



# Recognition Assessment Workbook

**PSP41604**

## Certificate IV in Government (Security)

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

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

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

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

\_\_\_\_\_

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

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

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



Registered Training Organisation

# 88101

(Version 1.1 February 2011)



## Table of Contents

Introduction .....	3
PSP41604 Certificate IV in Government (Security) program training strategy .....	4
PSP41604 Certificate IV in Government (Security) program assessment strategy.....	4
Assignments .....	4
Units of competency.....	5
Academic transcripts .....	5
How does Assessment by National Recognition work? .....	5
Evidence to support your assessment .....	6
Types of evidence .....	6
What to expect when compiling your evidence .....	8
Who will have access to my portfolio? .....	8
Complaints and appeals.....	8
Student Handbook.....	9
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 – Certificate IV in Government (Security) .....	14
Part 5: Units of competency .....	15
PSPETH401A – Uphold and support the values and principles of public service (Required)	20
PSPGOV402B – Deliver and monitor service to clients (Required).....	25
PSPGOV408A – Value Diversity (Required).....	30
PSPOHS301A – Contribute to workplace safety (Chosen required elective).....	34
PSPLEGN401A – Encourage compliance with legislation in the public sector (Required) ....	38
PSPGOV422A - Apply government processes (Required).....	42
PSPPOL404A – Support policy implementation (Required).....	45
PSPSEC405A – Handle security classified information (Required).....	49
PSPSEC403A – Develop and advise on government security procedures (Required).....	53
PSPSEC406A – Provide government security briefings (Chosen required elective) .....	56
PSPGOV405B – Provide input to change processes (Chosen required elective).....	61
PSPGOV406B – Gather and analyse information (Chosen required elective).....	65
PSPGOV412A – Use advanced workplace communication strategies (Required) .....	70
PSPREG413A – Undertake inspections and monitoring (Chosen required elective).....	77
PSPSEC401A – Undertake government security risk analysis (Required) .....	83
PSPSEC402A – Implement security risk treatments (Required) .....	88

## Introduction

Welcome to the PSP41604 Certificate IV in 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 Certificate IV in Government (Security) you will need to demonstrate your competency in at least 15 units of competency of which 11 units are required and 4 units are chosen electives. In the Protective Security Training Centre qualification you will obtain 16 units of competency.

Unit of competency	Assessment Strategy
PSPETHC401A - Uphold & support the values and principles of public service * PSPGOV402B - Deliver and monitor service to clients * PSPGOV408A - Value diversity * PSPOHS301A - Contribute to workplace safety **	Assessed by recognition of your knowledge and skills in the workplace and confirmed by third party referee reports. <i>(These units are usually covered in training conducted within government agencies. A special distance package will be made available for private sector candidates or those who have not done training through their agency.)</i>
PSPLEGN401A - Encourage compliance with legislation in the public sector* PSPGOV422A - Apply government processes * PSPPOL404A - Support policy implementation * PSPSEC405A - Handle security classified information *	Assessed by recognition of your knowledge and skills in the workplace and confirmed by third party referee reports.
PSPSEC403A - Develop and advise on government security procedures * PSPSEC406A - Provide government security briefings ** PSPGOV405B - Provide input to change processes ** PSPGOV406B - Gather and analyse information ** PSPGOV412A - Use advanced workplace communication strategies * PSPREG413A - Undertake inspections and monitoring **	Delivered through the Protective Security Practice course and partially assessed through submission of post course workplace assignment. Also assessed by recognition and confirmed by third party referee reports.

Unit of competency	Assessment Strategy
PSPSEC401A - Undertake government security risk analysis *  PSPSEC402A - Implement security risk treatments *	Delivered through the Introduction to Security Risk Management course and formally assessed through submission of post-course workplace assignment.

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

### **PSP41604 Certificate IV in Government (Security) program training strategy**

The Certificate IV in Government (Security) training program is made up of the following three Protective Security Training Centre courses:

- Two day Introduction to Protective Security course [from the underpinning qualification: Certificate III in Government (Security) – Government Security Stream]
- Two day Introduction to Security Risk Management course
- Five day Protective Security Practice course

### **PSP41604 Certificate IV in Government (Security) program assessment strategy**

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

- Introduction to Protective Security (IPS) course
- Introduction to Security Risk Management (ISRM) course
- Protective Security Practice (PSP) course
- in-class exercises, tests and presentations
- post-course workplace assignments
- Recognition / 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); Legislation and Compliance (LEGN); and Occupational Health and Safety (OHS). The **specialist** units of competency are: Policy (POL); Regulatory (REG); and 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 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 or 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

Evidence Type	Explanation	Examples
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 from previous employers/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 clients
Accredited training program	A qualification or statement of attainment including a transcript of units of competency awarded	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
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 chose 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, 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?	.....	
Job Title	.....	
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 3: Candidate's self-assessment summary

Unit of competency	I have performed these tasks (please tick)		
	Frequently	Sometimes	Never
PSPETHC401A - Uphold & support the values and principles of public service *			
PSPGOV402B - Deliver and monitor service to clients *			
PSPGOV408A - Value diversity *			
PSPOHS301A - Contribute to workplace safety **			
PSPLEGN401A - Encourage compliance with legislation in the public *			
PSPGOV422A - Apply government processes *			
PSPPOL404A - Support policy implementation *			
PSPSEC405A - Handle security classified information *			
PSPSEC403A - Develop and advise on government security procedures *			
PSPSEC406A - Provide government security briefings **			
PSPGOV405B - Provide input to change processes **			
PSPGOV406B - Gather and analyse information **			
PSPGOV412A - Use advanced workplace communication strategies *			
PSPREG413A - Undertake inspections and monitoring **			
PSPSEC401A - Undertake government security risk analysis *			
PSPSEC402A - Implement security risk treatments *			

### 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 – Certificate IV in 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 all units of competency required to be assessed for the qualification PSP41604 Certificate IV in 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).

Candidates are required to complete the form attached to each competency. This form is required to supplement the portfolio of evidence and to provide examples of the candidate's ability relating the standards.

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.**

For further information about the units comprising the qualification PSP41604 Certificate in Government (Security), please visit the following 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/>

Additional information on the 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>

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)

## PSPETHC401A - Uphold and support the values and principles of public service

### Introduction

This is a required unit of competency in the PSP41604 Certificate IV in Government (Security) and covers the ethical conduct required of those in public service and the responsibility to encourage ethical conduct in others – colleagues or supervised staff.

Being competent in this unit means being able to:

### Contribute to an ethical public sector workplace

This element requires:

- Information on the **ethical values and principles** of the workplace is accessed, its interpretation confirmed with others and applied accordingly
- Application of ethical values and principles is discussed with senior management and colleagues to ensure common understanding and application
- **Others** are assisted to access and use public sector ethics **legislation and guidelines** to ensure their work practices comply with requirements
- The differences between public sector ethics/values and personal beliefs/values are explained to others to encourage understanding and compliance
- Hypothetical work practices that would constitute **unethical conduct** are identified and discussed with work colleagues, and strategies to avoid or deal with them are identified in accordance with organisational policy and procedures

### Participate in ethical decision making

This element requires:

- Real and potential **ethical problems** are identified, and decision making processes are used to resolve or refer them in accordance with organisational policy and procedures
- Information is regularly accessed to ensure currency in ethical knowledge, and ethical judgment is developed through involvement in workplace discussions or ongoing professional development related to ethical standards and practices
- Other staff are supported as necessary to contribute to ethical discussions and problem solving to develop their ethical judgment
- Processes for preventing and reporting unethical conduct are used and others are assisted in their application

### 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>Ethical values and principles</i></b> <i>may include</i></p>	<ul style="list-style-type: none"> <li>• respect for the law</li> <li>• integrity</li> <li>• objectivity</li> <li>• accountability</li> <li>• honesty</li> <li>• openness</li> <li>• responsibility</li> <li>• impartiality</li> <li>• diligence</li> <li>• trustworthiness</li> <li>• confidentiality</li> <li>• respect for persons</li> <li>• responsible care</li> <li>• probity</li> <li>• economy and efficiency</li> <li>• natural justice/procedural fairness, that is:             <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 know reasons for decisions affecting you</li> <li>○ the right to know the outcomes/recommendations of an investigation involving you</li> <li>○ the right to privacy</li> <li>○ the right to representation</li> <li>○ the right to silence</li> <li>○ the decision maker should not be a judge in his/her own cause</li> </ul> </li> </ul>
<p><b><i>Others</i></b> <i>may include</i></p>	<ul style="list-style-type: none"> <li>• colleagues</li> <li>• supervised staff</li> <li>• contractors</li> </ul>
<p><b><i>Legislation and guidelines</i></b> <i>may include</i></p>	<ul style="list-style-type: none"> <li>• legislation for public sector management</li> <li>• freedom of information</li> <li>• privacy legislation</li> <li>• equal employment opportunity and anti-discrimination law</li> <li>• public sector standards</li> <li>• Ministerial directions</li> <li>• State/Territory/Commonwealth codes of ethics</li> <li>• organisational codes for conduct/ethics</li> <li>• organisational mission and values statements</li> <li>• organisational policy, procedures/guidelines</li> <li>• government policy</li> <li>• professional codes of ethics and conduct</li> <li>• equity guidelines, organisational workplace diversity guidelines</li> </ul>
<p><b><i>Unethical conduct</i></b> <i>may include</i></p>	<ul style="list-style-type: none"> <li>• fraud, corruption, maladministration and waste</li> <li>• unauthorised access to and/or use of information, money/finances, vehicles, equipment, resources, time</li> </ul>

	<ul style="list-style-type: none"> <li>• improper actions during contractual processes, such as release of intellectual property, infringing copyright, release of tender information, inappropriate disclosure during tender process</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 plant and equipment, credit cards, frequent flyer points, telephones, email and Internet</li> <li>• extravagant or wasteful practices</li> <li>• personal favours</li> <li>• preferential treatment</li> <li>• putting barriers in place, hindering, blocking action</li> <li>• compromising behaviour including sexual harassment</li> <li>• lack of confidentiality</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>Ethical problems</b> which may need to be referred rather than resolved at this level may include</p>	<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>
<p>Referrals of ethical problems may be made to</p>	<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>

## **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 PSPETH401A, candidates should provide evidence that confirms ethical conduct in a range of (3 or more) contexts (or occasions, over time) where contexts may be generalist or specialist work activities such as applying government processes, delivering and monitoring services to clients, using resources, conducting interviews, giving evidence, awarding contracts etc.

<b>Do you consistently meet your organisation's performance standards for:</b>			
<b>PSPETH401A – Uphold and support the values and principles of public service (Required)</b>	<b>Yes</b>	<b>Not Yet</b>	<b>Not able to comment</b>
Contributing to an ethical public sector workplace			
Participating in ethical decision making			
<b>Candidate's Comments and Attachment/s number as included in Portfolio of Evidence:</b>			
<b>Referee (Third party) 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>	

## PSPGOV402B - Deliver and monitor service to clients

### Introduction

This is a required unit of competency in the PSP41604 Certificate IV in Government (Security) and covers delivery and monitoring of service to clients that requires understanding of the needs of existing and new clients which influence service requirements.

Being competent in this unit means being able to:

### Identify and define clients

This element requires:

- **Client** information is used to identify services required
- **Specific** needs of clients are recognised and addressed in targeting client services
- Potential difficulties in providing **client services** are identified and addressed or referred for recommended action

### Deliver client services

This element requires:

- Responses to client enquiries are made in accordance with **legislation, policy and procedures**
- **Service delivery** is provided that is appropriate, timely and accurately targeted
- **Communication** with clients is tailored to the situation and their specific needs
- **Negotiation**/conflict resolution techniques are used to resolve difficult situations or referrals are made in accordance with organisational policy and procedures
- Remedial actions are undertaken or recommended for clients with specific needs or in potential areas of difficulty
- **Accountability requirements** are identified and used, including organisation client service charter and/or external *review*

### Monitor and improve client services

This element requires:

- Client service delivery is monitored and regular feedback from colleagues is used to improve personal service
- Feedback is provided to workgroup members in regard to quality of client service delivery
- Changes in policies and procedures that impact upon client relations are conveyed to clients in a timely manner in accordance with organisational policy and procedures
- **Assistance** is accessed to assist in dealing with client service issues, meeting changing needs and achieving service potential

## Review client services

This element requires:

- Client feedback about service is sought and responded to
- Procedural aspects of service delivery are monitored and records are maintained as appropriate
- Proposals for change are based on feedback on service development and delivery
- Modifications to client service are carried out where required, within area of responsibility and limits imposed by government

## Range statement

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>Clients</i></b> may include	<ul style="list-style-type: none"> <li>• individual members of the public</li> <li>• other agencies</li> <li>• community groups</li> <li>• other work areas in the organisation</li> <li>• individual members of the organisation</li> <li>• senior management</li> <li>• government</li> <li>• Minister</li> </ul>
<b><i>Specific needs</i></b> of clients may include	<ul style="list-style-type: none"> <li>• age</li> <li>• culture</li> <li>• disability</li> <li>• ethnicity</li> <li>• gender</li> <li>• language</li> <li>• literacy and numeracy</li> <li>• medical conditions</li> <li>• remote location</li> <li>• state of mind</li> </ul>
<b><i>Client services</i></b> may include	<ul style="list-style-type: none"> <li>• any services (or products) provided by the organisation to internal or external clients</li> </ul>
<b><i>Legislation, policy and procedures</i></b> may include	<ul style="list-style-type: none"> <li>• State/Territory and Commonwealth legislation and regulations such as: <ul style="list-style-type: none"> <li>○ organisational enabling legislation</li> <li>○ public sector management acts</li> <li>○ financial management acts</li> <li>○ privacy legislation</li> <li>○ equal employment opportunity, anti-discrimination and harassment legislation</li> <li>○ occupational health and safety legislation</li> <li>○ consumer legislation</li> <li>○ environment legislation</li> </ul> </li> <li>• risk management guidelines</li> <li>• ethics and accountability standards</li> </ul>

	<ul style="list-style-type: none"> <li>• public sector standards</li> <li>• fraud control standards</li> <li>• government security standards</li> <li>• organisational client service standards</li> <li>• client service charter</li> <li>• organisational policy, procedures and protocols</li> </ul>
<b>Service delivery</b> occurs within	<ul style="list-style-type: none"> <li>• protocols</li> <li>• duty of care responsibility</li> <li>• codes of conduct</li> <li>• framework of accountability</li> <li>• client service charter</li> </ul>
<b>Communication</b> techniques may include	<ul style="list-style-type: none"> <li>• active listening</li> <li>• using open and/or closed questions</li> <li>• speaking clearly and concisely</li> <li>• varying language and tone of voice to suit the audience and purpose</li> <li>• giving clients full attention</li> <li>• maintaining eye-contact when culturally appropriate (for face-to-face interactions)</li> <li>• using non-verbal communication (for face-to-face interactions) such as: <ul style="list-style-type: none"> <li>◦ body language</li> <li>◦ personal presentation</li> </ul> </li> <li>• using clear, legible writing</li> <li>• handling sensitive and confidential issues</li> </ul>
<b>Negotiation</b> may include	<ul style="list-style-type: none"> <li>• effective listening</li> <li>• questioning</li> <li>• constructive feedback</li> <li>• issues identification</li> <li>• exploring options</li> <li>• identifying areas of agreement</li> <li>• recording agreements</li> <li>• non-verbal as well as verbal communication</li> <li>• culturally appropriate strategies, language and non-verbal cues</li> </ul>
<b>Accountability requirements</b> may include	<ul style="list-style-type: none"> <li>• client service records</li> <li>• client feedback procedures</li> <li>• refund policy</li> <li>• grievance procedures</li> <li>• complaints register</li> </ul>
<b>Assistance</b> may include	<ul style="list-style-type: none"> <li>• advice</li> <li>• mentoring</li> <li>• coaching</li> <li>• training</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 PSPGOV402B, candidates should provide evidence that confirms client services were delivered and monitored in a range of (3 or more) contexts (or occasions, over time).



## PSPGOV408A - Value diversity

### Introduction

This is a required unit of competency in the PSP41604 Certificate IV in Government (Security) and covers promotion of the values of workplace diversity and the contribution it makes to effective work practices.

Being competent in this unit means being able to:

### Promote the benefits of diversity

This element requires:

- The **diversity** of the workgroup is analysed to identify the strengths and differences that benefit both staff and the organisation
- **Workplace diversity issues, benefits** and risks are explained to others using language and supporting material suitable to their needs and the situations they are likely to experience
- Diversity training and awareness programs are identified and **promoted** to encourage and support others to appreciate the benefits of diversity
- Opportunities for leadership in, and advocacy of, workplace diversity are identified and utilised within own area of responsibility.

### Contribute to diversity outcomes

This element requires:

- Currency is maintained in knowledge of diversity principles and practices that are applied in the workplace
- Others are assisted to access and use **legislation, policy and guidelines** to ensure work practices contribute to diversity benefits
- Development and use of a range of **communication styles** is modelled and fostered to respond to the diversity of the workplace and its clients
- Targeted responses to the needs of the organisation's diverse client group/s are identified and implemented in accordance with organisational policy and procedures
- Feedback on diversity policies, strategies and practices/services is provided to managers in accordance with organisational procedures.

### Range Statement

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>Diversity may include</i></b></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> <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>
<p><b><i>Workplace diversity issues may include</i></b></p>	<ul style="list-style-type: none"> <li>• equal employment opportunity issues such as:</li> <li>• direct and indirect discrimination – discriminatory systems and practices</li> <li>• harassment</li> <li>• racism</li> <li>• under-representation of equity groups in the public sector</li> <li>• employment of equity groups concentrated at lower levels in the public sector</li> <li>• women making up more than half of the public sector workforce but disproportionately represented at lower salary levels</li> <li>• barrier (or glass ceiling) that prevents equity group members progressing to higher salary levels</li> <li>• disproportionate representation of equity group members in non-permanent, casual or contract positions</li> <li>• inappropriate supervisory treatment of equity group members</li> <li>• culturally inappropriate workplaces</li> <li>• enabling access to buildings to people with a disability</li> <li>• making reasonable adjustment to work processes.</li> <li>• quality of service delivery to clients from diverse backgrounds</li> <li>• sidelining staff from diverse backgrounds to 'diversity roles' rather than the opportunity to</li> </ul>

	<p>pursue what interests them, or where they add most value</p> <ul style="list-style-type: none"> <li>• people from recognised diversity groups choosing not to be identified through usual statistical collection methods</li> <li>• workplace systems or practices that don't allow a balance between work and family responsibilities</li> <li>• inequitable access to acting opportunities, workplace training and development</li> <li>• questioning/disregarding the dominant paradigm of the organisation</li> <li>• inappropriate treatment of those who don't fit the dominant paradigm of the organisation</li> <li>• risks associated with diversity not managed</li> <li>• different values: <ul style="list-style-type: none"> <li>• uncertainty avoidance</li> <li>• collectivist/individualist</li> <li>• power/distance</li> <li>• masculine/feminine.</li> </ul> </li> <li>• resolving communication issues</li> <li>• developing cultural competence</li> <li>• negotiating commonalities</li> <li>• resolving conflict</li> <li>• negotiating difference.</li> </ul>
<b>Benefits of diversity</b> may include	<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</li> <li>• 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> <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>Promotion</b> of training and awareness programs may include	<ul style="list-style-type: none"> <li>• word of mouth</li> <li>• memos</li> <li>• emails</li> <li>• flyers</li> <li>• intranet.</li> </ul>
<b>Legislation, policy and guidelines</b> may include	<ul style="list-style-type: none"> <li>• Commonwealth and State/Territory legislation addressing diversity issues for example:</li> </ul>

	<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> <li>• Equal Opportunity for Women in the Workplace Act 1999.</li> <li>• public service/public sector management acts</li> <li>• workplace diversity guidelines/program</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 opportunity and/or workplace diversity requirements, such as: <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> </li> </ul>
<p><b>Communication styles</b> may include</p>	<ul style="list-style-type: none"> <li>• plain English</li> <li>• language in active rather than passive voice</li> <li>• simple sentence structure even though content may be complex</li> <li>• lack of jargon and acronyms</li> <li>• culturally appropriate body language</li> <li>• oral or written use of graphics and illustrations</li> <li>• use of colour</li> <li>• reader-friendly layout</li> <li>• effective paragraphing</li> <li>• different languages</li> <li>• interpreting and translating</li> <li>• use of different media eg online.</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 PSPGOV408A, candidates should provide evidence that confirms valuing diversity in a range of (3 or more) contexts (or occasions, over time) such as upholding and supporting public service values, providing input to change, contributing to policy development and implementation and administering contracts.

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

<b>PSPGOV408A – Value Diversity (Required)</b>	<b>Yes</b>	<b>Not Yet</b>	<b>Not able to comment</b>
Promoting the benefits of diversity			
Contributing to diversity outcomes			
<i>In-house training completed</i>			

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

**Referee (Third party) 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:**

## PSPOHS301A - Contribute to workplace safety

### Introduction

This is a chosen required elective unit of competency in the within the PSP41604 Certificate IV in Government (Security) and covers the competency to contribute to a safe workplace for self and others. It includes contributing to workplace safety arrangements, identifying hazards and controlling risks.

Being competent in this unit means being able to:

### Contribute to participative workplace safety arrangements

This element requires:

- Occupational health and safety **issues** are addressed/reported to **designated personnel** in accordance with workplace procedures and **occupational health and safety legislation**
- **Contributions** are made to participative workplace safety **arrangements** within organisational procedures and scope of responsibilities and competencies

### Identify hazards and control risks

This element requires:

- Existing and potential **hazards** in the work area are identified, dealt with and/or reported to designated personnel according to workplace procedures
- **Workplace procedures** and work instructions for **controlling risks** are identified and implemented
- Workplace procedures for dealing with accidents and **other hazardous events** are followed whenever necessary within scope of responsibilities and competencies
- Feedback on the effectiveness of safety procedures and risk control measures is provided to enable improvements to be made where necessary

### Range statement

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.

Occupational health and safety <b>issues</b> may include	<ul style="list-style-type: none"><li>• hazards relating to the physical environment</li><li>• workplace stress</li><li>• conflict</li><li>• bullying</li><li>• harassment</li></ul>
<b>Designated personnel</b> may include	<ul style="list-style-type: none"><li>• supervisors</li><li>• managers</li><li>• team leaders</li><li>• designated occupational health and safety officers</li></ul>

	<ul style="list-style-type: none"> <li>• health and safety representatives</li> <li>• other persons authorised or nominated by the enterprise or industry to: <ul style="list-style-type: none"> <li>○ perform specified work</li> <li>○ approve specified work</li> <li>○ inspect specified work</li> <li>○ direct specified work</li> </ul> </li> </ul>
<b>Occupational health and safety legislation</b> may include	<ul style="list-style-type: none"> <li>• State/Territory/Commonwealth occupational health and safety acts, regulations and codes of practice including, but not limited to: <ul style="list-style-type: none"> <li>○ regulations and codes of practice relating to hazards present in the workplace or industry</li> <li>○ general duty of care under occupational health and safety legislation and common law</li> <li>○ provisions relating to roles and responsibilities of health and safety representatives and/or occupational health and safety committees</li> <li>○ provisions relating to occupational health and safety issue resolution</li> </ul> </li> </ul>
<b>Contributions</b> may include	<ul style="list-style-type: none"> <li>• identifying and reporting hazards and their associated risks</li> <li>• identifying safety issues and hazards that can be addressed immediately and taking action in accordance with safety procedures</li> <li>• reporting on effectiveness of safety procedures and risk controls</li> <li>• suggesting improvements to procedures and controls</li> <li>• listening to the ideas and opinions of others in the workplace</li> <li>• sharing opinions, views, knowledge and skills</li> </ul>
Participative workplace safety <b>arrangements</b> may include	<ul style="list-style-type: none"> <li>• formal and informal health and safety meetings</li> <li>• health and safety committees</li> <li>• other committees, for example, consultative, planning and purchasing</li> <li>• meetings called by health and safety representatives</li> <li>• suggestions, requests, reports and concerns put forward to management</li> </ul>
<b>Hazard identification</b> may include	<ul style="list-style-type: none"> <li>• checking equipment or the work station and work area before work commences and during work</li> <li>• workplace inspections</li> <li>• responding to physical cues that ergonomics are ineffective and need adjustment</li> <li>• on-the-job housekeeping checks (spills, furniture out of place, loose hand rails, curling mats, frayed cords, etc)</li> <li>• anticipation of potential hazards</li> </ul>
<b>Workplace procedures</b> may include	<ul style="list-style-type: none"> <li>• complying with workplace occupational health and safety symbols and signs</li> <li>• hazard reporting procedures</li> <li>• job procedures, safe work instructions and allocation of responsibilities</li> <li>• emergency procedures</li> <li>• incident and near miss reporting and recording procedures</li> <li>• consultation on occupational health and safety issues</li> </ul>

	<ul style="list-style-type: none"> <li>• correct selection, use, storage and maintenance procedures for use of personal protective equipment</li> <li>• risk control procedures</li> </ul>
<b>Controlling risks</b> may include actions such as	<ul style="list-style-type: none"> <li>• consultation with others</li> <li>• measures to remove the cause of the risk at its source</li> <li>• application of the hierarchy of control, namely: <ul style="list-style-type: none"> <li>○ elimination</li> <li>○ substitution</li> <li>○ engineering controls</li> <li>○ administrative controls</li> <li>○ personal protective equipment</li> </ul> </li> </ul>
<b>Other hazardous events</b> may include	<ul style="list-style-type: none"> <li>• fires</li> <li>• bomb threats</li> <li>• chemical spills</li> <li>• occupational violence</li> <li>• natural disasters/events</li> <li>• terrorist attacks</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 PSPOHS301A, candidates should provide evidence that confirms contributions to workplace safety procedures in a range of (3 or more) contexts (or occasions, over time).

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

<b>PSPOHS301A – Contribute to workplace safety (Chosen required elective)</b>	<b>Yes</b>	<b>Not Yet</b>	<b>Not able to comment</b>
Contributing to participative workplace safety arrangements			
Identifying hazards and controlling risks			
In-house training completed			

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

**Referee (Third party) 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:**

## PSPLEGN401A - Encourage compliance with legislation in the public sector

### Introduction

This is a required unit of competency in the PSP41604 Certificate IV in Government (Security) and covers the competency to encourage others (colleagues or those supervised) in the workplace to comply with legislation.

Being competent in this unit means being able to:

### Assist others to comply with legislative requirements

This element requires:

- Knowledge of the range of **legislation** and **guidelines** relating to the public sector workplace is regularly updated to ensure currency
- The way various pieces of legislation are integrated to provide a legislative framework for public sector work and the key requirements of each piece of legislation are confirmed and conveyed to **others** using language and examples suited to their individual needs
- Own work practices and procedures are used to provide a consistent model of compliance with legislative requirements relating to the public sector work environment
- The **consequences of non-compliance** with public sector legislation are identified and conveyed to others using language and examples suited to individual needs
- **Others** are assisted to locate and access current information on legislation and guidelines
- Others are encouraged to identify and obtain advice on apparently **conflicting legislative requirements** in accordance with organisational policy and procedures

### Act on non-compliance

This element requires:

- Actions that might constitute breaches of legislation are identified and discussed with others in accordance with organisational requirements
- Possible breaches of legislation are acted upon or referred promptly to an authorised person/body in accordance with organisational procedures
- Inadequacies in workplace procedures which may contribute to non-compliance are reported and addressed in accordance with organisational procedures

### Range statement

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</b> and <b>guidelines</b> may relate to</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>Others</b> may include</p>	<ul style="list-style-type: none"> <li>• colleagues</li> <li>• supervised staff</li> <li>• contractors</li> </ul>

<b>Consequences of non-compliance</b> may include	<ul style="list-style-type: none"> <li>• for individuals: <ul style="list-style-type: none"> <li>○ counselling</li> <li>○ disciplinary action</li> <li>○ transfer, demotion, dismissal</li> <li>○ legal liability</li> <li>○ fine</li> </ul> </li> </ul>
	<ul style="list-style-type: none"> <li>• External consequences, for example: <ul style="list-style-type: none"> <li>○ to clients</li> <li>○ to the organisation's reputation</li> </ul> </li> </ul>
<b>Conflicting legislative requirements</b> may include	<ul style="list-style-type: none"> <li>• apparent contradiction between statutes</li> <li>• apparent conflict between statutes and policy requirements</li> <li>• contradictions between different policy requirements</li> <li>• contradictions within a single piece of legislation</li> </ul>
<b>Inadequacies in workplace procedures</b> may include	<ul style="list-style-type: none"> <li>• insufficient financial/other controls</li> <li>• insecure Internet/fax access</li> <li>• unauditible 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 PSPLEGN401A, candidates should provide evidence that confirms compliance with legislation in a range of (3 or more) contexts (or occasions, over time).

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

<b>PSPLEGN401A – Encourage compliance with legislation in the public sector (Required)</b>	<b>Yes</b>	<b>Not Yet</b>	<b>Not able to comment</b>
Assisting others to comply with legislative requirements			
Acting on non-compliance			

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

**Referee (Third party) 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:**

## PSPGOV422A - Apply government processes

### Introduction

This is a required unit of competency in the PSP41604 Certificate IV in Government (Security) and covers the application of knowledge of government processes. This unit focuses on government processes and the need to: monitor and respond to changes in structures and/or procedures; follow government protocols; and recognise lines of authority and responsibility within each individual workplace.

Being competent in this unit means being able to:

### Apply information relating to the Machinery of Government

This element requires:

- Up-to-date information relating to **Machinery of Government** relevant to work responsibilities is identified, accessed and applied
- Ambiguity in the structure and function of the organisation or work area as a result of past, present or future Machinery of Government changes is identified and advice obtained and implemented on required work priorities and outcomes for the transition period
- Role ambiguity as a result of past, present or future Machinery of Government changes is managed in accordance with organisational directions

### Apply knowledge of organisational functions

This element requires:

- Up-to-date **information** relating to the **structure** and functions of the organisation is accessed and applied
- Appropriate persons are identified to ensure correct levels of authority are utilised to deal with responsibilities within the organisation
- Areas of work where delegations apply are identified and delegation levels within the organisation are confirmed in accordance with organisational procedures/guidelines
- Approvals are obtained in the workplace in accordance with organisational delegations

### Apply knowledge of protocols

This element requires:

- Up-to-date information relating to government **protocols** is identified, accessed and applied
- Protocols are observed in dealings with other organisations and with persons from within and outside the organisation
- Written protocols, formats and standards are adhered to in writing government documents

## Range statement

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>Machinery of Government</i></b> may include</p>	<ul style="list-style-type: none"> <li>• cycles of government, such as budget cycle</li> <li>• separation of powers (Executive, Judiciary, Legislative)</li> <li>• levels of government (Federal, State/Territory, Local)</li> <li>• legislative process</li> <li>• role and functions of parliamentary structures (unicameral, bicameral)</li> <li>• Cabinet</li> <li>• Ministers</li> <li>• Ministerial portfolios</li> <li>• structure and functions of government departments</li> <li>• quasi-government organisations</li> </ul>
<p><b><i>Information</i></b> may include</p>	<ul style="list-style-type: none"> <li>• documents</li> <li>• databases</li> <li>• web sites</li> <li>• oral information from:             <ul style="list-style-type: none"> <li>○ managers</li> <li>○ supervisors</li> <li>○ colleagues</li> </ul> </li> </ul>
<p>Organisational <b><i>structures</i></b> may include</p>	<ul style="list-style-type: none"> <li>• bureaucratic structure and hierarchy</li> <li>• key personnel and their roles</li> <li>• key organisational functions and accountabilities</li> </ul>
<p><b><i>Protocols</i></b> may include</p>	<ul style="list-style-type: none"> <li>• forms of address</li> <li>• who may be addressed directly</li> <li>• written protocols/formats for written materials</li> <li>• restrictions relating to contact with:             <ul style="list-style-type: none"> <li>○ Minister's office</li> <li>○ media</li> <li>○ members of the public/specific interest groups</li> <li>○ Members of Parliament</li> <li>○ other government departments</li> <li>○ senior management/Board members</li> <li>○ government and opposition parties</li> </ul> </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 PSPGOV422A, candidates should provide evidence that confirms application of government processes handled in a range of (3 or more) contexts (or occasions, over time) in generalist or specialist work activities such as delivering and monitoring services to clients, using resources, conducting interviews, giving evidence, administering contracts etc.

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

<b>PSPGOV422A - Apply government processes (Required)</b>	<b>Yes</b>	<b>Not Yet</b>	<b>Not able to comment</b>
Applying information relating to the machinery of government			
Applying knowledge of organisational functions			
Applying knowledge of protocols			
Applying security policies and procedures			

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

**Referee (Third party) 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:**

## PSPPOL404A - Support policy implementation

### Introduction

This is a required unit of competency in the PSP41604 Certificate IV in Government (Security) and covers the identification and application of policy in a public sector work environment.

Policies explain an organisation's views and outline the principles that underpin an organisation's beliefs, direction and ways of working. Procedures and guidelines are developed from these policies so that everyone within an organisation knows how to turn organisational principles into practice.

This unit focuses on your ability to identify and access workplace policies, apply them to your work and monitor their effectiveness. In order to do this it's necessary to explain the legislation in ways people understand and recognise, and outline the consequences – for the individual and the workplace – if these standards aren't met.

Being competent in this unit means being able to:

### Identify relevant policy

This element requires:

- **Work situations** that are shaped by government or organisation policy are identified in accordance with public sector guidelines
- **Policy** relating to particular work situations is identified and located

### Implement Policy

This element requires:

- Policy to be implemented is interpreted under direction to identify and plan for change in work practices
- The implications of policy for individual work practices are identified, and practices are confirmed/adjusted to reflect policy requirements in accordance with organisational procedures
- Others affected by policy requirements are supported to accommodate those requirements
- Policy is implemented to support achievement of outcomes intended in specific work areas

## Monitor and report on policy implementation

This element requires:

- Information that will assist with the evaluation of the effectiveness of policy implementation is gathered, recorded and reported under direction in accordance with organisational procedures
- **Information** that will assist with the evaluation of the impact of policy implementation on organisational outcomes is gathered, recorded and reported under direction in accordance with organisational procedures

## Range statement

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>Work situations</b> may include	<ul style="list-style-type: none"><li>• processes</li><li>• outcomes</li><li>• priorities</li><li>• client services</li><li>• core business</li><li>• service delivery mode/s</li><li>• organisational structure</li></ul>
<b>Policy</b> may include	<ul style="list-style-type: none"><li>• government policy</li><li>• organisation policy</li></ul>
<b>Information</b> for evaluation may include	<ul style="list-style-type: none"><li>• statistical data</li><li>• qualitative data</li><li>• anecdotal feedback</li><li>• survey data</li><li>• stakeholder opinions</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 PSPPOL404A, candidates should provide evidence that confirms policy implementation supported in a range of (2 or more) contexts (or occasions, over time).

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

<b>PSPPOL404A – Support policy implementation (Required)</b>	<b>Yes</b>	<b>Not Yet</b>	<b>Not able to comment</b>
Identifying relevant policy			
Implementing policy			
Monitoring and reporting on policy implementation			

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

**Referee (Third party) 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:**

## PSPSEC405A – Handle security classified information

### Introduction

This is a required unit of competency in the PSP41604 Certificate IV in Government (Security) and covers the requirements related to handling security classified information. It includes receiving, dealing with and maintaining security classified information.

Being competent in this unit means being able to:

### Receive security classified information

This element requires:

- **Security classified information** is **received** and checked to ensure transmission protocols have been adhered to
- Action is taken in accordance with security policy and procedures where protocols have not been adhered to
- Security classified information is recorded in accordance with organisational policy and procedures

### Deal with security classified information

This element requires:

- Security classified information is **reviewed** to ensure classification meets the organisation's security policy for protection of information
- Aggregated security classified information is reviewed to ensure that it is classified in accordance with security requirements
- Classification requirement is checked to ensure it is warranted, and the level of protection is assigned in accordance with the consequences that might result from the compromise of the information's confidentiality, integrity and availability
- Originators of information who classify documents are contacted to discuss re-classification or de-classification where necessary
- Security classified information is **transmitted** in accordance with organisational security policy and procedures
- **Expert advice** is obtained as required in accordance with organisational policy and procedures

### Maintain security classified information

This element requires:

- Security classified information is **secured** in accordance with organisational policy and procedures
- Security classified information is **accounted for** in accordance with organisational policy and procedures
- Security classified information is **disposed of** in accordance with organisational policy and procedures

## Range statement

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>Security classified information may include</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 classified</li> <li>• non-national security classified</li> <li>• classified by third parties</li> </ul>
<b><i>Security classified information may be received by</i></b>	<ul style="list-style-type: none"> <li>• hand</li> <li>• mail</li> <li>• safe hand mail</li> <li>• courier</li> <li>• electronic means</li> </ul>
<b><i>Reviewed information may include</i></b>	<ul style="list-style-type: none"> <li>• single or aggregated information</li> </ul>
<b><i>Transmission may be by</i></b>	<ul style="list-style-type: none"> <li>• hand</li> <li>• mail</li> <li>• courier</li> <li>• electronic means</li> </ul>
<b><i>Expert advice may include</i></b>	<ul style="list-style-type: none"> <li>• agency security adviser/s</li> <li>• specialist agencies such as: <ul style="list-style-type: none"> <li>○ Australian Security Intelligence Organisation</li> <li>○ Department of Foreign Affairs and Trade</li> <li>○ Australian Public Service Commission</li> <li>○ Defence Signals Directorate</li> <li>○ Australian Federal Police</li> <li>○ Attorney-General's Department</li> <li>○ Australian National Audit Office</li> <li>○ Office of Privacy Commissioner</li> </ul> </li> </ul>

<p><b>Securing practices may include</b></p>	<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>
<p><b>Accounting for security classified information may include</b></p>	<ul style="list-style-type: none"> <li>• audit</li> <li>• spot checks</li> <li>• correct notation or markings</li> <li>• file records</li> <li>• transmission records</li> <li>• receipts</li> </ul>
<p><b>Methods of disposal may include</b></p>	<ul style="list-style-type: none"> <li>• pulping</li> <li>• burning</li> <li>• pulverisation</li> <li>• shredding</li> <li>• overwriting</li> <li>• degaussing</li> <li>• destruction</li> <li>• archiving</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 PSPSEC405A, candidates should provide evidence that confirms security classified information handled in a range of (3 or more) contexts (or occasions, over time).

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

<b>PSPSEC405A – Handle security classified information (Required)</b>	<b>Yes</b>	<b>Not Yet</b>	<b>Not able to comment</b>
Receiving security classified information			
Dealing with security classified information			
Maintaining security classified information			

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

**Referee (Third party) 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:**

## PSPSEC403A – Develop and advise on government security procedures

### Introduction

This is a required unit of competency in the PSP41604 Certificate IV in Government (Security) and covers interpretation of organisational data in the light of the organisation's security policy to identify the need for changed procedures, the development of the procedures and provision of advice. It includes interpreting security policy and legislation, analysing security-related data, developing procedures, and providing advice on government security matters.

Being competent in this unit means being able to:

### Interpret security policy and legislation

This element requires:

- **Legislation** impacting on security policy and procedures is identified and analysed
- The organisation's security policy is analysed in relation to risk identification, security management and security incidents
- Policy intent is confirmed and existing procedures impacted by the policy are identified and reviewed for consistency with the policy

### Analyse security-related data

This element requires:

- **Data** is collected in a timely fashion in accordance with organisational policy and procedures
- Data is analysed and its integrity confirmed
- Outcomes and trends are identified that need to be addressed through security procedures
- Any changes in organisational circumstances are determined and related security procedures are identified

### Develop procedures

This element requires:

- Intended audience/s for **procedures** are identified and structure, language style and format are determined in accordance with organisational requirements
- Security procedures are developed to reflect **changes** in circumstances
- Procedures are developed in consultation with security plan developer/s, end users and organisational approval personnel
- Procedures are structured to take account of workplace diversity and meet organisational requirements
- Procedures are submitted and approved in accordance with organisational policy and procedures

## Provide advice on government security matters

This element requires:

- Information and **advice** on security procedures and related legislation, regulations, standards and guidelines are provided in accordance with organisational procedures
- Current organisational policies and directions are reflected in advice provided
- Intended use and consequences of advice are considered, and advice is communicated in a manner that addresses the requirements of **stakeholders**
- Any documentation provided is checked to ensure it supports the information and advice given

## Range statement

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>Legislation may include</i></b>	<ul style="list-style-type: none"> <li>• Commonwealth and State/Territory Acts and regulations</li> </ul>
<b><i>Data may include</i></b>	<ul style="list-style-type: none"> <li>• security records</li> <li>• incident reports</li> <li>• security risk management plans</li> <li>• files</li> <li>• email</li> <li>• Internet/intranet</li> <li>• electronic records</li> <li>• video images</li> <li>• graphics</li> <li>• notes</li> <li>• diary entries</li> <li>• telephone messages</li> <li>• pager records</li> <li>• fax records</li> </ul>
<b><i>Procedures may be</i></b>	<ul style="list-style-type: none"> <li>• agency specific</li> <li>• area specific</li> <li>• relating to specific activities or practices</li> </ul>
<b><i>Changes may be caused by</i></b>	<ul style="list-style-type: none"> <li>• restructure</li> <li>• changes to legal risks</li> <li>• changes in strategic direction</li> <li>• changes to legislation and whole of government policies</li> <li>• major shift in business or corporate goals or plans</li> <li>• key projects</li> </ul>
<b><i>Advice may be</i></b>	<ul style="list-style-type: none"> <li>• formal</li> <li>• informal</li> <li>• briefing</li> </ul>

	<ul style="list-style-type: none"> <li>• awareness session</li> <li>• preventative</li> <li>• post incident</li> <li>• written</li> <li>• oral</li> </ul>
<b>Stakeholders</b> may be	<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>

### **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 PSPSEC403A, candidates should provide evidence that confirms development of and advice on government security procedures in a range of (3 or more) contexts (or occasions, over time).

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

<b>PSPSEC403A – Develop and advise on government security procedures (Required)</b>	<b>Yes</b>	<b>Not Yet</b>	<b>Not able to comment</b>
Interpreting security policy and legislation			
Analysing security-related data			
Developing procedures			
Providing advice on government security matters			

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

**Referee (Third party) 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:**

## **PSPSEC406A – Provide government security briefings**

### **Introduction**

This is a chosen required elective unit of competency in the PSP41604 Certificate IV in Government (Security) and covers the requirements to provide a range of security briefings. It includes determining the need for security briefings, organising and conducting briefings.

Being competent in this unit means being able to:

### **Organise security briefing**

This element requires:

- The need for a security briefing and related methodology are determined in accordance with individual, organisational and legislative requirements
- Briefing purpose, level, structure and content are determined in accordance with organisational policy and procedures
- Materials and any personnel to be involved in the briefing are determined and organised
- A plan is prepared to support delivery of the briefing in accordance with organisational requirements

### **Conduct security briefing**

This element requires:

- The purpose and structure of the briefing are outlined to participants in accordance with the briefing plan
- Active participation from participants in the briefing is sought, encouraged and valued
- Organisational and legislated government security requirements are conveyed to participants using language and examples suited to their levels of understanding and diverse needs
- Understanding of security requirements and the consequences of non-compliance with security requirements is checked and further information is provided for clarification as necessary
- Briefing is conducted in accordance with organisational policy and procedures
- Where required, a record/report of the briefing is prepared and submitted in accordance with organisational policy and procedures

### **Range statement**

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>Need for briefing may be determined by</i></b>	<ul style="list-style-type: none"> <li>• organisational policy</li> <li>• change in circumstances</li> <li>• security incident/s</li> </ul>
<b><i>Security briefing may be</i></b>	<ul style="list-style-type: none"> <li>• ad hoc</li> <li>• incident related</li> <li>• on induction</li> <li>• on initial clearance</li> <li>• on revalidation</li> <li>• on clearance upgrade</li> <li>• on clearance downgrade</li> <li>• overseas</li> <li>• high risk</li> <li>• a debriefing</li> </ul>
<b><i>Methodology may include</i></b>	<ul style="list-style-type: none"> <li>• facilitator-led</li> <li>• collaborative</li> <li>• problem-based</li> <li>• descriptive</li> <li>• illustrative</li> <li>• formality of language and structure</li> </ul>
<b><i>Briefing plan may include</i></b>	<ul style="list-style-type: none"> <li>• purpose</li> <li>• subject matter</li> <li>• timing</li> <li>• location</li> <li>• participant/s</li> <li>• methodology</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 PSPSEC406A, candidates should provide evidence that confirms provision of government security procedures in a range of (3 or more) contexts (or occasions, over time).

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

<b>PSPSEC406A – Provide government security briefings (Chosen required elective)</b>	<b>Yes</b>	<b>Not Yet</b>	<b>Not able to comment</b>
Organising security briefings			
Conducting security briefings			

**Candidate's Comments and Attachment/s number as included in Portfolio of Evidence:**  
 (For example: Attach PowerPoint Presentation/s; Handouts; and Evaluation Sheet/s.)

**Referee (Third party) 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:** \_\_\_\_\_

## PSPGOV405B - Provide input into change processes

### Introduction

This is a chosen required elective unit of competency in the PSP41604 Certificate IV in Government (Security) and covers understanding the reasons for change and initiating specific changes related to the work unit.

Being competent in this unit means being able to:

### Suggest options and opportunities for change

This element requires:

- The need for change in work practice within the work unit is identified, suggestions sought and options devised
- Options and opportunities for change are suggested to improve efficiency and effectiveness of the workgroup and the work environment
- The broader workplace context, including future trends, is taken into account in suggestions for change
- **Risk factors** affecting change are analysed to identify possible constraints

### Encourage commitment to workplace change

This element requires:

- Positive encouragement is provided to implement workplace **change**
- The needs and viewpoints of individuals are identified and considered when implementing change
- Communication strategies are developed and support is provided to colleagues on adjusting to change
- Issues requiring further action are identified and dealt with in accordance with **legislation, policy and procedures**

### Monitor and evaluate change

This element requires:

- Implementation of change is monitored and feedback on individual and group work practices is prompt and constructive
- Suggestions for improvements made by workgroup members are positively received and acted on where appropriate
- Work activities are evaluated based on feedback from workgroup members and other **stakeholders**
- **Evidence and information** is collected on the impact of change, is accurate, relevant and reported according to organisational requirements
- Recommendations for improving methods or techniques to manage change are **negotiated** in accordance with organisational policy and procedures

- Learnings from the implementation of change are identified, shared with others and transferred to other change initiatives

### Deal with ambiguities in the change process

This element requires:

- The need to operate within constraints beyond one's own control is recognised and accepted
- Areas of ambiguity in proposed change are identified
- Options for dealing with ambiguity and criteria for assessing those options are developed and communicated to the workgroup
- Best option is selected, work is undertaken and ambiguity handled in accordance with option determined
- The impact of change and identified related issues are communicated to management as required

### Range statement

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>Risk factors</i></b> may include	<ul style="list-style-type: none"> <li>• disturbances to workflow</li> <li>• confusion/loss of confidence</li> <li>• budget constraints</li> <li>• supplier problems</li> <li>• product/service delivery problems</li> <li>• time delays</li> <li>• ineffective communication</li> <li>• lack of participation/buy in of staff in workplace change leading to resistance and conflict</li> </ul>
<b><i>Change</i></b> may include	<ul style="list-style-type: none"> <li>• imposed change</li> <li>• self-initiated change</li> <li>• implementation of new work practices</li> <li>• legislative change</li> <li>• changes in the machinery of government</li> <li>• organisational restructuring</li> <li>• technology transfer to the workplace</li> <li>• changing work practices and procedures</li> <li>• staffing changes</li> <li>• shared services environment</li> </ul>
<b><i>Legislation, policy and procedures</i></b> may include	<ul style="list-style-type: none"> <li>• Commonwealth and State/Territory legislation</li> <li>• government policy</li> <li>• public sector code of ethics</li> <li>• national standards</li> <li>• the organisation's policies and practices</li> <li>• organisational code of conduct</li> </ul>

<p><b>Stakeholders</b> may include</p>	<ul style="list-style-type: none"> <li>• all those individuals and groups both inside and outside the organisation that have some direct interest in the organisation's behaviour, actions, products and services, including: <ul style="list-style-type: none"> <li>○ employees at all levels of the organisation</li> <li>○ clients</li> <li>○ other public sector organisations</li> <li>○ community organisations</li> <li>○ private sector organisations</li> <li>○ union and association representatives</li> <li>○ boards of management</li> <li>○ government</li> <li>○ Ministers</li> </ul> </li> </ul>
<p><b>Evidence and information</b> may include</p>	<ul style="list-style-type: none"> <li>• client surveys</li> <li>• employee satisfaction feedback</li> <li>• industrial disputes</li> <li>• supplier feedback</li> <li>• productivity/efficiency measures</li> <li>• cost savings</li> </ul>
<p><b>Negotiation</b> may include</p>	<ul style="list-style-type: none"> <li>• assertiveness</li> <li>• collaboration</li> <li>• solution designing</li> <li>• confidence building</li> <li>• conflict reduction</li> <li>• stress management</li> <li>• empathising</li> <li>• techniques such as: <ul style="list-style-type: none"> <li>○ speaking skills</li> <li>○ presentation techniques</li> <li>○ effective listening</li> <li>○ questioning techniques</li> <li>○ verbal and non-verbal communication</li> <li>○ using personal attributes</li> <li>○ culturally appropriate strategies</li> <li>○ constructive feedback</li> <li>○ issues identification</li> <li>○ exploring options</li> <li>○ identifying areas of agreement</li> <li>○ recording agreements</li> </ul> </li> <li>• clarifying</li> <li>• restating position</li> <li>• summarising progress</li> <li>• deferring decision</li> <li>• preparing a compromise</li> <li>• using a mediator/third party</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 PSPGOV405B, candidates should provide evidence that confirms provision of input to change in a range of (3 or more) contexts (or occasions, over time).

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

<b>PSPGOV405B – Provide input to change processes (Chosen required elective)</b>	<b>Yes</b>	<b>Not Yet</b>	<b>Not able to comment</b>
Suggesting options and opportunities for change			
Encouraging commitment to workplace change			
Monitoring and evaluating change			
Dealing with ambiguities in the change process			

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

**Referee (Third party) 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:**

## PSPGOV406B - Gather and analyse information

### Introduction

This is a chosen required elective unit of competency in the PSP41604 Certificate IV in Government (Security) and covers collection and analysis of information to achieve work unit objectives and meet client needs.

Being competent in this unit means being able to:

### Identify and collect information

This element requires:

- Nature, extent and purpose of required **information** is identified
- Internal and external **sources** are identified and accessed to produce required information in accordance with **legislation, policy and procedures**
- Information is collected, organised, recorded and reported in accordance with organisational procedures and defined guidelines
- Information collected is organised in a way which enables easy access and retrieval by other staff

### Analyse and interpret information

This element requires:

- Information and its sources are critically evaluated for relevance and validity to business/client requirements
- Basic **analysis** of information is undertaken as required to identify key issues
- More detailed analysis of information is carried out as required using relevant techniques including mathematical calculations and methods for numerical/graphical information

### Develop and apply workable solutions

This element requires:

- Workable solutions to business/client requirements are developed on consideration of analysed information
- Proposed solutions are communicated or implemented as required

### Present information

This element requires:

- Information is reported in the required format, style, structure and timeframe
- Information is **presented** in required medium in accordance with organisational requirements using relevant technology

## Maintain information

This element requires:

- A range of standard and complex **information systems** and operations is used in accordance with organisational policy and procedures
- Information and records are maintained in accordance with organisational procedures to ensure data and system integrity
- Routine data and records are reconciled as required
- Inadequacies in system/s relating to information retrieval are identified and corrected or reported to relevant staff as required

## Range statement

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>Information may include</b>	<ul style="list-style-type: none"> <li>• legislation, guidelines and awards</li> <li>• organisation, legal and policy materials</li> <li>• client information</li> <li>• market trends</li> <li>• media reports</li> <li>• registries and file records</li> <li>• library materials</li> <li>• financial records</li> <li>• basic statistical information</li> <li>• human resources/personnel records</li> <li>• asset records</li> <li>• meta-data</li> </ul>
<b>Sources of information may include</b>	<ul style="list-style-type: none"> <li>• those internal to the organisation such as:             <ul style="list-style-type: none"> <li>○ intranet</li> <li>○ databases/files</li> <li>○ library collections</li> <li>○ internal publications</li> <li>○ annual reports</li> <li>○ newsletters</li> <li>○ other staff</li> </ul> </li> <li>• those external to the organisation such as:             <ul style="list-style-type: none"> <li>○ Internet</li> <li>○ local, state, national and international libraries and archives</li> <li>○ other organisations' publications</li> <li>○ staff in external organisations</li> </ul> </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> </ul>

	<ul style="list-style-type: none"> <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/practices/code of conduct</li> </ul>
<b>Analysis of information</b> <i>may include</i>	<ul style="list-style-type: none"> <li>• qualitative analysis</li> <li>• quantitative analysis</li> <li>• critical analysis</li> <li>• problem solving</li> <li>• matching</li> <li>• statistical analysis</li> <li>• mathematical calculations</li> <li>• forecasting</li> </ul>
<b>Presentation of information</b> <i>may include</i>	<ul style="list-style-type: none"> <li>• routine reports and submissions</li> <li>• briefing notes, ministerials</li> <li>• proposals, project plans</li> <li>• articles and promotional material</li> <li>• tabular or graphical presentation</li> <li>• overhead transparencies</li> <li>• slideshow data presentation</li> <li>• face-to-face</li> <li>• telephone</li> </ul>
<b>Information systems</b> <i>may include</i>	<ul style="list-style-type: none"> <li>• file/records management systems</li> <li>• personnel/human resources systems</li> <li>• specific purpose databases</li> <li>• library systems</li> <li>• data warehouse systems</li> <li>• web sites</li> <li>• financial information systems</li> <li>• workplace communication systems</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 PSPGOV406B, candidates should provide evidence that confirms information gathered and analysed in a range of (3 or more) contexts (or occasions, over time).

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

<b>PSPGOV406B – Gather and analyse information (Chosen required elective)</b>	<b>Yes</b>	<b>Not Yet</b>	<b>Not able to comment</b>
Identifying and collecting information			
Analysing and interpreting information			
Developing and applying workable solutions			
Presenting information			
Maintaining information			

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

**Referee (Third party) 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:**

## PSPGOV412A - Use advanced workplace communication strategies

### Introduction

This is a required unit of competency in the PSP41604 Certificate IV in Government (Security) and covers the use of advanced communication strategies for interacting with internal and external clients. It includes dealing with complex enquiries and complaints, giving directions, managing meetings and making workplace and public presentations.

Being competent in this unit means being able to:

### Deal with complex enquiries /complaints

This element requires:

- Relationship with the client is established by displaying empathy towards client needs, and the nature of complaint/enquiry is established by listening, questioning and confirming
- Complaint/enquiry is recorded accurately in simple language, and verified with the client to ensure it has been recorded correctly
- Documentation to support complaint/enquiry is obtained if required
- Action available under organisational policies is identified, and procedures to respond to and resolve complaint/enquiry are followed/authorised
- Complaints/enquiries that require referral to other personnel or external organisations are identified and referred in accordance with organisational policy and procedures
- Client is informed of action taken to resolve/refer the complaint/enquiry and a record logged in accordance with organisational procedures

### Give directions

This element requires:

- Ethical, lawful and reasonable directions are given to others, and staff are protected from reprisals for refusing directions to act unethically
- Directions are relayed in a clear, concise manner appropriate to the receiver
- Questioning and listening skills are used to confirm understanding of directions
- Problems in directions being implemented are resolved promptly or referred in accordance with organisational policy and procedures
- Feedback is provided on implementation in accordance with organisational requirements

### Manage meetings

This element requires:

- Purpose of each meeting is clarified and the agenda developed in consultation with participants, in line with the ***purpose***

- The **procedure** for each meeting and the style of chairing/facilitating are selected in accordance with the meeting's purpose and the participants
- Meetings are chaired in accordance with organisational requirements, agreed **conventions** for the type of meeting and **legal and ethical requirements**
- Meetings are conducted to ensure they are focused on the objectives of the meeting and are time efficient
- Meetings are facilitated to enable participation, discussion, problem solving and **resolution** of issues by all those present
- Decisions and recommendations are summarised succinctly, checked for accuracy and recorded as required

### Make presentations

This element requires:

- Presentations are made to a range of audiences in accordance with organisational requirements
- Presentations are structured logically and contain relevant information/content to meet the purpose of the presentation
- **Supporting materials and presentation aids** are selected, created and organised to enhance audience understanding of key concepts and ideas
- **Presentation strategies** are chosen and used to match the **characteristics** of the target audience, the location, the resources and the personnel needed
- Effectiveness of the presentation is evaluated formally and informally for the purpose of continuously improving future presentations

### Range statement

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>Agenda may include</i></b>	<ul style="list-style-type: none"> <li>• statement of the meeting's purpose</li> <li>• date, time and location of meeting</li> <li>• welcome</li> <li>• minutes of the previous meeting</li> <li>• matters or business arising from the minutes</li> <li>• correspondence</li> <li>• reports</li> <li>• major agenda items</li> <li>• general business</li> <li>• date of next meeting</li> </ul>
<b><i>Purpose may include</i></b>	<ul style="list-style-type: none"> <li>• range of organisation-specific purposes</li> <li>• setting of organisation/team goals</li> <li>• planning and development of a project</li> <li>• progress of a project</li> <li>• discussion forum for internal/external clients</li> </ul>

<b>Meeting procedure</b> may include	<ul style="list-style-type: none"> <li>• formal</li> <li>• informal</li> <li>• semi-formal</li> <li>• structured</li> <li>• self-managed</li> </ul>
<b>Meeting conventions</b> may include	<ul style="list-style-type: none"> <li>• quorum requirements</li> <li>• informal discussion</li> <li>• waiting to be recognised by the chairperson</li> <li>• speaking through the chairperson</li> <li>• restricting discussion to agenda items</li> <li>• time limit on speakers</li> <li>• moving and seconding formal motions</li> <li>• voting procedures</li> <li>• conflict of interest provisions</li> <li>• consensus required</li> <li>• majority of members to agree</li> <li>• casting vote for chairperson</li> </ul>
<b>Legal and ethical requirements</b> may include	<ul style="list-style-type: none"> <li>• requirements for public meetings</li> <li>• codes of practice</li> <li>• legislation relating to the public sector</li> </ul>
<b>Resolution of issues</b> may include	<ul style="list-style-type: none"> <li>• agreeing on a course of action</li> <li>• deferring decisions to another meeting</li> </ul>
<b>Supporting materials and presentation aids</b> may include	<ul style="list-style-type: none"> <li>• audio recordings</li> <li>• charts</li> <li>• computer simulations and presentations</li> <li>• diagrams</li> <li>• flow charts</li> <li>• graphs</li> <li>• maps</li> <li>• models</li> <li>• overhead projector</li> <li>• paper-based materials</li> <li>• photographs</li> <li>• pictures</li> <li>• posters</li> <li>• tables</li> <li>• video images</li> <li>• whiteboard</li> </ul>
<b>Presentation strategies</b> may include	<ul style="list-style-type: none"> <li>• oral presentations</li> <li>• discussion</li> <li>• questioning</li> <li>• simulations and role play</li> <li>• case studies</li> <li>• group and/or pair work</li> <li>• demonstration</li> </ul>
<b>Characteristics of the target audience</b> may relate to	<ul style="list-style-type: none"> <li>• public sector level/s</li> <li>• language, literacy and numeracy levels</li> <li>• cultural and language background</li> <li>• educational background or general knowledge</li> <li>• gender</li> <li>• age</li> <li>• disability</li> <li>• previous experience with the topic</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 PSPGOV412A, 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:**

<b>PSPGOV412A – Use advanced workplace communication strategies (Required)</b>	<b>Yes</b>	<b>Not Yet</b>	<b>Not able to comment</b>
Dealing with complex enquiries/complaints			
Giving directions			
Managing meetings			
Making presentations			

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

**Referee (Third party) 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:**

## PSPREG413A - Undertake inspections and monitoring

### Introduction

This is a chosen required elective unit of competency in the PSP41604 Certificate IV in Government (Security) and covers the requirements to undertake both routine and non-routine inspections and monitoring of a more complex or detailed nature, with discretion to determine appropriate action in accordance with relevant Acts and regulations. Typically work will be under general direction, with full responsibility for delegated duties within a generally defined area.

Being competent in this unit means being able to:

### Plan and organise inspection and monitoring activities

This element requires:

- Outputs are confirmed and inspection and monitoring **activities** and responsibilities are determined in accordance with organisational requirements
- *Procedures*, timeframes, **resources and equipment** requirements are determined for self and others in accordance with organisational and task requirements
- Resources/equipment are obtained and prepared in accordance with organisational and task requirements
- Legislative requirements, risk management practices and occupational health and safety requirements are determined
- Communication strategies and development opportunities are identified and adjusted to suit a range of clients in making them aware of their obligations under relevant **legislation**, in accordance with organisational policy and procedures
- Procedural and information guides are reviewed and updated as required

### Undertake inspections and monitoring

This element requires:

- **Inspections and monitoring activities** are carried out under *general direction* in accordance with organisational and legislative requirements including occupational health and safety
- **Risk management strategies** are developed and implemented as required in accordance with set procedures and timelines
- Resources/equipment are used and maintained in accordance with organisational and task requirements
- When required, operational and technical advice is provided to subordinate officers in accordance with organisational policy and procedures

## Act on non-compliance

This element requires:

- Information/education is provided to achieve client compliance in accordance with organisational guidelines and legislative requirements relating to the seriousness of the possible breach
- Further **action** as a result of failure to achieve compliance is taken in accordance with organisational guidelines and legislative requirements relating to the seriousness of the possible breach
- Compliance requirements of legislation/regulations are identified, and contraventions and recommended action are reported in accordance with organisational policy and procedures
- Serious or complex situations are referred for advice or resolution in accordance with organisational policy and procedures
- The elements of each offence to be prosecuted under relevant legislation are identified, and information/evidence is **collected** and provided in accordance with legislation, procedures and rules of evidence
- When required, court attendance and conduct requirements are fulfilled in compliance with organisational guidelines

## Provide reports, information and training

This element requires:

- Workable solutions to business/client requirements are developed on consideration of analysed information
- **Records** are maintained and reports are prepared and provided in accordance with organisational requirements
- Requirements of relevant legislation are interpreted and information and advice are provided on technical and operational matters
- On-the-job inspection/monitoring training is provided in accordance with organisational requirements

## Range statement

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>Activities</b> may include	<ul style="list-style-type: none"><li>• inspections/examinations</li><li>• monitoring</li><li>• surveillance</li><li>• focused and benchmark audit activities</li><li>• remote monitoring</li><li>• other compliance assurance activities</li></ul>
<b>Procedures</b> may include	<ul style="list-style-type: none"><li>• observation</li></ul>

	<ul style="list-style-type: none"> <li>• handling procedures</li> <li>• sampling procedures</li> <li>• rejection procedures</li> <li>• storage procedures</li> <li>• disinfection procedures</li> <li>• treatment procedures</li> <li>• organisational guidelines and code of conduct</li> <li>• incident reporting procedures</li> <li>• safety procedures</li> <li>• emergency procedures</li> <li>• evacuation procedures</li> </ul>
<b>Resources and equipment may include</b>	<ul style="list-style-type: none"> <li>• inspection equipment</li> <li>• personal protective equipment – respirators, gloves, overalls, boots, hearing protection, goggles, masks etc</li> <li>• test kit equipment</li> <li>• recording equipment</li> <li>• storage equipment/facilities</li> <li>• entry authority/warrant</li> <li>• Global Positioning System (GPS) equipment</li> <li>• communication equipment</li> <li>• computers</li> <li>• satellite imagery</li> <li>• aerial photographs</li> <li>• spatial data and information</li> <li>• vehicles – 2 or 4 wheel drive</li> </ul>
<b>Legislation may include</b>	<ul style="list-style-type: none"> <li>• Commonwealth legislation and regulations, for example: <ul style="list-style-type: none"> <li>○ Commonwealth Quarantine Act 1908, proclamations and regulations</li> <li>○ Crimes Act 1914 and Criminal Code Act 1995</li> <li>○ Customs Act 1901 and regulations</li> <li>○ Wildlife Protection Act 1982</li> <li>○ Export Control Act 1982</li> <li>○ Imported Foods Act 1996</li> <li>○ Occupational Health and Safety Act 1988</li> </ul> </li> <li>• State, Territory and Local Government legislation and regulations, such as those relating to: <ul style="list-style-type: none"> <li>○ agriculture</li> <li>○ horticulture</li> <li>○ conservation and land management</li> <li>○ fisheries</li> <li>○ environmental protection</li> <li>○ building</li> <li>○ water</li> <li>○ emergencies</li> <li>○ international legislation/codes of behaviour</li> </ul> </li> </ul>
<b>Inspections and monitoring activities may relate to</b>	<ul style="list-style-type: none"> <li>• aircraft</li> <li>• airfreight</li> <li>• animal products</li> <li>• animals</li> <li>• cargo</li> <li>• cereals</li> </ul>

	<ul style="list-style-type: none"> <li>• collection of biological specimens</li> <li>• disposal of organic waste</li> <li>• fresh produce</li> <li>• goods</li> <li>• land condition, such as:</li> <li>• topography</li> <li>• salinity</li> <li>• erosion</li> <li>• weed infestation</li> <li>• vermin infestation</li> <li>• fire hazard</li> <li>• over grazing</li> <li>• land improvements, such as: <ul style="list-style-type: none"> <li>○ fences</li> <li>○ buildings</li> <li>○ sporting or playground equipment</li> <li>○ irrigation infrastructure</li> <li>○ sewerage infrastructure</li> <li>○ waterfront occupations</li> <li>○ community structures</li> </ul> </li> <li>• land usage</li> <li>• leases and other tenures, to ensure compliance with conditions</li> <li>• licence/permit compliance (eg vegetation clearing)</li> <li>• live fish</li> <li>• livestock</li> <li>• mail</li> <li>• mineral samples</li> <li>• passenger baggage</li> <li>• people</li> <li>• pests</li> <li>• plant products</li> <li>• plants</li> <li>• premises</li> <li>• properties</li> <li>• reserves and their use/s</li> <li>• survey activities to maintain readiness for district emergency plans</li> <li>• vector monitoring</li> <li>• vessels</li> </ul>
<p><b>General direction may include</b></p>	<ul style="list-style-type: none"> <li>• supervisors</li> <li>• senior policy officers</li> <li>• senior inspectors</li> <li>• line managers</li> <li>• project managers</li> <li>• program managers</li> <li>• inspection specialists</li> </ul>

<b><i>Risk management strategies may include</i></b>	<ul style="list-style-type: none"> <li>• monitoring</li> <li>• treatment</li> <li>• containment</li> <li>• control</li> <li>• eradication</li> <li>• destruction</li> <li>• biosecurity strategies</li> </ul>
<b><i>Non-compliance may include</i></b>	<ul style="list-style-type: none"> <li>• both routine and non-routine matters of a more complex or detailed nature with discretion to determine appropriate action</li> <li>• referral to senior staff of decisions that are more difficult, or of potential interest to external parties such as the media, public, political parties etc</li> </ul>
<b><i>Action may include</i></b>	<ul style="list-style-type: none"> <li>• advice</li> <li>• warning</li> <li>• formal notification of intent</li> <li>• infringement notices</li> <li>• on-the-spot fines</li> <li>• court prosecution</li> </ul>
<b><i>Collection of evidence may include</i></b>	<ul style="list-style-type: none"> <li>• observation</li> <li>• interviewing</li> <li>• seizure</li> <li>• sampling</li> <li>• specimen collection</li> <li>• recording</li> <li>• maintenance of case files</li> <li>• determination of land ownership</li> </ul>
<b><i>Records may include</i></b>	<ul style="list-style-type: none"> <li>• notes</li> <li>• case files</li> <li>• statistics</li> <li>• forms (application forms, disease notification forms, etc)</li> <li>• notices (seizure notice, infringement notice, etc)</li> <li>• invoices</li> <li>• receipts</li> <li>• commercial documentation such as bills of lading, airway bills</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 PSPREG413A, candidates should provide evidence that confirms performance under general direction with responsibility within a generally defined area for inspections and monitoring undertaken in a range of (3 or more) contexts (or occasions, over time).

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

<b>PSPREG413A – Undertake inspections and monitoring (Chosen required elective)</b>	<b>Yes</b>	<b>Not Yet</b>	<b>Not able to comment</b>
Planning and organising inspections and monitoring activities			
Undertaking inspections and monitoring			
Acting on non-compliance			
Providing information reports and training			

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

**Referee (Third party) 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:**

## PSPSEC401A – Undertake government security risk analysis

### Introduction

This is a required unit of competency in the PSP41604 Certificate IV in Government (Security) and covers work at an operational level, to analyse risk against the organisation's security plan. It includes establishing the security risk context; identifying, analysing and evaluating risk against the organisation's security plan; and compiling of a security risk register.

Being competent in this unit means being able to:

### Establish security risk context

This element requires:

- **Strategic** and **organisational contexts** are confirmed in accordance with the organisation's security plan
- **Stakeholders** are identified and their expectations and input are gathered in accordance with **legislation, policy and procedures**
- **Security risk criteria** are identified from the security plan and confirmed as current and relevant
- Information and resources are obtained to conduct the risk analysis in accordance with organisational policy and procedures

### Identify security risk

This element requires:

- **Sources** of security risk are identified and recorded in accordance with organisational policy and procedures
- Risks are identified using a **specified methodology or tools** in accordance with the security plan
- Sources of risk are identified from the perspective of all stakeholders
- Stakeholders are consulted during the risk identification process to finalise a list of risks

### Analyse security risk

This element requires:

- **Threat assessments**, current **exposure** and current security arrangements are identified in accordance with the security plan to estimate the **likelihood** of each risk event occurring
- Potential **consequences** of each risk are determined in accordance with the security plan, including **critical lead time for recovery**
- **Risk ratings** are determined, documented and communicated in accordance with the security plan and organisational standards
- A rationale for each risk rating is included in accordance with organisational requirements

### Evaluate security risk

This element requires:

- Risks are assessed against the organisation's security risk criteria
- Risks are prioritised for treatment in accordance with the security plan
- Risks are monitored in accordance with the security plan until treatment measures have been implemented

### Compile security risk register

This element requires:

- A **security risk register** is developed that records identified risks, their nature and source
- The consequences and likelihood of risks, and the adequacy of existing controls are identified in the register
- Risk ratings are recorded for identified risks in accordance with organisational procedures
- The security risk register is compiled to meet organisational standards for content, format and presentation and reflects changes in circumstances
- Risk register is referred to management for decision on which risks will be accepted and which will require treatment

### Range statement

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>Strategic context</b> may include</p>	<ul style="list-style-type: none"> <li>• the relationship between the organisation and the environment in which it operates</li> <li>• organisational structure</li> <li>• the organisation's functions: <ul style="list-style-type: none"> <li>• political</li> <li>• operational</li> <li>• financial</li> <li>• social</li> <li>• legal</li> <li>• commercial</li> </ul> </li> <li>• the various stakeholders and clients</li> </ul>
<p><b>Organisational context</b> may include</p>	<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>
<p><b>Stakeholders</b> may include</p>	<ul style="list-style-type: none"> <li>• all those individuals and groups both inside and outside the organisation that have some direct interest in the organisation's behaviour, actions, products and services such as:</li> </ul>

	<ul style="list-style-type: none"> <li>○ employees at all levels of the organisation</li> <li>○ community</li> <li>○ clients</li> <li>○ other public sector organisations</li> <li>○ union and association representatives</li> <li>○ boards of management</li> <li>○ government</li> <li>○ Ministers</li> </ul>
<b>Legislation, policy and procedures may include</b>	<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>● 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>● Security Guidelines for Australian Government IT Systems (ACSI 33)</li> <li>● Commonwealth Protective Security Manual</li> <li>● Australian and New Zealand standards – Risk management AS/NZS 4360:1999</li> </ul>
<b>Security risk criteria may concern</b>	<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>Risk may be to</b>	<ul style="list-style-type: none"> <li>● personnel</li> <li>● information</li> <li>● property</li> <li>● reputation</li> </ul>
<b>Sources of security risk 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>Specified methodology or tools may be</b>	<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, threats (SWOT) analysis</li> <li>● analysis of risk registers</li> <li>● examination of available data such as audit</li> </ul>

	<ul style="list-style-type: none"> <li>• results, incident reports</li> <li>• nomogram</li> <li>• risk matrix</li> <li>• scenario analysis</li> <li>• business continuity planning</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>Threats may be</b>	<ul style="list-style-type: none"> <li>• criminal</li> <li>• terrorist</li> <li>• from foreign intelligence services</li> <li>• from commercial/industrial competitors</li> <li>• from malicious people</li> <li>• real or perceived</li> </ul>
<b>Risk exposure is</b>	<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>
<b>Likelihood of risk may be determined through analysis of</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 may include</b>	<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> </ul>
<b>Critical lead time for recovery is</b>	<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>Risk ratings 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 or trivial</li> </ul>
<b>Security risk register may include</b>	<ul style="list-style-type: none"> <li>• source</li> <li>• nature</li> <li>• existing controls</li> <li>• likelihood</li> <li>• consequences</li> <li>• initial rating</li> <li>• vulnerability</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 PSPSEC401A, candidates should provide evidence that confirms government security risk analysis 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>PSPSEC401A – Undertake government security risk analysis (Required)</b>	<b>Yes</b>	<b>Not Yet</b>	<b>Not able to comment</b>
Demonstrating knowledge of Security Risk Management Reference material including: – Australian Government Protective Security Policy Framework (2010) – AS/NZS ISO 31000:2009 – Risk management – Principles and guidelines – HB167:2006 – Security risk management			
Demonstrating knowledge of risk analysis terminology and applying techniques			
Establishing security risk context			
Identifying security risks			
Analysing security risks			
Evaluating security risks			
Compiling a security risk register			
<b>Candidate's Comments and Attachment/s number as included in Portfolio of Evidence:</b>			
<b>Referee (Third party) Comments:</b>			
<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>			
<b>Signature of Referee:</b>			<b>Date:</b>
<i>I agree with the statements above and that I have met the knowledge and skill requirements in this unit of competency.</i>			
<b>Signature of Candidate:</b>			<b>Date:</b>

## PSPSEC402A – Implement security risk treatments

### Introduction

This is a required unit of competency in the PSP41604 Certificate IV in Government (Security) and covers identification and implementation of security risk treatments. It includes confirming risk decisions identifying security risk treatment options, implementing countermeasures, and monitoring and reviewing the security risk management process.

Being competent in this unit means being able to:

### Confirm risk decisions

This element requires:

- Management decisions determining **acceptable** and **unacceptable risks** are confirmed in accordance with organisational policy and procedures
- Low-level risks that the organisation decides to accept are noted and monitored to detect changed circumstances
- Unacceptable high-**level** risks are referred for the development of formal management plans
- Major or significant risks identified as unacceptable are noted for treatment

### Identify risk treatments

This element requires:

- **Treatments** are determined that are consistent with organisational policies, procedures and guidelines and the organisation's security plan
- Treatments are determined that are cost-effective and match the level and type of risk and the importance of the function or resource
- Treatments are selected to reduce the **likelihood** of occurrence or the **consequences** of the risk, or both
- **Continuity plans** are included in treatments, where appropriate, in accordance with the security plan
- Treatments are documented and submitted for approval in accordance with organisational policy and procedures

### Implement countermeasures

This element requires:

- A **treatment plan** is developed and implemented in accordance with organisational policy and procedures
- Implementation of **countermeasures** is undertaken in accordance with the implementation strategy detailed in the security plan
- Countermeasures are implemented in accordance with timeframe and budgetary requirements
- Countermeasures are implemented in accordance with **legal requirements, government** and **organisational policy**

## Monitor and review security risk management process

This element requires:

- **Strategies** to monitor risk environment are implemented
- **Monitoring** is conducted on a regular basis in accordance with organisational policy and procedures
- Risk treatments are evaluated against the objectives of the security plan to ensure these remain effective and/or necessary
- Feedback is obtained from **stakeholders** on the adequacy and need for current security measures affecting their work/area
- Recommendations for re-examination of security risk or improved risk treatments are conveyed to the appropriate personnel in accordance with organisational policy and procedures.

## Range statement

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>Risk may be to</i>	<ul style="list-style-type: none"> <li>• personnel</li> <li>• information</li> <li>• property</li> <li>• reputation</li> </ul>
<i>Acceptable risks are</i>	<ul style="list-style-type: none"> <li>• those which an organisation has determined have the least potential for harm</li> </ul>
<i>Unacceptable risks are</i>	<ul style="list-style-type: none"> <li>• those which an organisation has determined have the most potential for harm</li> </ul>
<i>Sources of security risk may include</i>	<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>
<i>Level of risk may be</i>	<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>Treatment options 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>Likelihood of risk may be determined through analysis of</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 and intent) of threat source/s</li> </ul>
<b>Consequences may include</b>	<ul style="list-style-type: none"> <li>• what constitutes harm</li> <li>• degree of harm</li> <li>• who would be affected and how</li> <li>• how much disruption would occur</li> <li>• levels that are: <ul style="list-style-type: none"> <li>• extreme</li> <li>• very high</li> <li>• medium</li> <li>• low</li> <li>• negligible</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>Treatment plans may include</b>	<ul style="list-style-type: none"> <li>• responsibilities</li> <li>• schedules</li> <li>• expected outcomes</li> <li>• budget information</li> <li>• performance measures</li> <li>• monitoring process</li> </ul>
<b>Countermeasures may include</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 <ul style="list-style-type: none"> <li>• personnel-oriented</li> <li>• information-oriented</li> <li>• property-oriented</li> <li>• reputation-oriented</li> </ul> </li> </ul>
<b>Legal requirements, government and organisational policy may include</b>	<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> </ul>

	<ul style="list-style-type: none"> <li>• the organisation's policies and practices</li> <li>• government policy</li> <li>• codes of conduct/codes of ethics</li> <li>• Security Guidelines for Australian Government IT Systems (ACSI 33)</li> <li>• Commonwealth Protective Security Manual</li> <li>• Australian and New Zealand standards – Risk management AS/NZS 4360:1999</li> </ul>
<b>Strategies</b> may include	<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>Monitoring</b> may include	<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>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>

## 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 PSPSEC402A, candidates should provide evidence that confirms implementation of security risk treatments in a range of (3 or more) contexts (or occasions, over time).

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

<b>PSPSEC402A – Implement security risk treatments (Required)</b>	<b>Yes</b>	<b>Not Yet</b>	<b>Not able to comment</b>
Confirming risk decisions			
Identifying risk treatments			
Implementing countermeasures			
Monitoring and reviewing security risk management process			

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

**Referee (Third party) 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:**

