



Recognition Assessment Workbook

PSP41704

Certificate IV in Government (Personnel 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
PSP41704 Certificate IV in Government (Personnel Security) program training strategy.....	4
PSP41704 Certificate IV in Government (Personnel 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 (Personnel Security).....	14
Part 5: Units of competency.....	15
PSPETHC401A – Uphold and support the values and principles of public service (Required)	20
PSPGOV408A – Value diversity (Required).....	26
PSPLEGN401A – Encourage compliance with legislation in the public sector (Required)	30
PSPOHS301A – Contribute to workplace safety (Chosen required elective).....	34
PSPREG415A – Receive and validate data (Chosen required elective).....	38
PSPSEC404A – Conduct personnel security assessments (Chosen required elective).....	42
PSPSEC405A – Handle security classified information (Required).....	47
PSPGOV412A – Use advanced workplace communication strategies (Required).....	52
PSPGOV413A – Compose complex workplace documents (Chosen required elective).....	57
PSPGOV422A - Apply government processes (Required).....	61
PSPREG411A – Gather information through interviews (Required).....	66
PSPREG416A – Conduct data analysis (Required).....	69
PSPSEC406A – Provide government security briefings (Required).....	72
PSPSEC401A – Undertake government security risk analysis (Required).....	78
PSPSEC402A – Implement security risk treatments (Required).....	84

Introduction

Welcome to the PSP41704 Certificate IV in Government (Personnel 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 (Personnel Security) you will need to demonstrate your competency in at least 15 units of competency of which 12 units are required and 3 units are chosen electives.

Unit of competency	Assessment Strategy
PSPETHC401A - Uphold & support the values and principles of public service * PSPGOV408A - Value diversity * PSPLEGN401A - Encourage compliance with legislation in the public sector * 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>
PSPREG415A – Receive and validate data ** PSPSEC404A – Conduct personnel security assessments * PSPSEC405A - Handle security classified information *	Partially delivered and assessed through the Introduction to Personnel Security course. Also assessed by recognition evidence and confirmed by third party referee reports.
PSPGOV412A – Use advanced workplace communication strategies * PSPGOV413A – Compose complex workplace documents ** PSPGOV422A - Apply government processes * PSPREG411A - Gather information through interviews * PSPREG416A – Conduct data analysis * PSPSEC406A - Provide government security briefings *	Partially delivered and assessed through the Advanced Personnel Security course. Also assessed by recognition evidence and confirmed by third party referee reports.

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

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

PSP41704 Certificate IV in Government (Personnel Security) program training strategy

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

- Five day Introduction to Personnel Security course
- Two day Introduction to Security Risk Management course
- Five day Advanced Personnel Security course

PSP41704 Certificate IV in Government (Personnel 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 Personnel Security (IPERS) course
- Introduction to Security Risk Management (ISRM) course
- Advanced Personnel Security (APERS) 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/letters 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

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"/>	
If Yes		
What occupation were you trained in?		
Training completion Date (month, year)		
Country where you trained		

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

Part 2: Candidate's employment history

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

Attach additional sheet if required

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

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

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

Part 3: Candidate's self-assessment summary

Unit of competency	I have performed these tasks (please tick)		
	Frequently	Sometimes	Never
PSPETHC401A - Uphold & support the values and principles of public service *			
PSPGOV408A - Value diversity *			
PSPLEGN401A - Encourage compliance with legislation in the public sector *			
PSPOHS301A - Contribute to workplace safety **			
PSPREG415A – Receive and validate data **			
PSPSEC404A – Conduct personnel security assessments *			
PSPSEC405A - Handle security classified information *			
PSPGOV412A – Use advanced workplace communication strategies *			
PSPGOV413A – Compose complex workplace documents **			
PSPGOV422A - Apply government processes *			
PSPREG411A - Gather information through interviews*			
PSPREG416A – Conduct data analysis *			
PSPSEC406A - Provide government security briefings *			
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 (Personnel 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:

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

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 PSP41704 Certificate IV in Government (Personnel 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 PSP41704 Certificate IV in Government (Personnel 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

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

Introduction

This is a required unit of competency in the PSP41704 Certificate IV in Government (Personnel 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><i>Ethical values and principles may include</i></p>	<ul style="list-style-type: none"> • respect for the law • integrity • objectivity • accountability • honesty • openness • responsibility • impartiality • diligence • trustworthiness • confidentiality • respect for persons • responsible care • probity • economy and efficiency • natural justice/procedural fairness, that is: <ul style="list-style-type: none"> ○ the right to be heard/put your case ○ the right to be informed of a complaint or case against you ○ the right to know reasons for decisions affecting you ○ the right to know the outcomes/recommendations of an investigation involving you ○ the right to privacy ○ the right to representation ○ the right to silence ○ the decision maker should not be a judge in his/her own cause
<p><i>Others may include</i></p>	<ul style="list-style-type: none"> • colleagues • supervised staff • contractors
<p><i>Legislation and guidelines may include</i></p>	<ul style="list-style-type: none"> • legislation for public sector management • freedom of information • privacy legislation • equal employment opportunity and anti-discrimination law • public sector standards • Ministerial directions • State/Territory/Commonwealth codes of ethics • organisational codes for conduct/ethics • organisational mission and values statements

	<ul style="list-style-type: none"> • organisational policy, procedures/guidelines • government policy • professional codes of ethics and conduct • equity guidelines, organisational workplace diversity guidelines
Unethical conduct may include	<ul style="list-style-type: none"> • fraud, corruption, maladministration and waste • unauthorised access to and/or use of information, money/finances, vehicles, equipment, resources, time • improper actions during contractual processes, such as release of intellectual property, infringing copyright, release of tender information, inappropriate disclosure during tender process • improper public comment on matters relating to the government and/or the organisation • falsifying records • giving false testimonials • dishonesty • improper use of plant and equipment, credit cards, frequent flyer points, telephones, email and Internet • extravagant or wasteful practices • personal favours • preferential treatment • putting barriers in place, hindering, blocking action • compromising behaviour including sexual harassment • lack of confidentiality • directing others to act unethically • oppressive/coercive management decisions • resorting to illegality to obtain evidence
Ethical problems which may need to be referred rather than resolved at this level may include	<ul style="list-style-type: none"> • conflict between public sector standards and personal values • conflict between public sector standards and other standards such as professional standards • conflict between public sector standards and directions of a senior officer or Minister • tension between two 'rights' – for example, the right to privacy versus the right to freedom of information • conflict regarding issues of personal and organisational intellectual property
Referrals of ethical problems may be made to	<ul style="list-style-type: none"> • line management • human resources • workplace relations officer or grievance officer • chief executive officer • public service commissioner • public sector standards body • organisational ethics committee

	<ul style="list-style-type: none">• internal grievance mechanisms• confidant programs (whistleblower protection programs)• organisational professional reporting procedures• unions and professional bodies• ombudsman
--	--

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.

Do you consistently meet your organisation's performance standards for:			
PSPETHC401A – Uphold and support the values and principles of public service (Required)	Yes	Not Yet	Not able to comment
Contributing to an ethical public sector workplace			
Participating in ethical decision making			
Candidate's Comments and Attachment/s number as included in Portfolio of Evidence:			
Referee (Third party) Comments:			
<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>			
Signature of Referee:		Date:	
<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>			
Signature of Candidate:		Date:	

PSPGOV408A - Value diversity

Introduction

This is a required unit of competency in the PSP41704 Certificate IV in Government (Personnel 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>Diversity may include</p>	<ul style="list-style-type: none"> • age • cultural background • educational level • ethnicity • expertise • family responsibilities • gender • interests • interpersonal approach • language • life experience • marital status • not fitting the dominant paradigm of the organisation • personality • physical ability • political orientation • religious belief • sexual orientation • socio-economic background • thinking/learning styles • work experience • working styles.
<p>Workplace diversity issues may include</p>	<ul style="list-style-type: none"> • equal employment opportunity issues such as: • direct and indirect discrimination – discriminatory systems and practices • harassment • racism • under-representation of equity groups in the public sector • employment of equity groups concentrated at lower levels in the public sector • women making up more than half of the public sector workforce but disproportionately represented at lower salary levels • barrier (or glass ceiling) that prevents equity group members progressing to higher salary levels • disproportionate representation of equity group members in non-permanent, casual or contract positions • inappropriate supervisory treatment of equity group members • culturally inappropriate workplaces • enabling access to buildings to people with a disability • making reasonable adjustment to work processes. • quality of service delivery to clients from diverse backgrounds • sidelining staff from diverse backgrounds to 'diversity roles' rather than the opportunity to pursue what interests them, or where they add

	<p>most value</p> <ul style="list-style-type: none"> • people from recognised diversity groups choosing not to be identified through usual statistical collection methods • workplace systems or practices that don't allow a balance between work and family responsibilities • inequitable access to acting opportunities, workplace training and development • questioning/disregarding the dominant paradigm of the organisation • inappropriate treatment of those who don't fit the dominant paradigm of the organisation • risks associated with diversity not managed • different values: <ul style="list-style-type: none"> • uncertainty avoidance • collectivist/individualist • power/distance • masculine/feminine • resolving communication issues • developing cultural competence • negotiating commonalities • resolving conflict • negotiating difference
Benefits of diversity may include	<ul style="list-style-type: none"> • improved client service – internal and external • improved service delivery • promotion of equity and fairness • improved access for clients from diverse backgrounds to government services and programs • improved relationship with the community • wider sources of recruitment • greater responsiveness to change • cultural enrichment • promotion of creativity • creation of a harmonious and supportive work environment • retention of staff • facilitation of attainment of organisation goals • increased skills and experience added to the workplace • a workforce representative of the client base • a balanced workforce in terms of age, gender, race and culture
Promotion of training and awareness programs may include	<ul style="list-style-type: none"> • word of mouth • memos • emails • flyers • intranet
Legislation, policy and guidelines may include	<ul style="list-style-type: none"> • Commonwealth and State/Territory legislation addressing diversity issues for example: <ul style="list-style-type: none"> • Racial Discrimination Act 1975

	<ul style="list-style-type: none"> • Sex Discrimination Act 1984 • Disability Discrimination Act 1992 • Workplace Relations Act 1996 • Privacy Act 1988 • Human Rights and Equal Opportunity Commission Act 1984 • Equal Opportunity for Women in the Workplace Act 1999. • public service/public sector management acts • workplace diversity guidelines/program • national and international codes of practice and standards • the organisation's plans, strategies and policies relating to diversity • policies relating to language services • government policy mandating equal employment opportunity and/or workplace diversity requirements, such as: <ul style="list-style-type: none"> ○ Managing diversity in the Western Australian public sector, August 1995 ○ Valuing cultural diversity, State of Victoria, 2002. ○ public sector ethics/values/codes of conduct ○ Public Sector Management Standards (subordinate law) ○ Commissioner's directions/instructions ○ community guidelines, policy and practices (such as those within Aboriginal and Torres Strait Islander communities)
<p>Communication styles may include</p>	<ul style="list-style-type: none"> • plain English • language in active rather than passive voice • simple sentence structure even though content may be complex • lack of jargon and acronyms • culturally appropriate body language • oral or written use of graphics and illustrations • use of colour • reader-friendly layout • effective paragraphing • different languages • interpreting and translating • use of different media eg online

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:			
PSPGOV408A – Value diversity (Required)	Yes	Not Yet	Not able to comment
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 Comments:			
<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>			
Signature of Referee:			Date:
<i>I agree with the statements above and that I have met the knowledge and skill requirements in this unit of competency.</i>			
Signature of Candidate:			Date:

PSPLEGN401A - Encourage compliance with legislation in the public sector

Introduction

This is a required unit of competency in the PSP41704 Certificate IV in Government (Personnel 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>Legislation and guidelines may relate to</p>	<ul style="list-style-type: none"> • public sector standards: <ul style="list-style-type: none"> codes of conduct/ethics guarantee of service legislated standards State/Territory/Commonwealth/organisational standards technical/industrial standards professional standards industry competency standards anti-corruption legislation whistleblowers' protection • public sector employment: <ul style="list-style-type: none"> ○ employee relations ○ chief executive officer's instructions ○ Commissioner's instructions ○ public sector notices • workplace environment: <ul style="list-style-type: none"> ○ equal employment opportunity ○ affirmative action ○ workplace diversity ○ anti-discrimination ○ workplace harassment ○ occupational health and safety ○ duty of care ○ security, storage, handling and classification of documents • financial management and accountability <ul style="list-style-type: none"> ○ Treasurer's instructions ○ contractual obligations • transparency: <ul style="list-style-type: none"> ○ freedom of information ○ professional reporting ○ accountability ○ fair trading • business and community: <ul style="list-style-type: none"> ○ privacy ○ trade practices ○ competition ○ road transport legislation • information and records management standards and legislation • the organisation's enabling legislation, regulations • aspects of common law, criminal law, contract law, employment law and administrative law, including judges' rules • International legislation/codes of behaviour
<p>Others may include</p>	<ul style="list-style-type: none"> • colleagues • supervised staff • contractors

<p><i>Consequences of non-compliance may include</i></p>	<ul style="list-style-type: none"> • for individuals: <ul style="list-style-type: none"> ○ counselling ○ disciplinary action ○ transfer, demotion, dismissal ○ legal liability ○ fine • External consequences, for example: <ul style="list-style-type: none"> ○ to clients ○ to the organisation's reputation
<p><i>Conflicting legislative requirements may include</i></p>	<ul style="list-style-type: none"> • apparent contradiction between statutes • apparent conflict between statutes and policy requirements • contradictions between different policy requirements • contradictions within a single piece of legislation
<p><i>Inadequacies in workplace procedures may include</i></p>	<ul style="list-style-type: none"> • insufficient financial/other controls • insecure Internet/fax access • unauditible records processes • ambiguous guidelines • no guidelines • unnecessary complexity • use of non-current legislation

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:

PSPLEGN401A – Encourage compliance with legislation in the public sector (Required)	Yes	Not Yet	Not able to comment
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 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 PSP41704 Certificate IV in Government (Personnel 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 issues may include	<ul style="list-style-type: none">● hazards relating to the physical environment● workplace stress● conflict● bullying● harassment
Designated personnel may include	<ul style="list-style-type: none">● supervisors● managers● team leaders

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

	<ul style="list-style-type: none"> • incident and near miss reporting and recording procedures • consultation on occupational health and safety issues • correct selection, use, storage and maintenance procedures for use of personal protective equipment • risk control procedures
Controlling risks may include actions such as	<ul style="list-style-type: none"> • consultation with others • measures to remove the cause of the risk at its source • application of the hierarchy of control, namely: <ul style="list-style-type: none"> ○ elimination ○ substitution ○ engineering controls ○ administrative controls ○ personal protective equipment
Other hazardous events may include	<ul style="list-style-type: none"> • fires • bomb threats • chemical spills • occupational violence • natural disasters/events • terrorist attacks

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:

PSPOHS301A – Contribute to workplace safety (Chosen required elective)	Yes	Not Yet	Not able to comment
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 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:

PSPREG415A – Receive and validate data

Introduction

This is a chosen required elective unit of competency in the PSP41704 Certificate IV in Government (Personnel Security) and covers activities related to handling data received from a variety of sources which may then be acted upon or referred for further action. It includes receiving and recording data, verifying its authenticity and recommending/taking action as a result.

Being competent in this unit means being able to:

Receive information

This element requires:

- Required **information** is identified, requested and/or received in accordance with legislative powers, organisational policy and procedures
- Incoming information is checked for gaps, anomalies, deficiencies or discrepancies, and compared with pre-existing information, where relevant
- Additional **data sources** are accessed and information is obtained to fill gaps and compare with information received
- Incoming information is received if required in accordance with organisational policy and procedures

Record information

This element requires:

- Accurate recording of information is carried out in line with organisational procedures, confirming relevant details of source
- Records are maintained as accurate, complete and up-to-date and are presented in the required format
- Legislative requirements for recording and storage of information are complied with
- Procedures for storage and management of confidential and sensitive information are adhered to

Verify authenticity of information

This element requires:

- Initial selection of information is completed using preliminary cull to eliminate unreliable data
- Information is corroborated and assessed for its integrity, validity and reliability
- Validation or corroboration is carried out with existing information as well as information from outside organisations and other sources where relevant
- Useful and useable information is extracted, interpreted and organised in a form that is accessible to users
- Analysis is conducted in accordance with agreed indicators and assessment is accurate, relevant and complete

Recommend/take action as a result of information received

This element requires:

- Outcomes are recorded and reported in accordance with organisational policy and procedures
- Actions are recommended or taken as a result of the outcomes
- Decision is documented showing reasons for proceeding/not proceeding or taking other action, after discussion with management, where required
- Areas or other organisations that may be affected by information received or outcomes, are identified and informed, in accordance with organisational procedures and legislative requirements, to optimise usefulness of information

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><i>Information may be</i></p>	<ul style="list-style-type: none"> ● written ● oral ● photographic ● electronic ● classified ● not in the public domain ● financial ● personal: ● academic qualifications/academic transcripts ● birth certificate ● citizenship ● decree nisi/decrece absolute ● deed poll ● discharge certificate ● employment histories ● marriage certificate ● passport ● travel documents ● about clients or staff ● checked for age, compatibility and validity
<p><i>Data sources may include</i></p>	<ul style="list-style-type: none"> ● applications ● correspondence ● declarations ● diary entries ● electronic records ● email ● fax records ● files ● graphics ● incident reports

	<ul style="list-style-type: none">• Internet/intranet• notes• personal records• pager records• security records• security risk management plans• telephone messages• video images• information provided under public interest disclosures, protected disclosures or whistleblowing legislation
--	--

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 PSPREG415A, candidates should provide evidence that confirms receipt and validation of data in a range of (3 or more) contexts (or occasions, over time).

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

PSPREG415A – Receive and validate data (Chosen required elective)	Yes	Not Yet	Not able to comment
Receiving information			
Recording information			
Verifying authenticity of information			
Recommending/taking action as a result of information received			

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

Referee Comments:

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

Signature of Referee: **Date:**

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

Signature of Candidate: **Date:**

PSPSEC404A – Conduct personnel security assessments

Introduction

This is a required unit of competency in the PSP41704 Certificate IV in Government (Personnel Security) and covers the conduct of personnel security assessments to ensure that government staff and contractors who have access to security classified information meet general suitability indicators. It includes collecting, analysing and evaluating personal information, making recommendations on security assessment outcomes, and recording and reporting on personnel security assessments.

Being competent in this unit means being able to:

Collect, analyse and evaluate personal information

This element requires:

- **Information** is collected from the subject to be assessed in accordance with the purpose of the **security assessment**
- Where gaps, anomalies, deficiencies or discrepancies exist in the information provided, additional information is obtained in accordance with organisational policy and procedures
- Information is **corroborated** in accordance with organisational policy and procedures and **assessed** for its validity and reliability
- Analysis is conducted in accordance with general suitability indicators in accordance with **legislation and security standards**
- Data is extracted and interpreted and outcomes are recorded in accordance with organisational policy and procedures
- Assessment process is conducted with care and sensitivity to assist subjects to deal with its discriminatory and intrusive nature

Make recommendations on security assessment outcomes

This element requires:

- **Recommendations** are formulated consistent with the information obtained
- Recommendations are consistent with organisational guidelines and security standards
- Recommendations are conveyed in accordance with organisational guidelines
- Where recommendations are negative, the right to seek a review of the decision is confirmed with the requester of the security assessment and the subject, where appropriate, in accordance with organisational policy and procedures
- Improvements to procedures are recommended as required as part of the cycle of continuous improvement

Record and report on personnel security assessments

This element requires:

- Accurate, **complete**, up-to-date records are presented in the required format

- **Reports** are prepared that are clear, fair and objective and use language suited to the purpose of the report and organisational requirements
- Reports are presented in the required format
- Urgency and levels of risk are addressed in reports
- Procedures for storage and management of confidential and sensitive information are adhered to

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.

Information may include	<ul style="list-style-type: none"> • birth certificate • marriage certificate • decree nisi/decre absolute • deed poll • academic qualifications/academic transcripts • employment histories • citizenship • passport • defence forces discharge certificate
Security assessment may be for	<ul style="list-style-type: none"> • initial evaluation • re-evaluation • temporary access • emergency access • provisional access • limited higher access
Corroboration of information may be with	<ul style="list-style-type: none"> • official records • referee reports • employer records • third party reports
Assessment of information may relate to	<ul style="list-style-type: none"> • character • attributes • background • actions • anything in a person's background or lifestyle likely to pose a security threat
Legislation and security standards may include those referred to in	<ul style="list-style-type: none"> • Public Service Acts • Protective security policy • Fraud control policy • Crimes Act 1914 • Criminal Code 1985 • Freedom of Information Act 1982 • Privacy Act 1988 • Occupational Health and Safety acts • Australian standards such as Risk management AS/NZS 4360:1999 and 2004 • Security Guidelines for Australian Government IT

	Systems (ISM – formerly ACSI 33) <ul style="list-style-type: none"> • Commonwealth Protective Security Manual (PSM)
Recommendations may relate to	<ul style="list-style-type: none"> • assessment of suitability • action required
Completeness of records includes	<ul style="list-style-type: none"> • request from someone other than the subject, such as a supervisor • despatch of information pack/forms • all enquiries and responses • receipt of incoming documents • consent to collect/corroborate information • personal security file
Reports may include	<ul style="list-style-type: none"> • interview reports • assessment reports • case notes • incidents • records of interview • notes for file

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 PSPSEC404A, candidates should provide evidence that confirms conduct of personnel security assessments in a range of (3 or more) contexts (or occasions, over time).

Do you consistently meet your organisation's performance standards for:			
PSPSEC404A – Conduct personnel security assessments (Chosen required elective)	Yes	Not Yet	Not able to comment
Collecting, analysing and evaluating personal information by <ul style="list-style-type: none"> ▪ Managing a Personnel Security File (PSF) ▪ Liaising with candidate ▪ Explaining the clearance process ▪ Explaining the types of security clearances ▪ Reviewing personal documentation ▪ Establishing proof of identity ▪ Requesting and assessing a Police Records Check ▪ Requesting and assessing an ASIO assessment ▪ Conducting referee interviews ▪ Analysing the PSF to identify gaps, anomalies and discrepancies ▪ Conducting factor analysis of candidate 			
Making recommendations on security assessment outcomes by: <ul style="list-style-type: none"> ▪ Demonstrating knowledge of the security assessing review process for: <ul style="list-style-type: none"> ○ Re-validation ○ Re-evaluation ○ Review for cause 			
Recording and reporting on personnel security assessments by: <ul style="list-style-type: none"> ▪ Compiling delegate reports based on outcomes of file and explaining: <ul style="list-style-type: none"> ○ appeal provisions ○ temporary clearance process ○ separation process 			
Candidate's Comments and Attachment/s number as included in Portfolio of Evidence:			

Referee Comments:

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

Signature of Referee:

Date:

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

Signature of Candidate:

Date:

PSPSEC405A – Handle security classified information

Introduction

This is a required unit of competency in the PSP41704 Certificate IV in Government (Personnel 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.

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

<p>Securing practices may include</p>	<ul style="list-style-type: none"> • correct filing • clean desk • quitting all electronic systems and networks • checking environment including: <ul style="list-style-type: none"> • desks • whiteboards • waste bins • computer drives • containers • cabinets • safes • vaults • windows • doors • safe carriage of keys
<p>Accounting for security classified information may include</p>	<ul style="list-style-type: none"> • audit • spot checks • correct notation or markings • file records • transmission records • receipts
<p>Methods of disposal may include</p>	<ul style="list-style-type: none"> • pulping • burning • pulverisation • shredding • overwriting • degaussing • destruction • archiving

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:

PSPSEC405A – Handle security classified information (Required)	Yes	Not Yet	Not able to comment
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 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 PSP41704 Certificate IV in Government (Personnel 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.

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

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

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:

PSPGOV412A – Use advanced workplace communication strategies (Required)	Yes	Not Yet	Not able to comment
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 Comments:

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

Signature of Referee: _____ **Date:** _____

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

Signature of Candidate: _____ **Date:** _____

PSPGOV413A – Compose complex workplace documents

Introduction

This is a chosen required elective unit of competency in the PSP41704 Certificate IV in Government (Personnel Security) and covers written communication involving the evaluation and composition of complex workplace documents. It includes interpreting and evaluating workplace information, composing complex written materials and editing

Being competent in this unit means being able to:

Interpret and evaluate workplace information

This element requires:

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

Compose complex written materials

This element requires:

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

Edit written material

This element requires:

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

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>Information for evaluation may include</p>	<ul style="list-style-type: none"> • applications • briefing papers • discussion papers • expert opinion • literature • minutes • project briefs • reports • research • speeches • strategic and operational plans • submissions • web site information
<p>Purpose may include</p>	<ul style="list-style-type: none"> • to influence opinion • to report on achievement • to recommend options and corresponding actions • to meet regulatory requirements • to meet public sector reporting requirements • to develop policy • to document policy • to obtain funding • to provide briefing material • to provide or contribute to strategic planning • to respond to enquiries/complaints

<p>Materials to be composed <i>may include</i></p>	<ul style="list-style-type: none"> • position papers • discussion papers • briefing materials • funding submissions • business cases • project briefs • reports • operational and other plans
<p>Content, structure and sequencing <i>may include</i></p>	<ul style="list-style-type: none"> • facts and observations • case studies • critical analysis • opinion • creative ideas • recommendations and supporting arguments • anticipated arguments and rebuttals • conclusions • division into chapters or sections • tables of contents and indexes • glossaries • executive summary • précis • chronological structure • alphabetic structure • operating sequence
<p>Organisational and legislative requirements <i>may include</i></p>	<ul style="list-style-type: none"> • use of plain English • style formats • acknowledgements • particular terminology to be used/not used: • acronyms and technical terms • bureaucratic language • abbreviations • requirements for minimising jargon in written materials • requirements for written material to take account of cultural, ethnic, religious or language differences, disabilities, etiquette • guidelines for illustrative items • standards for references, acknowledgements, citations, footnotes, endnotes, bibliographies • particular communication channels • State/Territory or Commonwealth legislation, regulations, policies, procedures and guidelines relating to the preparation and security of written information in the public sector, including freedom of information, copyright, privacy, confidentiality, equal employment opportunity, diversity, occupational health and safety • risk assessment • information security requirements • public sector standards • fraud control standards

	<ul style="list-style-type: none"> • codes of practice • codes of ethics • private or confidential materials • embargoed materials • security requirements • politically sensitive materials • security standards for government information
<i>Information for evaluation may include</i>	<ul style="list-style-type: none"> • applications • briefing papers • discussion papers • expert opinion • literature • minutes • project briefs • reports • research • speeches • strategic and operational plans • submissions • web site information

Evidence Guide

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

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

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

PSPGOV413A – Compose complex workplace documents (Chosen required elective)	Yes	Not Yet	Not able to comment
Interpreting and evaluating workplace information			
Composing complex written materials			
Editing written material			

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

Referee Comments:

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

Signature of Referee:

Date:

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

Signature of Candidate:

Date:

PSPGOV422A - Apply government processes

Introduction

This is a required unit of competency in the PSP41704 Certificate IV in Government (Personnel 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><i>Machinery of Government</i> may include</p>	<ul style="list-style-type: none"> • cycles of government, such as budget cycle • separation of powers (Executive, Judiciary, Legislative) • levels of government (Federal, State/Territory, Local) • legislative process • role and functions of parliamentary structures (unicameral, bicameral) • Cabinet • Ministers • Ministerial portfolios • structure and functions of government departments • quasi-government organisations
<p><i>Information</i> may include</p>	<ul style="list-style-type: none"> • documents • databases • web sites • oral information from: <ul style="list-style-type: none"> ○ managers ○ supervisors ○ colleagues
<p>Organisational <i>structures</i> may include</p>	<ul style="list-style-type: none"> • bureaucratic structure and hierarchy • key personnel and their roles • key organisational functions and accountabilities
<p><i>Protocols</i> may include</p>	<ul style="list-style-type: none"> • forms of address • who may be addressed directly • written protocols/formats for written materials • restrictions relating to contact with: <ul style="list-style-type: none"> ○ Minister's office ○ media ○ members of the public/specific interest groups ○ Members of Parliament ○ other government departments ○ senior management/Board members ○ government and opposition parties

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:

PSPGOV422A - Apply government processes (Required)	Yes	Not Yet	Not able to comment
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 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:

PSPREG411A – Gather information through interviews

Introduction

This is a required unit of competency in the PSP41704 Certificate IV in Government (Personnel Security) and covers gathering information through interviews that do not result in a formal record of interview in the legal sense. Interviews may be conducted in a range of locations for a range of reasons. They may be overt or covert. The unit includes preparing for the interview, conducting the interview, and reviewing and correlating interview information.

Being competent in this unit means being able to:

Prepare for interview

This element requires:

- The need for an interview is determined, and the **context** and **requirements** are established in accordance with **organisational and legislative requirements**
- Interview **planning** is undertaken to ensure desired outcomes are achieved
- Interview arrangements are made in accordance with legislative and organisational requirements
- **Materials** to be used during the interview are prepared as required
- Advice is obtained as required on legislative or administrative issues relating to the conduct of the interview

Conduct interview

This element requires:

- Commencement of the interview is undertaken following organisational **protocols** and complies with legislative requirements
- Interview is conducted in a planned manner, with the sequence evident to others who may use the outcomes
- **Questions** are selected and used that are relevant, comprehensive, appropriate to the situation and the interviewee and adhere to the rules of evidence
- Problem solving skills are used to test, compare and contrast information as it is provided to influence the direction of further questions
- Information is **recorded** in accordance with organisational policy and procedures
- Personal conduct is maintained in accordance with legal and organisational requirements and takes account of cultural and ethical issues

Review and correlate information

This element requires:

- Information is reviewed and clarified to ensure its relevance and sufficiency prior to concluding the interview
- Information is transcribed if necessary and sensitive information is **dealt with** in accordance with organisational policy and procedures

- Detailed analysis is conducted, and incomplete and irregular information is identified and noted or followed up in accordance with the nature of the interview and organisational requirements
- Behavioural characteristics of significance to the purpose of the interview are confirmed
- **Post-interview activities** are undertaken as required 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.

<p>Contexts may include</p>	<ul style="list-style-type: none"> • informal interviews • interviews against set criteria • interviews to assess applications • initial investigation of complaints • audits • intelligence gathering • threat assessment • security vetting • overt interviews • covert interviews, under specific legislative powers
<p>Requirements may include</p>	<ul style="list-style-type: none"> • interview location/environment: <ul style="list-style-type: none"> • office • designated interview room • in the field (including overseas) • private home • at a client/contractor location • in other agencies • timing • personnel present: <ul style="list-style-type: none"> ○ senior staff ○ colleagues ○ interpreter ○ support persons • method of recording: <ul style="list-style-type: none"> ○ tape recording ○ videotaping ○ hand written ○ typewritten/word processed ○ file notes • equipment: <ul style="list-style-type: none"> ○ electronic equipment ○ recording equipment ○ computer equipment • availability of interviewee

<p>Organisational and legislative requirements may include</p>	<ul style="list-style-type: none"> • organisational policy, procedures and guidelines • international treaties and protocols • cross-jurisdictional protocols • organisation's strategic objectives • national strategic objectives • security constraints • public sector codes of conduct/ethics • confidentiality requirements • Commonwealth, State/Territory or Local Government legislation such as: <ul style="list-style-type: none"> ○ Freedom of Information Act 1982 ○ Privacy Act 1988 ○ Archives Act ○ Crimes Act 1914 and Criminal Code 1995 ○ Evidence Act ○ the organisation's enabling legislation
<p>Interview planning may include</p>	<ul style="list-style-type: none"> • purpose • structure • context • expectations • intended/desired outcomes • criteria for assessment • risk management considerations • key questions in sequential order, highlighting main points • assessing sources of information • interview strategies appropriate to the situation and purpose of the interview, such as: <ul style="list-style-type: none"> ○ direct questioning ○ empathetic questioning ○ investigative interviewing ○ exclusion of leading questions • avoidance of cross-examination • safety requirements for interviewer, interviewee and others present
<p>Materials may include</p>	<ul style="list-style-type: none"> • paper-based and electronic documents, including: <ul style="list-style-type: none"> ○ maps ○ photographs ○ videotapes ○ physical objects and materials ○ audiotapes
<p>Commencement protocols may include</p>	<ul style="list-style-type: none"> • introductions • producing identification/authority • explaining the purpose, process and recording requirements • confirming confidentiality of information, if appropriate to the interview purpose

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 PSPREG411A, candidates should provide evidence that confirms information gathered via interviews in a range of (3 or more) contexts (or occasions, over time).

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

PSPREG411A – Gather information through interviews (Required)	Yes	Not Yet	Not able to comment
Preparing for interview			
Conducting interview			
Reviewing and correlating information			

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

Referee Comments:

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

Signature of Referee:

Date:

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

Signature of Candidate:

Date:

PSPREG416A – Conduct data analysis

Introduction

This is a required unit of competency in the PSP41704 Certificate IV in Government (Personnel Security) and covers activities involved in analysing and matching data from a range of sources. It includes analysing information, and documenting outcomes of the analysis.

Being competent in this unit means being able to:

Analyse data

This element requires:

- **Analysis** is undertaken dependent upon the nature of the data and intended purpose of the analysis
- **Methods of analysis** are selected in accordance with any relevant industry standards, precedents and techniques
- Trends are identified and inferences drawn in light of environmental and cultural factors relevant to the particular situation
- The chain of reasoning in formulating inferences is made clear to ensure transparency to users of the data
- A proactive approach is taken to identify and assess the need for new or changed systems and processes for analysing data to more effectively meet objectives

Document outcomes of analysis

This element requires:

- Recommended actions are based upon analysis of **data** in the context of the purpose of the analysis and the objectives and priorities of the organisation's strategies and plans
- Links between the outcomes proposed as a result of the data analysis and the organisation's strategies are made clear to the intended audience
- Timely and relevant reports are completed and disseminated to appropriate staff and management
- Results of data analysis are **incorporated** into ongoing review of organisational strategies and plans
- Documentation is prepared that is clear, concise and accessible to all relevant staff

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>Analysis can be</i>	<ul style="list-style-type: none">• quantitative and/or qualitative• explorative• descriptive• causative• predictive
<i>Methods of analysis can include</i>	<ul style="list-style-type: none">• hypothesis development• link analysis• comparative analysis• biographical analysis• demographic or geographic analysis• historical analysis• scenario generation• delphi technique• morphological analysis
<i>Data sources may include</i>	<ul style="list-style-type: none">• program files• agency systems• other agencies• law enforcement agencies• standards setting organisations
<i>Incorporation may be in terms of</i>	<ul style="list-style-type: none">• identifying and assessing risk• monitoring and reviewing procedures

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 PSPREG416A, candidates should provide evidence that confirms analysis of data in a range of (3 or more) contexts (or occasions, over time).

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

PSPREG416A – Conduct data analysis (Required)	Yes	Not Yet	Not able to comment
Documenting outcomes of analysis			
Analysing data			

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

Referee Comments:

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

Signature of Referee:

Date:

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

Signature of Candidate:

Date:

PSPSEC406A – Provide government security briefings

Introduction

This is a required unit of competency in the PSP41704 Certificate IV in Government (Personnel 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.

<i>Need for briefing may be determined by</i>	<ul style="list-style-type: none"> • organisational policy • change in circumstances • security incident/s
<i>Security briefing may be</i>	<ul style="list-style-type: none"> • ad hoc • incident related • on induction • on initial clearance • on revalidation • on clearance upgrade • on clearance downgrade • overseas • high risk • a debriefing
<i>Methodology may include</i>	<ul style="list-style-type: none"> • facilitator-led • collaborative • problem-based • descriptive • illustrative • formality of language and structure
<i>Briefing plan may include</i>	<ul style="list-style-type: none"> • purpose • subject matter • timing • location • participant/s • methodology

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).

PSPSEC401A – Undertake government security risk analysis

Introduction

This is a required unit of competency in the PSP41704 Certificate IV in Government (Personnel 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.

Strategic context may include	<ul style="list-style-type: none">• the relationship between the organisation and the environment in which it operates• organisational structure• the organisation's functions:<ul style="list-style-type: none">• political• operational• financial• social• legal• commercial• the various stakeholders and clients
Organisational context may include	<ul style="list-style-type: none">• the organisation, how it is organised, and its capabilities• any official resources, including physical areas and assets, that are vital to the operation of the organisation• key operational elements of the organisation• any major projects

<p>Stakeholders may include</p>	<ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • employees at all levels of the organisation • community • clients • other public sector organisations • union and association representatives • boards of management • government • Ministers
<p>Legislation, policy and procedures may include</p>	<ul style="list-style-type: none"> • Commonwealth and State/Territory legislation including equal employment opportunity, occupational health and safety, privacy and anti-discrimination law • national and international codes of practice and standards • the organisation's policies and practices • government policy • codes of conduct/codes of ethics • Security Guidelines for Australian Government IT Systems (ACSI 33) • Commonwealth Protective Security Manual • Australian and New Zealand standards – Risk management AS/NZS 4360:1999
<p>Security risk criteria may concern</p>	<ul style="list-style-type: none"> • vital functions and capabilities • the expectations of stakeholders and clients • the personal security of employees and clients • general expectations about confidentiality • the availability of the organisation's official resources
<p>Risk may be to</p>	<ul style="list-style-type: none"> • personnel • information • property • reputation
<p>Sources of security risk may include</p>	<ul style="list-style-type: none"> • technical • actual events • political circumstances • human behaviour • environmental • conflict • terrorism • internal • external • local • national • international

Specified methodology or tools may be	<ul style="list-style-type: none"> • qualitative and/or semi-quantitative and/or quantitative • brainstorming • focus groups • expert judgment • strengths, weaknesses, opportunities, threats (SWOT) analysis • analysis of risk registers • examination of available data such as audit results, incident reports • nomogram • risk matrix • scenario analysis • business continuity planning
Threat assessment	<ul style="list-style-type: none"> • is used to provide information about people and events that may pose a threat to a particular resource or function • evaluates and discusses the likelihood of a threat being realised • determines the potential of a threat to actually cause harm
Threats may be	<ul style="list-style-type: none"> • criminal • terrorist • from foreign intelligence services • from commercial/industrial competitors • from malicious people • real or perceived
Risk exposure is	<ul style="list-style-type: none"> • a measure of how open a resource is to harm, or • the potential of a resource to attract harm
Likelihood of risk may be determined through analysis of	<ul style="list-style-type: none"> • current controls to deter, detect or prevent harm • effectiveness of current controls • level of exposure • threat assessment • determination of threat source/s • competence/capability of threat source/s • opportunity for threat to occur
Consequences may include	<ul style="list-style-type: none"> • degree of harm • who would be affected and how • how much disruption would occur • damage to: <ul style="list-style-type: none"> • the organisation • other organisations • government • third parties
Critical lead time for recovery is	<ul style="list-style-type: none"> • the period of time a function is compromised • critical if the function is vital to the organisation

<i>Risk ratings may include</i>	<ul style="list-style-type: none"> • severe • high • major • significant • moderate • low • trivial
<i>Security risk register may include</i>	<ul style="list-style-type: none"> • source • nature • existing controls • likelihood • consequences • initial rating • vulnerability

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).

PSPSEC402A – Implement security risk treatments

Introduction

This is a required unit of competency in the PSP41704 Certificate IV in Government (Personnel 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"> • personnel • information • property • reputation
<i>Acceptable risks are</i>	<ul style="list-style-type: none"> • those which an organisation has determined have the least potential for harm
<i>Unacceptable risks are</i>	<ul style="list-style-type: none"> • those which an organisation has determined have the most potential for harm
<i>Sources of security risk may include</i>	<ul style="list-style-type: none"> • technical • actual events • political circumstances • human behaviour • environmental • conflict • terrorism • internal • external • local • national • international
<i>Level of risk may be</i>	<ul style="list-style-type: none"> • severe • high • major • significant

	<ul style="list-style-type: none"> • moderate • low • trivial
Treatment options may include	<ul style="list-style-type: none"> • addition of security measures • reduction of security measures • avoiding the risk through change of practice • acceptance of residual risk • minimisation of harm through response mechanisms • accepting the risk
Likelihood of risk may be determined through analysis of	<ul style="list-style-type: none"> • current controls to deter, detect or prevent harm • effectiveness of current controls • level of exposure • threat assessment • determination of threat source/s • competence (capability and intent) of threat source/s
Consequences may include	<ul style="list-style-type: none"> • what constitutes harm • degree of harm • who would be affected and how • how much disruption would occur • levels that are: <ul style="list-style-type: none"> • extreme • very high • medium • low • negligible
Continuity plans	<ul style="list-style-type: none"> • may lessen the adverse consequences of risk • 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
Treatment plans may include	<ul style="list-style-type: none"> • responsibilities • schedules • expected outcomes • budget information • performance measures • monitoring process
Countermeasures may include	<ul style="list-style-type: none"> • revision of agency security plan • upgrade of existing security • installation of new security measures • technical controls • training <ul style="list-style-type: none"> • personnel-oriented • information-oriented • property-oriented • reputation-oriented

<p>Legal requirements, government and organisational policy may include</p>	<ul style="list-style-type: none"> • Commonwealth and State/Territory legislation including equal employment opportunity, occupational health and safety, privacy and anti-discrimination law • access and equity • ethics and accountability • national and international codes of practice and standards • the organisation's policies and practices • government policy • codes of conduct/codes of ethics • Security Guidelines for Australian Government IT Systems (ACSI 33) • Commonwealth Protective Security Manual • Australian and New Zealand standards – Risk management AS/NZS 4360:1999
<p>Strategies may include</p>	<ul style="list-style-type: none"> • audits • incident reporting mechanisms • technical controls • systems • rosters • access controls • training
<p>Monitoring may include</p>	<ul style="list-style-type: none"> • regular checking • critical observation • regular recording • information, such as threat assessments, from senior management • reports from business units on current security measures • identification of changes over time such as: <ul style="list-style-type: none"> ○ notification of major changes to business or corporate goals or plans ○ notification of key projects
<p>Stakeholders may include</p>	<ul style="list-style-type: none"> • supervisors • managers • other areas within the organisation • other organisations • government • third parties

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:

PSPSEC402A – Implement security risk treatments (Required)	Yes	Not Yet	Not able to comment
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 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:** _____

