy and procedures
- **Threat assessment** is conducted against organisational policies, procedures and guidelines
- Access to, availability of and procedures relating to resources/areas are analysed to determine risk **exposure**

- Risks are assessed using **risk assessment techniques** to suit the type and level of risk in accordance with organisational policy and procedures
- Risk potential is determined and risks are documented in accordance with organisational requirements

### Analyse security risks

This element requires:

- Potential **consequences** of risks/threats are analysed in light of potential damage to agency, including **critical lead time for recovery**
- Analysis techniques are used in accordance with organisational policy and procedures
- Intent, capability and opportunity for each risk/threat to occur are assessed
- Using all known information, **likelihood** of risks/threats occurring is assessed
- Current security countermeasures/treatment options are analysed to determine areas of vulnerability
- **Risk ratings** are determined and documented in agreed **format** using all known information

### Assess and prioritise security risks

This element requires:

- Stakeholders are consulted about acceptable/unacceptable risk levels
- **Acceptable/unacceptable** levels of risk are documented
- Identified risks are compared with security risk criteria to determine whether they are acceptable/unacceptable
- Identified risks are prioritised in accordance with security criteria
- Risks are documented in priority order in accordance with organisational policies, procedures and guidelines
- **Residual** risks are determined and documented in accordance with organisational policies, procedures and guidelines

### Range statement

The following information is taken from the Unit of Competency as outlined in the Public Sector Training Package (PSP04).

The range statement provides information about the context in which the unit of competency is carried out. The variables cater for differences between States and Territories and the Commonwealth, and between organisations and workplaces. They allow for different work requirements, work practices and knowledge. The range statement also provides a focus for assessment. It relates to the unit as a whole. Text in italics in the Performance Criteria is explained here.

<b>Strategic context may include</b>	<ul style="list-style-type: none"> <li>• the relationship between the organisation and the environment in which it operates</li> <li>• the organisation's functions:             <ul style="list-style-type: none"> <li>○ political</li> <li>○ operational</li> </ul> </li> </ul>
--------------------------------------	---

	<ul style="list-style-type: none"> <li>○ financial</li> <li>○ social</li> <li>○ legal</li> <li>○ commercial</li> <li>● the various stakeholders and clients</li> </ul>
<b>Organisational context</b> may include	<ul style="list-style-type: none"> <li>● the organisation, how it is organised, and its capabilities</li> <li>● any official resources, including physical areas and assets, that are vital to the operation of the organisation</li> <li>● key operational elements of the organisation</li> <li>● any major projects</li> </ul>
<b>Stakeholders</b> may include	<ul style="list-style-type: none"> <li>● supervisors</li> <li>● managers</li> <li>● other areas within the organisation</li> <li>● other organisations</li> <li>● government</li> <li>● third parties</li> </ul>
<b>Security risk criteria</b> may concern	<ul style="list-style-type: none"> <li>● vital functions and capabilities</li> <li>● the expectations of stakeholders and clients</li> <li>● the personal security of employees and clients</li> <li>● general expectations about confidentiality</li> <li>● the availability of the organisation's official resources</li> </ul>
<b>Jurisdictional policies and legislation relating to risk criteria</b> cover	<ul style="list-style-type: none"> <li>● expectations about the care and confidentiality of official information reflected in legislation such as Public Service Act 1999, Crimes Act 1914 and Criminal Code 1985</li> <li>● the availability of official information to the public (Freedom of Information Act 1982)</li> <li>● expectations about the collection, use and care of personal information (the Privacy Act 1988)</li> <li>● expectations about the well-being and personal security of staff (Occupational Health and Safety [Commonwealth Employment] Act 1991)</li> <li>● the measures and procedures agencies must adopt to protect official resources from fraud (Commonwealth fraud control policy)</li> <li>● the expectation that there will be a Commonwealth-wide system for providing appropriate protection to security classified information (Commonwealth protective security policy)</li> </ul>
<b>Risk assessment plan</b> will include	<ul style="list-style-type: none"> <li>● the strategic and organisational context of the agency (or organisation, area or project under review)</li> <li>● the scope and objectives of the review</li> <li>● information and resources required to complete the review</li> <li>● the security risk criteria</li> </ul>
<b>Information</b> may be	<ul style="list-style-type: none"> <li>● hardcopy</li> <li>● audio-visual</li> <li>● electronic</li> </ul>

<p><b>Sources of threat</b> may include</p>	<ul style="list-style-type: none"> <li>• people</li> <li>• systems</li> <li>• environmental</li> <li>• financial</li> <li>• natural</li> <li>• conflict</li> <li>• terrorism</li> <li>• political circumstances</li> <li>• internal</li> <li>• external</li> <li>• local</li> <li>• national</li> <li>• international</li> </ul>
<p><b>Resources</b> may be</p>	<ul style="list-style-type: none"> <li>• agency owned</li> <li>• contractor owned</li> <li>• hired</li> <li>• leased</li> <li>• owned by third parties</li> </ul>
<p><b>Threats/potential threats</b> may be</p>	<ul style="list-style-type: none"> <li>• internal</li> <li>• external</li> <li>• national</li> <li>• international</li> <li>• real</li> <li>• perceived</li> <li>• to: <ul style="list-style-type: none"> <li>○ people</li> <li>○ property</li> <li>○ information</li> <li>○ reputation</li> <li>○ criminal</li> <li>○ terrorist</li> </ul> </li> <li>• from foreign intelligence services</li> <li>• from commercial/industrial competitors</li> <li>• from malicious people</li> </ul>
<p><b>Threat assessment</b></p>	<ul style="list-style-type: none"> <li>• is used to provide information about people and events that may pose a risk to a particular resource or function</li> <li>• evaluates and discusses the likelihood of a threat being realised</li> <li>• determines the potential of a threat to actually cause harm</li> </ul>
<p><b>Risk exposure</b> is</p>	<ul style="list-style-type: none"> <li>• a measure of how open a resource is to harm, or</li> <li>• the potential of a resource to attract harm</li> </ul>
<p><b>Risk assessment techniques</b> may include</p>	<ul style="list-style-type: none"> <li>• qualitative and/or semi-quantitative and/or quantitative</li> <li>• brainstorming</li> <li>• focus groups</li> <li>• expert judgment</li> <li>• strengths, weaknesses, opportunities and threats (SWOT) analysis</li> <li>• analysis of risk registers and risk matrix</li> </ul>

	<ul style="list-style-type: none"> <li>• examination of available data such as audit results, incident reports</li> <li>• nomogram</li> <li>• scenario analysis</li> <li>• business continuity planning</li> </ul>
<b>Consequences</b> may include	<ul style="list-style-type: none"> <li>• degree of harm</li> <li>• who would be affected and how</li> <li>• how much disruption would occur</li> <li>• damage to: <ul style="list-style-type: none"> <li>• the organisation</li> <li>• other organisations</li> <li>• government</li> <li>• third parties</li> </ul> </li> <li>• critical lead time for recovery</li> </ul>
<b>Critical lead time for recovery</b> is	<ul style="list-style-type: none"> <li>• the period of time a function is compromised</li> <li>• critical if the function is vital to the organisation</li> </ul>
<b>Likelihood of risk</b> may be determined through analysis of	<ul style="list-style-type: none"> <li>• current controls to deter, detect or prevent harm</li> <li>• effectiveness of current controls</li> <li>• level of exposure</li> <li>• threat assessment</li> <li>• determination of threat source/s</li> <li>• competence/capability of threat source/s</li> <li>• opportunity for threat to occur</li> </ul>
<b>Risk ratings</b> may include	<ul style="list-style-type: none"> <li>• severe</li> <li>• high</li> <li>• major</li> <li>• significant</li> <li>• moderate</li> <li>• low</li> <li>• trivial</li> </ul>
<b>Format for risk documentation</b> may include	<ul style="list-style-type: none"> <li>• matrix</li> <li>• table</li> <li>• graphs</li> <li>• graphics</li> <li>• computer modelling</li> </ul>
<b>Acceptable risks</b> are	<ul style="list-style-type: none"> <li>• those which an organisation has determined have the least potential for harm</li> </ul>
<b>Unacceptable risks</b> are	<ul style="list-style-type: none"> <li>• those which an organisation has determined have the most potential for harm</li> </ul>
<b>Residual risks</b> are	<ul style="list-style-type: none"> <li>• those which cannot be treated but still need to be documented</li> </ul>

## Evidence Guide

Evidence must be gathered over time in a range of contexts to ensure the person can achieve the unit outcome and apply the competency in different situations or environments.

In relation to unit PSPSEC501A, candidates should provide evidence that confirms assessment of security risks in a range of (3 or more) contexts (or occasions, over time).

**Does you consistently meet your organisation's performance standards for:**

<b>PSPSEC501A – Assess security risks (Required unit)</b>	<b>Yes</b>	<b>Not Yet</b>	<b>Not able to comment</b>
Establishing security risk context			
Gathering and analysing information			
Identifying security risks			
Analysing security risks			
Assessing and prioritising security risks			

**Candidate's Comments and Attachment/s number as included in Portfolio of Evidence:**

**Referee Comments:**

*I have read the candidate's recognition application and documentation. I support the claims of the candidate to have met the knowledge and skill requirements in performing the tasks in this unit of competency.*

**Signature of Referee:**

**Date:**

*I agree with the statements above and that I have met the knowledge and skill requirements in this unit of competency.*

**Signature of Candidate:**

**Date:**

## PSPSEC502A – Develop security risk management plans

### Introduction

This is a required unit of competency in the PSP51804 Diploma of Government (Security) and covers planning to treat security risks through the development of a security risk management plan. It includes identifying security countermeasures and developing a formal security plan.

Being competent in this unit means being able to:

### Identify countermeasures

This element requires:

- Documented **risks/threats** are **reviewed** and management decisions on **acceptable** and **unacceptable** risks are confirmed
- **Treatment options/countermeasures** are determined that are consistent with organisational policies, procedures and guidelines to reduce the **likelihood** of occurrence or the **consequences** of the risk, or both
- Treatments include **continuity plans**, where appropriate, in accordance with organisational policy and procedures
- Treatments match the **level** and type of risk and the importance of the function or resource
- A **cost-benefit analysis** is conducted to determine cost-effective countermeasures
- **Stakeholders** are consulted on the cost-benefit analysis, and countermeasures are determined and submitted for decision/prioritising in accordance with organisational policy and procedures

### Develop security plan

This element requires:

- Security plan is prepared in accordance with organisational policy and procedures
- The plan contains explanatory information on the importance of security and the organisation's security objectives in achieving corporate and business objectives
- The plan summarises **threat assessments** undertaken, current **exposure** and current protective security arrangements
- The plan outlines security strategies for implementation of countermeasures, monitoring and evaluation
- The plan includes a timetable and security budget for implementation of countermeasures including how they will be implemented and by whom
- Security plan is submitted for approval and communicated to stakeholders in accordance with organisational policy and procedures

### Range statement

The following information is taken from the Unit of Competency as outlined in the Public Sector Training Package (PSP04).

The range statement provides information about the context in which the unit of competency is carried out. The variables cater for differences between States and Territories and the Commonwealth, and between organisations and workplaces. They allow for different work requirements, work practices and knowledge. The range statement also provides a focus for assessment. It relates to the unit as a whole. Text in italics in the Performance Criteria is explained here.

<b><i>Risks/threats may be</i></b>	<ul style="list-style-type: none"> <li>• internal</li> <li>• external</li> <li>• national</li> <li>• international</li> <li>• real</li> <li>• perceived</li> <li>• to: <ul style="list-style-type: none"> <li>○ people</li> <li>○ property</li> <li>○ information</li> <li>○ reputation</li> <li>○ criminal</li> <li>○ terrorist</li> </ul> </li> <li>• from foreign intelligence services</li> <li>• from commercial/industrial competitors</li> <li>• from malicious people</li> </ul>
<b><i>Risk review includes</i></b>	<ul style="list-style-type: none"> <li>• consideration of current and historical information</li> </ul>
<b><i>Acceptable risks are</i></b>	<ul style="list-style-type: none"> <li>• those which an organisation has determined have the least potential for harm</li> </ul>
<b><i>Unacceptable risks are</i></b>	<ul style="list-style-type: none"> <li>• those which an organisation has determined have the most potential for harm</li> </ul>
<b><i>Treatment options may include</i></b>	<ul style="list-style-type: none"> <li>• addition of security measures</li> <li>• reduction of security measures</li> <li>• avoiding the risk through change of practice</li> <li>• acceptance of residual risk</li> <li>• minimisation of harm through response mechanisms</li> <li>• accepting the risk</li> </ul>
<b><i>Countermeasures may include</i></b>	<ul style="list-style-type: none"> <li>• revision of agency security plan</li> <li>• upgrade of existing security</li> <li>• installation of new security measures</li> <li>• technical controls</li> <li>• training</li> <li>• personnel-oriented</li> <li>• information-oriented</li> <li>• property-oriented</li> <li>• reputation-oriented</li> </ul>
<b><i>Likelihood of risk may be determined through analysis of</i></b>	<ul style="list-style-type: none"> <li>• current controls to deter, detect or prevent harm</li> <li>• effectiveness of current controls</li> <li>• level of exposure</li> <li>• threat assessment</li> <li>• determination of threat source/s</li> <li>• competence/capability of threat source/s</li> <li>• opportunity for threat to occur</li> </ul>

<b>Consequences</b> may include	<ul style="list-style-type: none"> <li>• degree of harm</li> <li>• who would be affected and how</li> <li>• how much disruption would occur</li> <li>• damage to: <ul style="list-style-type: none"> <li>○ the organisation</li> <li>○ other organisations</li> <li>○ government</li> <li>○ third parties</li> </ul> </li> <li>• critical lead time for recovery: <ul style="list-style-type: none"> <li>○ the period of time a function is compromised</li> <li>○ critical if the function is vital to the organisation</li> </ul> </li> </ul>
<b>Continuity plans</b>	<ul style="list-style-type: none"> <li>• may lessen the adverse consequences of risk</li> <li>• provide a set of planned procedures that enable organisations to continue or recover services to the government and the public with minimal disruption over a given period, irrespective of the source of the disruption</li> </ul>
<b>Level of risk</b> may be	<ul style="list-style-type: none"> <li>• severe</li> <li>• high</li> <li>• major</li> <li>• significant</li> <li>• moderate</li> <li>• low</li> <li>• trivial</li> </ul>
<b>Cost-benefit analysis</b> may be against	<ul style="list-style-type: none"> <li>• existing requirements</li> <li>• future requirements</li> <li>• forecast requirements</li> </ul>
<b>Stakeholders</b> may include	<ul style="list-style-type: none"> <li>• supervisors</li> <li>• managers</li> <li>• other areas within the organisation</li> <li>• other organisations</li> <li>• government</li> <li>• third parties</li> <li>• workgroup</li> </ul>
<b>Threat assessment</b>	<ul style="list-style-type: none"> <li>• is used to provide information about people and events that may pose a threat to a particular resource or function</li> <li>• evaluates and discusses the likelihood of a threat being realised</li> <li>• determines the potential of a threat to actually cause harm</li> </ul>
<b>Risk exposure</b> is	<ul style="list-style-type: none"> <li>• a measure of how open a resource is to harm, or</li> <li>• the potential of a resource to attract harm</li> </ul>

### Evidence Guide

Evidence must be gathered over time in a range of contexts to ensure the person can achieve the unit outcome and apply the competency in different situations or environments.

In relation to unit PSPSEC502A, candidates should provide evidence that confirms security risk management plans developed in a range of (2 or more) contexts (or occasions, over time).

**Do you consistently meet your organisation's performance standards for:**

PSPSEC502A – Develop security risk management plans (Required unit)	Yes	Not Yet	Not able to comment
Identifying countermeasures			
Developing security plans			

**Candidate's Comments and Attachment/s number as included in Portfolio of Evidence:**

**Referee Comments:**

*I have read the candidate's recognition application and documentation. I support the claims of the candidate to have met the knowledge and skill requirements in performing the tasks in this unit of competency.*

**Signature of Referee:**

**Date:**

*I agree with the statements above and that I have met the knowledge and skill requirements in this unit of competency.*

**Signature of Candidate:**

**Date:**

## PSPSEC503A – Implement and monitor security risk management plans

### Introduction

This is a required unit of competency in the PSP51804 Diploma of Government (Security) and covers implementation and monitoring of security risk management plans. It includes implementing a security plan, monitoring the risk environment and evaluating the security plan.

Being competent in this unit means being able to:

### Implement security plan

This element requires:

- **Security risks** are treated/**countermeasures** are implemented in accordance with the security plan
- Security plan is implemented to meet timeframe and budgetary requirements
- Countermeasures are implemented in compliance with **legal requirements, government and organisational policy**
- **Residual risks** are documented and monitored

### Monitor the risk environment

This element requires:

- **Strategies** to monitor the risk environment are determined and documented
- Security risks, and the **type/s** and **source/s** of threats are monitored to detect changing circumstances that may alter risk management priorities
- **Monitoring** is conducted on a regular basis in accordance with organisational policy and procedures
- Changes to the organisation are monitored to identify circumstances where re-examination of the security environment becomes necessary
- Results of monitoring are documented and acted on

### Evaluate security plan

This element requires:

- **Risk treatments** are monitored to gauge whether they are being implemented properly and fully
- Treatments are evaluated against the objectives of the security plan to ensure they remain effective and/or necessary
- Feedback is obtained from **stakeholders** on the adequacy and need for current security measures affecting their work area
- Weaknesses in the security plan are identified and addressed in accordance with organisational policy and procedures
- Security plan is reviewed on an on-going basis, as a result of incidents, breaches, and changes in circumstances

- Security plan is updated in accordance with organisational policies, procedures and guidelines to reflect current circumstances

### Range statement

The following information is taken from the Unit of Competency as outlined in the Public Sector Training Package (PSP04).

The range statement provides information about the context in which the unit of competency is carried out. The variables cater for differences between States and Territories and the Commonwealth, and between organisations and workplaces. They allow for different work requirements, work practices and knowledge. The range statement also provides a focus for assessment. It relates to the unit as a whole. Text in italics in the Performance Criteria is explained here.

<p><b><i>Security risks may include</i></b></p>	<ul style="list-style-type: none"> <li>• internal</li> <li>• external</li> <li>• national</li> <li>• international</li> <li>• real</li> <li>• perceived</li> <li>• to: <ul style="list-style-type: none"> <li>○ people</li> <li>○ property</li> <li>○ information</li> <li>○ reputation</li> <li>○ criminal</li> <li>○ terrorist</li> </ul> </li> <li>• from foreign intelligence services</li> <li>• from commercial/industrial competitors</li> <li>• from malicious people</li> </ul>
<p><b><i>Countermeasures may include</i></b></p>	<ul style="list-style-type: none"> <li>• revision of agency security plan</li> <li>• upgrade of existing security</li> <li>• installation of new security measures</li> <li>• technical controls</li> <li>• training</li> <li>• personnel-oriented</li> <li>• information-oriented</li> <li>• property-oriented</li> <li>• reputation-oriented</li> </ul>
<p><b><i>Legal requirements, government and organisational policy may include</i></b></p>	<ul style="list-style-type: none"> <li>• Commonwealth and State/Territory legislation including equal employment opportunity, occupational health and safety, privacy and anti-discrimination law</li> <li>• access and equity</li> <li>• ethics and accountability</li> <li>• national and international codes of practice and standards</li> <li>• the organisation's policies and practices</li> <li>• government policy</li> <li>• codes of conduct/codes of ethics</li> <li>• Australian and New Zealand standards – Risk management AS/NZS 4360:1999</li> </ul>

	<ul style="list-style-type: none"> <li>• Security Guidelines for Australian Government IT Systems (ACSI 33)</li> <li>• Commonwealth Protective Security Manual</li> </ul>
<b>Residual risks are</b>	<ul style="list-style-type: none"> <li>• those that cannot be treated</li> </ul>
<b>Strategies may include</b>	<ul style="list-style-type: none"> <li>• audits</li> <li>• incident reporting mechanisms</li> <li>• technical controls</li> <li>• systems</li> <li>• rosters</li> <li>• access controls</li> <li>• training</li> </ul>
<b>Type of risk may include</b>	<ul style="list-style-type: none"> <li>• severe</li> <li>• high</li> <li>• major</li> <li>• significant</li> <li>• moderate</li> <li>• low</li> <li>• trivial</li> </ul>
<b>Sources of threats may include</b>	<ul style="list-style-type: none"> <li>• technical</li> <li>• actual events</li> <li>• political circumstances</li> <li>• human behaviour</li> <li>• environmental</li> <li>• conflict</li> <li>• terrorism</li> <li>• internal</li> <li>• external</li> <li>• local</li> <li>• national</li> <li>• international</li> </ul>
<b>Monitoring may include</b>	<ul style="list-style-type: none"> <li>• regular checking</li> <li>• critical observation</li> <li>• regular recording</li> <li>• information, such as threat assessments, from senior management</li> <li>• reports from business units on current security measures</li> <li>• identification of changes over time such as: <ul style="list-style-type: none"> <li>○ notification of major changes to business or corporate goals or plans</li> <li>○ notification of key projects</li> </ul> </li> </ul>
<b>Risk treatments may include</b>	<ul style="list-style-type: none"> <li>• addition of security measures</li> <li>• reduction of security measures</li> <li>• avoiding the risk through change of practice</li> <li>• acceptance of residual risk</li> <li>• minimisation of harm through response mechanisms</li> <li>• accepting the risk</li> </ul>
<b>Stakeholders may include</b>	<ul style="list-style-type: none"> <li>• supervisors</li> <li>• managers</li> <li>• other areas within the organisation</li> </ul>

	<ul style="list-style-type: none"><li>• other organisations</li><li>• government</li><li>• third parties</li><li>• external contractors</li></ul>
--	---

## **Evidence Guide**

Evidence must be gathered over time in a range of contexts to ensure the person can achieve the unit outcome and apply the competency in different situations or environments.

In relation to unit PSPSEC503A, candidates should provide evidence that confirms security risk management plans implemented and monitored in a range of (2 or more) contexts (or occasions, over time).

**Do you consistently meet your organisation's performance standards for:**

<b>PSPSEC503A – Implement and monitor security risk management plans (Required unit)</b>	<b>Yes</b>	<b>Not Yet</b>	<b>Not able to comment</b>
Implementing security plans			
Monitoring the risk environment			
Evaluating security plans			

**Candidate's Comments and Attachment/s number as included in Portfolio of Evidence:**

**Referee Comments:**

*I have read the candidate's recognition application and documentation. I support the claims of the candidate to have met the knowledge and skill requirements in performing the tasks in this unit of competency.*

**Signature of Referee:**

**Date:**

*I agree with the statements above and that I have met the knowledge and skill requirements in this unit of competency.*

**Signature of Candidate:**

**Date:**

## PSPLEGN501B – Promote compliance with legislation in the public sector

### Introduction

This is a required unit of competency in the PSP51804 Diploma of Government (Security) and covers promotion of compliance with legislation in the public sector. It includes modelling compliance with legislation and related public sector guidelines and procedures and encouraging and assisting others to comply.

Being competent in this unit means being able to:

### Model and encourage compliance with legislative requirements

This element requires:

- Personal work practices are used to provide a consistent model of compliance with current public sector **legislation and guidelines**
- Responses to staff enquiries about the legislative requirements of the workplace are provided in a timely, consistent and constructive manner
- The **consequences of non-compliance** relating to a range of legislation are explained to staff using language and materials suited to their levels of experience, learning styles and individual needs
- **Compliance strategies** are used to encourage compliance with legislation, policies and guidelines in accordance with the situation at hand

### Monitor compliance with legislative requirements

This element requires:

- Compliance with legislative requirements is monitored in accordance with organisational procedures
- Compliance issues are resolved or referred in accordance with organisational policy and procedures
- **Inadequacies in workplace procedures** which may contribute to non-compliance are raised promptly and addressed in accordance with organisational procedures
- Compliance with legislative requirements is reported on, in accordance with organisational policy and procedure

### Range statement

The following information is taken from the Unit of Competency as outlined in the Public Sector Training Package (PSP04).

The range statement provides information about the context in which the unit of competency is carried out. The variables cater for differences between States and Territories and the Commonwealth, and between organisations and workplaces. They allow for different work requirements, work practices and knowledge. The range statement also provides a focus for assessment. It relates to the unit as a whole. Text in italics in the Performance Criteria is explained here.

<p><b>Legislation and guidelines</b> <i>may include</i></p>	<ul style="list-style-type: none"> <li>• public sector standards: <ul style="list-style-type: none"> <li>○ codes of conduct/ethics</li> <li>○ guarantee of service</li> <li>○ legislated standards</li> <li>○ State/Territory/Commonwealth/organisational standards</li> <li>○ technical/industrial standards</li> <li>○ professional standards</li> <li>○ industry competency standards</li> <li>○ anti-corruption legislation</li> <li>○ whistleblowers' protection.</li> </ul> </li> <li>• public sector employment: <ul style="list-style-type: none"> <li>○ employee relations</li> <li>○ chief executive officer's instructions</li> <li>○ Commissioner's instructions</li> <li>○ public sector notices.</li> </ul> </li> <li>• workplace environment: <ul style="list-style-type: none"> <li>○ equal employment opportunity</li> <li>○ affirmative action</li> <li>○ workplace diversity</li> <li>○ anti-discrimination</li> <li>○ workplace harassment</li> <li>○ occupational health and safety</li> <li>○ duty of care</li> <li>○ security, storage, handling and classification of documents.</li> </ul> </li> <li>• financial management and accountability: <ul style="list-style-type: none"> <li>○ Treasurer's instructions</li> <li>○ contractual obligations.</li> </ul> </li> <li>• transparency: <ul style="list-style-type: none"> <li>○ freedom of information</li> <li>○ professional reporting</li> <li>○ accountability</li> <li>○ fair trading.</li> </ul> </li> <li>• business and community: <ul style="list-style-type: none"> <li>○ privacy</li> <li>○ trade practices</li> <li>○ competition</li> <li>○ road transport legislation.</li> </ul> </li> <li>• information and records management standards and legislation</li> <li>• the organisation's enabling legislation, regulations</li> <li>• aspects of common law, criminal law, contract law, employment law and administrative law, including judges' rules</li> <li>• international legislation/codes of behaviour</li> </ul>
<p><b>Consequences of non-compliance</b> <i>may include</i></p>	<ul style="list-style-type: none"> <li>• for individuals: <ul style="list-style-type: none"> <li>○ counselling</li> <li>○ disciplinary action</li> <li>○ transfer</li> <li>○ demotion</li> <li>○ dismissal</li> <li>○ legal liability</li> </ul> </li> </ul>

	<ul style="list-style-type: none"> <li>○ fine.</li> <li>● external consequences, for example: <ul style="list-style-type: none"> <li>○ to clients</li> <li>○ customer service</li> <li>○ to the organisation's reputation</li> </ul> </li> </ul>
<b><i>Compliance strategies may include</i></b>	<ul style="list-style-type: none"> <li>● education</li> <li>● mentoring</li> <li>● coaching</li> <li>● shadowing</li> <li>● supervision</li> <li>● taking disciplinary or legal action</li> </ul>
<b><i>Inadequacies in workplace procedures may include</i></b>	<ul style="list-style-type: none"> <li>● insufficient financial/other controls</li> <li>● insecure Internet/fax access</li> <li>● non-auditable records processes</li> <li>● ambiguous guidelines</li> <li>● no guidelines</li> <li>● unnecessary complexity</li> <li>● use of non-current legislation</li> </ul>

## Evidence Guide

Evidence must be gathered over time in a range of contexts to ensure the person can achieve the unit outcome and apply the competency in different situations or environments.

In relation to unit PSPLEGN501B, candidates should provide evidence that confirms compliance with legislation promoted in a range of (3 or more) contexts (or occasions, over time).

**Do you consistently meet your organisation's performance standards for:**

<b>PSPLEGN501B – Promote compliance with legislation in the public sector (Required unit)</b>	<b>Yes</b>	<b>Not Yet</b>	<b>Not able to comment</b>
Modelling and encouraging compliance with legislative requirements			
Monitoring compliance with legislative requirements			
Promoting compliance with PSM / Information Security Manual (previously ACSI 33)			

**Candidate's Comments and Attachment/s number as included in Portfolio of Evidence:**

**Referee Comments:**

*I have read the candidate's recognition application and documentation. I support the claims of the candidate to have met the knowledge and skill requirements in performing the tasks in this unit of competency.*

**Signature of Referee:**

**Date:**

*I agree with the statements above and that I have met the knowledge and skill requirements in this unit of competency.*

**Signature of Candidate:**

**Date:**

## PSPGOV512A – Use complex workplace communication strategies

### Introduction

This is a required unit of competency in the PSP51804 Diploma of Government (Security) and covers complex workplace communication for working at middle management level with internal and external clients, colleagues and other staff. It includes preparing for complex communication, analysing and responding to opinions, presenting a convincing argument, and developing a range of communication strategies.

Being competent in this unit means being able to:

### Prepare for complex communication

This element requires:

- **Communication objectives** are clarified, those to be **present** are confirmed and communication **mode** is identified
- Analysis is undertaken to anticipate the likely positions to be taken by those present on the matters under discussion
- Subject matter is researched/**organised**, key points to be conveyed are identified and recorded, and information to counter other positions is summarised
- Requirements of **legislation, policy and guidelines** relevant to the discussion are identified and incorporated

### Analyse and respond to opinions

This element requires:

- Discussion is evaluated to identify impartiality, bias or unsupported argument
- Points of view of other speakers are noted and information to counter opposing views is presented objectively in accordance with required position
- **Reaction** to speakers and their point of view is analysed to identify and manage emotional reactions and maintain objectivity
- Opposing/challenging views are examined for their value in achieving the same ends
- Active listening and questioning are used to clarify own understanding, challenge or justify other points of view

### Present a convincing argument

This element requires:

- **Communication approach** is chosen and used to suit the given audience
- Prepared position is asserted with conviction and purpose
- **Verbal and non-verbal behaviour** are adjusted to maintain listener interest if the audience is unresponsive
- Questions are used to elicit feedback and check audience understanding

- Audience questions and argument are responded to objectively, and answers are backed by reasoned explanation
- Agreement is negotiated where possible, concluding with a summary of agreed items

### Develop a range of communication strategies

This element requires:

- Feedback from others is obtained and the outcomes of communication are assessed
- Lessons learnt are recorded and used to underpin future interactions
- **Language structures and features** that influence audiences to a preferred point of view are developed and practised
- Communication strategies are explored and practised for a range of workplace applications in accordance with organisational requirements

### Range statement

The following information is taken from the Unit of Competency as outlined in the Public Sector Training Package (PSP04).

The range statement provides information about the context in which the unit of competency is carried out. The variables cater for differences between States and Territories and the Commonwealth, and between organisations and workplaces. They allow for different work requirements, work practices and knowledge. The range statement also provides a focus for assessment. It relates to the unit as a whole. Text in italics in the Performance Criteria is explained here.

<b>Communication objectives</b> <i>may be to</i>	<ul style="list-style-type: none"> <li>• share information</li> <li>• reach consensus</li> <li>• contribute to policy</li> <li>• represent the business unit's position/interests in internal negotiations</li> <li>• resolve differences</li> <li>• negotiate a joint position/compromise</li> <li>• build reputation (of self and organisation/business unit)</li> <li>• market services</li> </ul>
<b>Those to be present</b> <i>may include</i>	<ul style="list-style-type: none"> <li>• peers</li> <li>• colleagues</li> <li>• those senior or junior to the position</li> <li>• staff from other agencies</li> </ul>
<b>Mode of communication</b> <i>may include</i>	<ul style="list-style-type: none"> <li>• telephone</li> <li>• teleconference</li> <li>• video conference</li> <li>• Internet (online forums)</li> <li>• face-to-face</li> <li>• one-on-one, or in a group</li> <li>• forum, seminar or conference</li> </ul>
<b>Organisation of subject matter</b> <i>may include</i>	<ul style="list-style-type: none"> <li>• identifying features, advantages and benefits and aligning evidence/examples</li> </ul>

	<ul style="list-style-type: none"> <li>• anticipating likely disagreements and structuring material to address these</li> </ul>
<b>Legislation, policy and guidelines may include</b>	<ul style="list-style-type: none"> <li>• State/Territory and Commonwealth legislation, regulations, policies, guidelines and standards relating to exchange of information in the public sector, such as: <ul style="list-style-type: none"> <li>○ ethics and accountability guidelines/codes of practice</li> <li>○ information security standards</li> <li>○ principles of equal employment opportunity, equity and diversity</li> <li>○ freedom of information and privacy.</li> </ul> </li> <li>• intellectual property</li> <li>• fraud standards</li> <li>• professional liability</li> </ul>
<b>Reaction to speakers may include</b>	<ul style="list-style-type: none"> <li>• own reaction</li> <li>• others present</li> </ul>
<b>Communication approach may include</b>	<ul style="list-style-type: none"> <li>• catering to political sensitivities</li> <li>• working within government processes and operational frameworks</li> <li>• balancing debate and action</li> <li>• consideration of wider organisational/public sector issues</li> <li>• speaking with confidence</li> <li>• cultural, ethnic, diversity or equity considerations</li> <li>• consultative</li> <li>• collaborative</li> <li>• assertive</li> <li>• reasonable</li> <li>• humorous</li> </ul>
<b>Verbal and non-verbal behaviour may include</b>	<ul style="list-style-type: none"> <li>• inclusive language, ideas and information</li> <li>• congruent speech and body language</li> <li>• speaking with confidence</li> <li>• impartiality</li> <li>• responsiveness</li> <li>• drawing on different sources of information</li> </ul>
<b>Language structures and features may include</b>	<ul style="list-style-type: none"> <li>• use of metaphors and similes</li> <li>• use of analogy, imagery and other comparisons</li> <li>• use of passive voice</li> <li>• using personal names repeatedly to convey intimacy or sincerity</li> <li>• tone, style and point of view</li> </ul>

## **Evidence Guide**

Evidence must be gathered over time in a range of contexts to ensure the person can achieve the unit outcome and apply the competency in different situations or environments.

In relation to unit PSPGOV512A, candidates should provide evidence that confirms use of complex communication strategies in a range of (3 or more) contexts (or occasions, over time).



## PSPSEC504A – Coordinate protective security

### Introduction

This is a required unit of competency in the PSP51804 Diploma of Government (Security) and covers the requirements for those with day-to-day responsibility for performance of an organisation's protective security function. It includes providing advice and support to others, monitoring and coordinating security, and liaising with specialist security services.

Being competent in this unit means being able to:

### Provide security advice and support

This element requires:

- Assistance is provided to management to analyse the security environment and plan to counter potential **threats**
- Advice is provided to management on **physical** and **procedural** security measures in accordance with organisational circumstances
- Assistance is provided in the development of the organisation's security policy and procedures in consultation with management and staff
- Promotion as the first point of contact for security concerns and queries is undertaken within the organisation in accordance with organisational requirements
- Advice is provided on **security matters** in accordance with legislation and security **standards**

### Coordinate and monitor security

This element requires:

- Protective security arrangements are developed and implemented in conjunction with senior management to create and maintain a secure environment for official information and resources
- Devolved security measures are coordinated/overseen to ensure organisational standards are maintained in a cost-effective and consistent way
- The organisation's security procedures and systems are monitored in an ongoing manner and audited as required in accordance with the organisation's security policy and plan
- Monitoring is undertaken to ensure that employees and contractors are aware of their security responsibilities and obligations, and recommendations are prepared/actions are taken to address any gaps
- **Security incident** reports are reviewed and the implications are assessed for security risk, security procedures and security awareness training

## Access security specialists

This element requires:

- Contact between the organisation and external **security authorities/organisations** is coordinated in accordance with organisational policy and procedures
- Specialist security organisations are contacted for advice, technical assistance, learning and development to ensure compliance with jurisdictional and organisational security policies, procedures and standards
- Security incidents and **other security issues** are reported/referred to government security authorities in accordance with legislation and security standards

## Range statement

The following information is taken from the Unit of Competency as outlined in the Public Sector Training Package (PSP04).

The range statement provides information about the context in which the unit of competency is carried out. The variables cater for differences between States and Territories and the Commonwealth, and between organisations and workplaces. They allow for different work requirements, work practices and knowledge. The range statement also provides a focus for assessment. It relates to the unit as a whole. Text in italics in the Performance Criteria is explained here.

<i>Threats may be</i>	<ul style="list-style-type: none"> <li>• real or perceived</li> <li>• criminal</li> <li>• terrorist</li> <li>• from foreign intelligence services</li> <li>• from commercial/industrial competitors</li> <li>• from malicious people</li> <li>• to: <ul style="list-style-type: none"> <li>○ personnel</li> <li>○ information</li> <li>○ property</li> <li>○ reputation</li> </ul> </li> </ul>
<i>Physical security measures may include</i>	<ul style="list-style-type: none"> <li>• storage arrangements</li> <li>• access control</li> <li>• barriers and alarms</li> </ul>
<i>Procedural security measures may include</i>	<ul style="list-style-type: none"> <li>• use</li> <li>• classification</li> <li>• labelling</li> <li>• handling</li> <li>• transmission</li> <li>• restricted access</li> </ul>
<i>Security matters may include</i>	<ul style="list-style-type: none"> <li>• security incidents</li> <li>• personnel vetting</li> <li>• home-based work</li> <li>• conference security</li> <li>• classification of information</li> <li>• security clearances</li> </ul>
<i>Protective security</i>	<ul style="list-style-type: none"> <li>• fraud control policy</li> </ul>

<b>standards</b> may include those in	<ul style="list-style-type: none"> <li>• protective security policy</li> <li>• public service codes of conduct/ethics</li> <li>• legislation/regulations, such as: <ul style="list-style-type: none"> <li>○ public service Acts</li> <li>○ Crimes Act 1914 and Criminal Code 1985</li> <li>○ Freedom of Information Act 1982</li> <li>○ Privacy Act 1988</li> </ul> </li> </ul>
<b>Security incidents</b> may be	<ul style="list-style-type: none"> <li>• breaches</li> <li>• violations</li> <li>• contact</li> <li>• approach</li> <li>• intentional</li> <li>• unintentional</li> <li>• deliberate</li> </ul>
<b>Security authorities/organisations</b> may include	<ul style="list-style-type: none"> <li>• organisations contracted to provide security services</li> <li>• government authorities/organisations with a security mandate</li> </ul>
<b>Other security issues</b> may include	<ul style="list-style-type: none"> <li>• briefings for people preparing to serve overseas</li> <li>• national security clearances</li> <li>• security incidents</li> <li>• security investigations</li> </ul>

### **Evidence Guide**

Evidence must be gathered over time in a range of contexts to ensure the person can achieve the unit outcome and apply the competency in different situations or environments.

In relation to unit PSPSEC504A, candidates should provide evidence that confirms coordination of protective security in a range of (3 or more) contexts (or occasions, over time).

**Do you consistently meet your organisation's performance standards for:**

PSPSEC504A – Coordinate protective security (Required unit)	Yes	Not Yet	Not able to comment
Providing security advice and support			
Coordinating and monitoring security			
Accessing security specialists in line with organisational policy and procedures to gain advice and assistance as required			

**Candidate's Comments and Attachment/s number as included in Portfolio of Evidence:**

**Referee Comments:**

*I have read the candidate's recognition application and documentation. I support the claims of the candidate to have met the knowledge and skill requirements in performing the tasks in this unit of competency.*

**Signature of Referee:**

**Date:**

*I agree with the statements above and that I have met the knowledge and skill requirements in this unit of competency.*

**Signature of Candidate:**

**Date:**

## PSPSEC505A – Protect security classified information

### Introduction

This is a required chosen elective unit of competency in the PSP51804 Diploma of Government (Security) and covers the provision of advice and guidance to senior managers and staff on classifying information and determining clearances to ensure the protection of official information. It includes advising on classified information and improving information security.

Being competent in this unit means being able to:

### Advise on security classified information

This element requires:

- The combination of the 'need to know' principle with different levels of security clearance to protect official information, is explained to staff and contractors in accordance with organisational policy and procedures
- Guidance is provided on the type of **information** requiring security classification and the range of classification levels available in accordance with security **standards**
- Advice is provided on determining the necessity for security clearances and the level of access required in different situations
- Advice is provided in accordance with organisational policy and procedures on the eligibility and suitability of applicants for security clearances
- Advice is provided on **other security measures** to protect security classified information

### Improve information security

This element requires:

- Recipients of security classified information are encouraged to challenge any security classification they believe to be unnecessary or inaccurate
- Originators of security classified information are contacted to discuss re-classification or de-classification of information in accordance with organisational policy and procedures
- Advice is provided to senior management on the extent to which the organisation meets government standards for the protection of security classified information
- Recommendations for improvements to information security measures are made in accordance with organisational policy and procedures

### Range statement

The following information is taken from the Unit of Competency as outlined in the Public Sector Training Package (PSP04).

The range statement provides information about the context in which the unit of competency is carried out. The variables cater for differences between States and Territories and the Commonwealth, and between organisations and workplaces. They

allow for different work requirements, work practices and knowledge. The range statement also provides a focus for assessment. It relates to the unit as a whole. Text in italics in the Performance Criteria is explained here.

<b><i>Information may be</i></b>	<ul style="list-style-type: none"> <li>• hard copy</li> <li>• electronic</li> <li>• audio-visual</li> <li>• photographic</li> <li>• encrypted</li> <li>• national security information</li> <li>• non-national security information</li> <li>• classified by third parties</li> </ul>
<b><i>Standards may include those referred to in</i></b>	<ul style="list-style-type: none"> <li>• public service Acts</li> <li>• protective security policy</li> <li>• fraud control policy</li> <li>• Crimes Act 1914 and Criminal Code 1985</li> <li>• Freedom of Information Act 1982</li> <li>• Privacy Act 1988</li> <li>• occupational health and safety legislation</li> <li>• Australian standards such as Risk management AS/NZS 4360:1999</li> <li>• Security Guidelines for Australian Government IT Systems (ACSI 33)</li> <li>• Commonwealth Protective Security Manual</li> </ul>
<b><i>Other security measures may include</i></b>	<ul style="list-style-type: none"> <li>• correct filing</li> <li>• clean desk</li> <li>• quitting all electronic systems and networks</li> <li>• checking environment including: <ul style="list-style-type: none"> <li>• desks</li> <li>• whiteboards</li> <li>• waste bins</li> <li>• computer drives</li> <li>• containers</li> <li>• cabinets</li> <li>• safes</li> <li>• vaults</li> <li>• windows</li> <li>• doors</li> </ul> </li> <li>• safe carriage of keys</li> </ul>

### **Evidence Guide**

Evidence must be gathered over time in a range of contexts to ensure the person can achieve the unit outcome and apply the competency in different situations or environments.

In relation to unit PSPSEC505A, candidates should provide evidence that confirms protection of security classified information in a range of (3 or more) contexts (or occasions, over time).

<b>Do you consistently meet your organisation's performance standards for:</b>			
<b>PSPSEC505A – Protect security classified information (Required chosen elective unit)</b>	<b>Yes</b>	<b>Not Yet</b>	<b>Not able to comment</b>
Advising on security classified information			
Improving information security			
<b>Candidate's Comments and Attachment/s number as included in Portfolio of Evidence:</b>			
<b>Referee Comments:</b>			
<p><i>I have read the candidate's recognition application and documentation. I support the claims of the candidate to have met the knowledge and skill requirements in performing the tasks in this unit of competency.</i></p>			
<b>Signature of Referee:</b>		<b>Date:</b>	
<p><i>I agree with the statements above and that I have met the knowledge and skill requirements in this unit of competency.</i></p>			
<b>Signature of Candidate:</b>		<b>Date:</b>	

## PSPSEC506A – Communicate security awareness

### Introduction

This is a required chosen elective unit of competency in the PSP51804 Diploma of Government (Security) and covers security awareness raising to improve government security management. It includes planning and designing security awareness activities, promoting security management, developing and nurturing cooperative client relationships, conducting security activities and evaluating their success.

Being competent in this unit means being able to:

### Plan security awareness activities

This element requires:

- **Need** for activities is determined, taking into account identified client needs and feedback from clients and staff, and priorities are identified in the organisation's security plan
- Ideas for new or improved activities are initiated, gathered and assessed, taking into account the human, financial and physical resources required
- Approval for **security awareness activities** is obtained in accordance with organisational guidelines

### Design security awareness activities

This element requires:

- Individuals and groups are targeted, and formal and informal networks are established and used regularly as communication channels
- Precedents in security management are incorporated into security awareness activities
- Effective awareness/information presentations are implemented where required
- Security awareness activities are linked in an integrated and cohesive manner with organisational ethical and security management standards and guidelines, codes of conduct and include related aspects of corporate policy
- Security awareness activities are based on a knowledge of the organisation's corporate objectives, core business, the culture of the organisation and a knowledge of the organisation's client base

### Promote government security management

This element requires:

- Incidents and effects of non-compliance are publicised in accordance with organisational requirements
- **Information** to promote government security management is provided in line with audience needs

## Develop and nurture cooperative client relationships

This element requires:

- Expectations of clients and contractors are established and documented
- Opportunities for establishing contacts and **networks** with external and internal clients are anticipated in consultation with work colleagues and managers
- Changes in organisational focus are monitored for effects on organisation–client relationships and action is taken to inform clients of changes in accordance with organisational policy and procedures
- Feedback on organisational activities is obtained and reported within the organisation in accordance with policy and procedures
- Organisation’s security management philosophy, policy and procedures are imparted in a way which facilitates **stakeholder** understanding
- Where required, clients are advised when and how they should modify their practices to meet organisational standards

## Conduct security management activities

This element requires:

- Security management activities are planned and are feasible within existing resource and time constraints
- Intended outcomes are identified and are based on realistic expectations of the target audience
- Activities are varied, refined and adapted as indicated by audience response or by changes in the organisation’s security strategy and procedures
- Adult learning techniques are utilised
- Security awareness information is linked with codes of conduct and ethical and security management guidelines of the organisation, together with its broader corporate goals

## Evaluate success of awareness raising activities

This element requires:

- Security awareness activities are assessed against predetermined objectives
- Results of evaluation are documented and used as the basis for planning future activities
- Opportunities for new security awareness activities are identified and acted on as required
- Evidence, if any, is obtained of a *decrease* in the level of security breaches as a result of activities

## Range statement

The following information is taken from the Unit of Competency as outlined in the Public Sector Training Package (PSP04).

The range statement provides information about the context in which the unit of competency is carried out. The variables cater for differences between States and Territories and the Commonwealth, and between organisations and workplaces. They allow for different work requirements, work practices and knowledge. The range statement also provides a focus for assessment. It relates to the unit as a whole. Text in italics in the Performance Criteria is explained here.

<b><i>Needs analysis may include</i></b>	<ul style="list-style-type: none"> <li>• consultation with staff, clients, security management networks</li> </ul>
<b><i>Others may include</i></b>	<ul style="list-style-type: none"> <li>• colleagues</li> <li>• supervised staff</li> <li>• contractors</li> </ul>
<b><i>Security awareness raising activities may include</i></b>	<ul style="list-style-type: none"> <li>• formal training sessions</li> <li>• briefings</li> <li>• addressing industry groups</li> <li>• consulting groups</li> </ul>
<b><i>Information may include</i></b>	<ul style="list-style-type: none"> <li>• security guidelines</li> <li>• instructions</li> </ul>
<b><i>Means of information dissemination may include</i></b>	<ul style="list-style-type: none"> <li>• computer-based information</li> <li>• newsletters</li> <li>• written policy manuals and procedures</li> <li>• internal instructions and guidelines</li> <li>• videos, pamphlets, posters</li> <li>• case studies, hypothetical examples</li> <li>• staff orientation processes</li> <li>• training and awareness sessions</li> <li>• conferences and seminars</li> <li>• liaison meetings with clients and stakeholders</li> </ul>
<b><i>Networks may include</i></b>	<ul style="list-style-type: none"> <li>• contact with peers or colleagues in or outside own organisation</li> </ul>
<b><i>Stakeholders may include</i></b>	<ul style="list-style-type: none"> <li>• internal or external to the organisation</li> <li>• agency staff and senior management</li> <li>• contractors and consultants</li> <li>• other agencies</li> <li>• related program staff</li> <li>• client organisations</li> <li>• industry associations</li> <li>• law enforcement agencies</li> </ul>
<b><i>Decrease in security breaches may be as a result of</i></b>	<ul style="list-style-type: none"> <li>• awareness raising and training activities</li> <li>• communicating the organisation's attitude to ethical behaviour and security requirements</li> <li>• using administrative remedies</li> <li>• establishing accessible and confidential reporting channels</li> <li>• publicising agency security practices both within the agency and to clients of the agency</li> </ul>

## **Evidence Guide**

Evidence must be gathered over time in a range of contexts to ensure the person can achieve the unit outcome and apply the competency in different situations or environments.

In relation to unit PSPSEC506A, candidates should provide evidence that confirms communication of security awareness in a range of (3 or more) contexts.

**Do you consistently meet your organisation's performance standards for:**

<b>PSPSEC506A - Communicate security awareness (Required chosen elective unit)</b>	<b>Yes</b>	<b>Not Yet</b>	<b>Not able to comment</b>
Planning security awareness activities			
Designing security awareness activities			
Promoting government security management			
Developing and nurturing cooperative client relationships			
Conducting security management activities			
Evaluating the success of security awareness raising activities			

**Candidate's Comments and Attachment/s number as included in Portfolio of Evidence:**

**Referee Comments:**

*I have read the candidate's recognition application and documentation. I support the claims of the candidate to have met the knowledge and skill requirements in performing the tasks in this unit of competency.*

**Signature of Referee:** \_\_\_\_\_ **Date:** \_\_\_\_\_

*I agree with the statements above and that I have met the knowledge and skill requirements in this unit of competency.*

**Signature of Candidate:** \_\_\_\_\_ **Date:** \_\_\_\_\_

