



Recognition Assessment Workbook

PSP30504

Certificate III in Government (Security)

-

Personnel Security Stream

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
PSP30504 Certificate III in Government (Security) – Personnel Security Stream program training strategy.....	4
PSP30504 Certificate III in Government (Security) – Personnel Security Stream 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 III in Government (Security) – Personnel Security Stream.....	14
Part 5: Units of competency	15
PSPETH301B – Uphold the values and principles of public service (Required unit)	20
PSPGOV301B – Work effectively in the organisation (Required unit).....	25
PSPGOV302B – Contribute to workgroup activities (Required unit)	29
PSPGOV308B – Work effectively with diversity (Required unit).....	33
PSPGOV312A – Use workplace communication strategies (Required unit)	38
PSPOHS301A – Contribute to workplace safety (Required unit)	42
PSPLEGN301B – Comply with legislation in the public sector (Required unit)	46
PSPSEC301A – Secure government assets (Chosen required elective)	50
PSPSEC404A – Conduct personnel security assessments (Chosen required elective)	54
PSPSEC405A – Handle security classified information (Required unit).....	59
PSPREG415A – Receive and validate data (Required unit)	63
PSPSEC401A – Undertake government security risk analysis (Required unit)	69
PSPSEC402A – Implement security risk treatments (Chosen required elective).....	75

Introduction

Welcome to the PSP30504 Certificate III in Government (Security) – Personnel Security Stream 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 III in Government (Security) – Personnel Security Stream you will need to demonstrate your competency in at least 11 units of competency of which 10 units are required and 1 unit is a chosen elective. In the Protective Security Training Centre qualification, you will obtain 13 units of competency.

Unit of competency	Assessment Strategy
PSPETHC301B - Uphold the values and principles of public service * PSPGOV301B – Work effectively in the organisation * PSPGOV302B – Contribute to workgroup activities * PSPGOV308B – Work effectively with diversity * PSPGOV312A – Use workplace communication strategies * PSPOHS301A – Contribute to workplace safety *	Generalist units assessed by recognition of your knowledge and skills in the workplace and confirmed by third party referee reports. <i>(Most of 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>
PSPLEGN301B – Comply with legislation in the public sector * PSPSEC301A – Secure government assets ** PSPSEC404A – Conduct personnel security assessments ** PSPSEC405A - Handle security classified information * PSPREG415A – Receive and validate data *	Delivered and partially assessed through the Introduction to Personnel Security course. Also assessed by recognition and confirmed by third party referee reports.

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

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

PSP30504 Certificate III in Government (Security) – Personnel Security Stream program training strategy

The Certificate III in Government (Security) – Personnel Security stream training program is made up of the following two Protective Security Training Centre courses:

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

PSP30504 Certificate III in Government (Security) – Personnel Security Stream program assessment strategy

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

- Introduction to Personnel Security (IPERS) course
- Introduction to Security Risk Management (ISRM) course
- in-class exercises, tests and presentations
- post-course workplace assignments
- Recognition of prior learning / assessment in the workplace

Assignments

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

Units of competency

Units of competency contain a **competency field** that covers the following industry sectors. The **generalist** units of competency are: Ethics and Accountability (ETH); Working in Government (GOV); 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 successfully completed.

How does Assessment by National Recognition work?

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

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

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

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

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

Evidence to support your assessment

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

- 1 **Validity** – refers to the requirement that the evidence be relevant to the competencies being assessed and to current workplace practices.
- 2 **Authenticity** – evidence presented for assessment must be the candidate's own work.
- 3 **Consistency** – refers to the requirements that the portfolio shows a consistent standard over a period of time.
- 4 **Sufficient** – requires that there be sufficient recent evidence to cover all components of competency – task skills, task management skills, contingency skills and job/role environment skills – as well as to provide evidence of competent performance over time.
- 5 **Currency** – demands the assessor be confident that the candidate performs to the standard to demonstrate competency. This is based on performance at this time, so evidence must be provided from either the present or the very recent past.
- 6 **Reliability** – requires that the evidence has come from a reliable and verifiable source.

Types of evidence

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

Evidence Type	Explanation	Examples
Job experience	Details of work history and past and current job experience	Resume or Curriculum Vitae
Job duties	Details work responsibilities and the standard of performance of job tasks	Current and/or recent previous Job Descriptions or Duty Statements
Performance Management	Details standard and competence in the performance of job tasks	PPI, Performance Appraisals Reports, Performance Management Agreements
Work history	Documents that demonstrate completion of relevant workplace training and the capacity to	CV, current and/or previous Job Descriptions, membership of relevant professional associations,

Evidence Type	Explanation	Examples
	apply the skills in the workplace	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 testimonials from 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:

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:

<p>List of Candidate's Portfolio Attachments (documentary evidence): (For example, resume, photos, awards, PM KEYs record etc)</p> <ul style="list-style-type: none"> • • • • • • • • • • • • • • •
--

Part 3: Candidate's self-assessment summary

Unit of competency	I have performed these tasks (please tick)		
	Frequently	Sometimes	Never
PSPETHC301B - Uphold the values and principles of public service *			
PSPGOV301B – Work effectively in the organisation *			
PSPGOV302B – Contribute to workgroup activities *			
PSPGOV308B – Work effectively with diversity *			
PSPGOV312A – Use workplace communication strategies *			
PSPOHS301A – Contribute to workplace safety *			
PSPLEGN301B – Comply with legislation in the public sector *			
PSPSEC301A – Secure government assets **			
PSPSEC404A – Conduct personnel security assessments **			
PSPSEC405A - Handle security classified information *			
PSPREG415A – Receive and validate data *			
PSPSEC401A - Undertake government security risk analysis *			
PSPSEC402A - Implement security risk treatments **			

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

Candidate Declaration

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

Candidate's Signature: _____ **Date:** _____

Part 4: Third Party Referee reports – Certificate III in Government (Security) – Personnel Security Stream

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 PSP30504 Certificate III in Government (Security) – Personnel Security Stream. 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 PSP30504 Certificate III in Government (Security) – Personnel Security Stream, 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

PSPETHC301B - Uphold the values and principles of public service

Introduction

This is a required unit of competency in the PSP30504 Certificate III in Government (Security) – Personnel Security Stream and describes the outcomes required to demonstrate ethical conduct required of those in public service. It includes applying ethical standards and dealing with ethical problems.

Being competent in this unit means being able to:

Apply ethical standards

This element requires:

- Interpretation of **ethical values and principles** is reviewed with senior staff to ensure accuracy
- Personal **work practices** are undertaken in compliance with public sector ethics standards, organisational policy and **guidelines**
- Verbal and written advice and reports are prepared containing information which is impartial, substantiated, accurate and complete
- Public **resources** are **used** in accordance with public sector ethics standards, organisational policy and guidelines
- **Conflicts of interest** are identified, declared, addressed and documented in accordance with policy and procedures
- Personal behaviour and relationships with the public, suppliers and business contacts are conducted in accordance with ethics standards, policy and guidelines

Deal with ethical problems

This element requires:

- Situations which pose ethical problems are resolved or **referred** in accordance with organisational guidelines
- Decision-making **processes** used to resolve ethical problems are recorded in accordance with organisational policy and procedures
- Organisational policies/codes on the prevention and reporting of **unethical conduct** are accessed and applied

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>Ethical values and principles may include</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>Work practices may include</p>	<ul style="list-style-type: none"> • behaviours • conduct • relationships with work colleagues, external individuals and organisations • the manner in which work activities are carried out
<p>Legislation and guidelines may include</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 • organisational policy, procedures/guidelines • government policy • professional codes of ethics and conduct • equity guidelines, organisational workplace diversity guidelines
<p>Unethical conduct may include</p>	<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

	<ul style="list-style-type: none"> • 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
<p>Ethical problems which may need to be referred rather than resolved at this level may include</p>	<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
<p>Referrals of ethical problems may be made to</p>	<ul style="list-style-type: none"> • line management • human resources • workplace relations officer • grievance officer • chief executive officer • public service commissioner • public sector standards body • organisational ethics committee • 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 PSPETH301B, 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 building and maintaining networks, delivering client services, using financial resources, procuring goods or services etc.

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

PSPETH301B – Uphold the values and principles of public service (Required unit)	Yes	Not Yet	Not able to comment
Applying ethical standards			
Dealing with ethical problems			

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

Referee (Third party) Comments:

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

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

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

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

PSPGOV301B – Work effectively in the organisation

Introduction

This is a required unit of competency in the PSP30504 Certificate III in Government (Security) – Personnel Security Stream and covers the requirements for working effectively in a public sector organisation with a focus on self-management. It includes evaluating and developing your own expertise, identifying career options, working within the organisational structure and culture, and managing your own work.

Being competent in this unit means being able to:

Evaluate and develop own expertise

This element requires:

- Self-assessment of **work-related competencies** is made by reflecting on own workplace experience and training, and from monitoring feedback on performance in the workplace
- Research is undertaken to identify possible careers and compare the requirements of these careers with current skill base and development opportunities available within the organisation and across the public sector
- Areas requiring competency development are **identified** by comparing current competencies with the competency requirements of current or anticipated duties
- Personal learning goals are set and progress towards them monitored
- Potential **competency recognition or development opportunities** are identified and accessed in accordance with organisational policy and procedures
- **Records** of competency development are maintained and work-related competencies and experience are conveyed to **relevant people** as required

Work within the organisational structure and context

This element requires:

- A comprehensive knowledge of the organisation's **structure and functioning** is developed and utilised in accordance with **legislation, policy and procedures**
- An understanding of the organisation's **context** is developed and **used**
- The work unit's **position** in the organisational structure is identified, its relationship with other organisational work units examined and any **protocols/difficulties/special requirements** determined
- The contribution of the work role and the work unit to the organisation's vision, goals and outcomes is identified and confirmed
- Work is undertaken in a manner that has regard for the workgroup position and the organisation's structure, functioning, culture and vision

Manage own work

This element requires:

- Individual work goals are identified, clarified and prioritised in accordance with the organisation's requirements
- **Risks** to the achievement of personal work outcomes are identified and managed in accordance with organisational risk management requirements
- Work strategies are selected with regard to applicable **work parameters**
- Progress with work is monitored relative to set goals, strategies and outcomes
- Work goals are achieved and work plans revised to attend to ongoing or new responsibilities

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>Work-related competencies may include</i></p>	<ul style="list-style-type: none"> • competencies as defined in the Public Sector Training Package • competencies as specified in other relevant Training Packages • enterprise competency standards • qualifications relevant to work responsibilities • essential knowledge and skills specified in position descriptions
<p><i>Competencies may be identified through</i></p>	<ul style="list-style-type: none"> • self-assessment/self-identification • colleagues • supervisors • workplace mentors • counsellors • educational programs • specialist services for specific individual needs, such as disability, Aboriginal, language, literacy, numeracy
<p><i>Competency recognition or development opportunities may include</i></p>	<ul style="list-style-type: none"> • recognition of prior learning/recognition of current competencies • formal campus-based training • workplace learning • workplace-based training • work experience • conference and seminar attendance • peer support • mentoring • coaching

	<ul style="list-style-type: none"> • acting positions • new positions
Records may include	<ul style="list-style-type: none"> • reports of achievement • curriculum vitae • training record books • job applications
Relevant people may include	<ul style="list-style-type: none"> • colleagues/team members • supervisors or managers • clients
Organisational structure and functioning may include	<ul style="list-style-type: none"> • organisational hierarchy • teaming • policies • products • services • clients/customers
Legislation, policy and procedures may include	<ul style="list-style-type: none"> • State/Territory and Commonwealth legislation and regulations such as: • public sector management acts • privacy legislation • equal employment opportunity, anti-discrimination and harassment legislation • occupational health and safety legislation. • ethics and accountability standards • public sector standards • organisational policy, procedures and protocols • international legislation/codes of behaviour
Organisational context may encompass	<ul style="list-style-type: none"> • goals • objectives • mission • values • ethos • politics • culture • social ethic
Using knowledge of organisational culture may include	<ul style="list-style-type: none"> • to determine the importance of work requirements • to adjust working style and outcomes • to support the organisation's values/ethos • to interpret directions in light of political reality
Position of the work unit may include	<ul style="list-style-type: none"> • position in a hierarchy • number of reporting levels • seniority of work unit head • branch of an agency/department • country branch • small/regional/remote branch
Protocols/difficulties/special requirements may include	<ul style="list-style-type: none"> • 'head office' syndrome that develops between remote branches and head office • time for decisions to be made (in hierarchy) • amount of autonomy of work unit • practicality of delegations • approval processes • role ambiguity between work units

<i>Risks may include</i>	<ul style="list-style-type: none"> • local level/self issues which can be controlled • time wasters • misuse of equipment • personal stress
<i>Work parameters may include</i>	<ul style="list-style-type: none"> • productivity • flexibility • quality • opportunities • risks • timeframes • organisational structure • constraints • contingencies • support or equipment needed

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 PSPGOV301B, candidates should provide evidence that confirms effective work performance in a range of (3 or more) contexts (or occasions, over time).

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

PSPGOV301B – Work effectively in the organisation (Required unit)	Yes	Not Yet	Not able to comment
Evaluating and develop own expertise			
Working within organisation structure and context			
Managing own work			

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:

PSPGOV302B – Contribute to workgroup activities

Introduction

This is a required unit of competency in the PSP30504 Certificate III in Government (Security) and covers contributing as a workgroup member and assisting with support, learning and development for others in achieving workgroup goals. It includes the establishing workgroup parameters, participating in the workgroup, assisting in learning and development and assisting workgroup members.

Establish workgroup parameters

This element requires:

- Roles, responsibilities and professional working relationships in the **workgroup** are identified and clarified as necessary
- Individual differences within the workgroup are identified and valued
- Emotional triggers for self and others are identified and clarified to assist in the **management of emotional responses** to work issues
- The varying cultural expressions of **emotion** are identified and utilised to respond to emotional cues within a diverse workgroup

Participate in the workgroup

This element requires:

- Workgroup tasks are *negotiated* in accordance with individual strengths, personal preferences or development needs
- Cooperation is demonstrated with others in the workgroup
- Knowledge is shared with the group in accordance with **legislation, policy and procedures**, in order to complete tasks
- Communication language/style is selected and used to take account of the task requirements and diversity of workgroup members
- Constructive contributions are made to workgroup goals
- Conflict/problems are addressed and resolved through discussion in the workgroup or referred in accordance with organisational policy and procedures

Assist workgroup members

This element requires:

- Support is provided to workgroup members to achieve goals
- Assistance is provided on routine tasks as required
- Professional working relationships are maintained with colleagues
- Assistance with on-the-job **learning and development** is provided as required

Range statement

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

<i>Workgroup may include</i>	<ul style="list-style-type: none"> • formal and informal work units • directed or self-directed teams
<i>Management of emotions may be</i>	<ul style="list-style-type: none"> • emotional intelligence, widely recognised as the ability of an individual to monitor their own and others' emotions in a social or work environment, to discriminate among the emotions and to use the information to guide their thinking and actions • characterised by: <ul style="list-style-type: none"> • self-awareness (personal) • self-management (personal) • social awareness (social) • relationship management (social)
<i>Emotions may include</i>	<ul style="list-style-type: none"> • anger and anxiety • apathy • apprehension • caring • confidence • depression • elation • enthusiasm • excitement • fear • happiness • inadequacy • joy • nervousness • over-confidence • pride • stress • under-confidence • unhappiness
<i>Negotiation may include</i>	<ul style="list-style-type: none"> • effective listening • questioning • verbal and non-verbal communication • culturally appropriate strategies • constructive feedback • issues identification • exploring options • identifying areas of agreement • recording agreements

<p>Legislation, policy and procedures may include</p>	<ul style="list-style-type: none"> • State/Territory and Commonwealth legislation and regulations such as: • public sector management acts • privacy legislation • equal employment opportunity, anti-discrimination and harassment legislation • equity and diversity • racial tolerance • occupational health and safety legislation. • ethics and accountability standards • public sector standards • organisational policy, procedures and practices • organisational and public sector protocols • international legislation/codes of behaviour
<p>Communication techniques may include</p>	<ul style="list-style-type: none"> • active listening • using open and/or closed questions • speaking clearly and concisely • varying language and tone of voice to suit the audience and purpose • giving clients full attention • maintaining eye-contact when culturally appropriate (for face-to-face interactions) • using non-verbal communication (for face-to-face interactions) such as: • body language • personal presentation • using clear, legible writing • handling sensitive and confidential issues
<p>Learning and development opportunities may include</p>	<ul style="list-style-type: none"> • formal internal and external courses • on-the-job learning • work experiences and assignments • placement at level and higher duties • self-paced multimedia learning • assisted formal study • conference and seminar attendance • induction and orientation

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 PSPGOV302B, candidates should provide evidence that confirms contribution to workgroup activities in a range of (3 or more) contexts (or occasions, over time).

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

PSPGOV302B – Contribute to workgroup activities (Required unit)	Yes	Not Yet	Not able to comment
Establishing workgroup parameters			
Participating in the workgroup			
Assisting workgroup members			

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:

PSPGOV308B – Work effectively with diversity

Introduction

This is a required unit of competency in the PSP30504 Certificate III in Government (Security) – Personnel Security Stream. This unit covers the competency for individuals without supervisory responsibilities to work effectively with diversity. It includes recognising and valuing individual differences and working effectively with diverse clients and colleagues.

Being competent in this unit means being able to:

Recognise and value individual differences

This element requires:

- Workgroup ***diversity*** is explored to identify attributes that may be of benefit to the organisation and its client base
- ***Colleagues*** are assisted to acknowledge and use their diverse attributes to contribute to workgroup processes, outcomes and delivery of services to diverse clients
- Own work practices are used to acknowledge and reflect the diversity of self and colleagues for the benefit of workplace activities, stakeholder relationships and outcomes
- Client diversity is identified and responded to in accordance with ***legislation, policy and guidelines***

Work effectively with diverse clients and colleagues

This element requires:

- A range of communication styles is developed and used to respect and reflect the diversity of the workplace and client groups
- Compliance with the requirements of public sector legislation, policies and guidelines relating to workplace diversity is demonstrated through personal conduct in the workplace
- Feedback from clients and the workgroup is sought and utilised to continuously improve personal effectiveness in working with diversity

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>Diversity may include</i>	<ul style="list-style-type: none">• age• cultural background• disability• educational level• ethnicity• expertise
-------------------------------------	--

	<ul style="list-style-type: none"> • family responsibilities • gender • interests • interpersonal approach • language • learning styles • life experience • marital status • not fitting the dominant paradigm of the organisation • personality • physical capability • political orientation • race • religious belief • sexual orientation • socio-economic background • thinking styles • work experience • working styles
Colleagues may include	<ul style="list-style-type: none"> • peers • trainees • work experience personnel • supervisors and senior management • internal stakeholders • external stakeholders/clients/customers
Legislation, policy and guidelines may include	<ul style="list-style-type: none"> • Commonwealth legislation addressing diversity issues, for example: <ul style="list-style-type: none"> • Racial Discrimination Act 1975 • Sex Discrimination Act 1984 • Disability Discrimination Act 1992 • Workplace Relations Act 1996 • Privacy Act 1988 • Human Rights and Equal Opportunity Commission Act 1984. • State/Territory legislation addressing diversity issues, such as Victoria's Racial and Religious Tolerance Act • public service/public sector management acts • workplace diversity guidelines • 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

	<ul style="list-style-type: none">• community guidelines, policy and practices (such as those within Aboriginal and Torres Strait Islander communities)
--	---

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 PSPGOV308B, candidates should provide evidence that confirms working effectively with diversity in a range of (3 or more) contexts (or occasions, over time) in contexts such as participating in a workgroup or delivering client services.

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

PSPGOV308B – Work effectively with diversity (Required unit)	Yes	Not Yet	Not able to comment
Recognising and value individual differences			
Working effectively with diverse clients and colleagues			

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:

PSPGOV312A – Use workplace communications strategies

Introduction

This is a required unit of competency in the PSP30504 Certificate III in Government (Security) – Personnel Security Stream and covers the use of workplace communication strategies for interacting with internal and external clients. It includes responding to enquiries, receiving and giving directions, participating in meetings and making presentations in the workgroup.

Being competent in this unit means being able to:

Respond to enquiries

This element requires:

- Responses are provided to **enquiries** from staff, the public and **other clients** in a timely manner or the matter is referred in accordance with organisational procedures
- **Active listening** techniques are utilised
- Respect for the individual is maintained and **specific needs** are identified and addressed in accordance with organisational policy and procedures
- Conflict or difficult situations are resolved in a confidential manner in accordance with standard procedures or are referred to others in accordance with organisational policy and procedures
- Communication is undertaken within the mandate of public sector **legislation, the organisational code of conduct and ethics standards**

Receive and give directions

This element requires:

- Policy to be implemented is interpreted under direction to identify and plan for change in work practices
- Oral directions are received, clarified and assessed to ensure they are ethical, lawful and reasonable
- Directions are acted on promptly in accordance with organisational policy and procedures or refused in accordance with public sector standards and ethics guidelines
- Directions are relayed in a clear and concise manner appropriate to the receiver
- Understanding of the directions by the receiver is questioned and confirmed
- Feedback on directions and outcomes is provided in accordance with organisational requirements

Participate in meetings

This element requires:

- Meeting agenda is confirmed and followed
- Input is focused on the objectives of the meeting and the agenda item at hand
- Input is provided fully but succinctly and in accordance with meeting protocol

- Other attendees are encouraged to participate in a manner suited to their experience and individual needs
- Meeting participants are treated with respect and **trust-building behaviours** are used to enhance relationships and meeting outcomes

Make presentations within the workgroup

This element requires:

- Job-related **presentations** are prepared and made within the workgroup
- Presentations are logically structured to contain relevant, accurate and complete information/content
- Presentations are structured and delivered to suit the intended audience
- **Feedback** is obtained from the audience and used to improve 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.

<i>Enquiries may be</i>	<ul style="list-style-type: none"> • face-to-face • by telephone • via technology and other media, such as computers, email, short message service (SMS), facsimile, pagers • long or complex enquiries from internal or external clients • at organisational rather than workgroup level
<i>Other clients may be</i>	<ul style="list-style-type: none"> • other agencies • unions • professional bodies • special interest groups • Minister's office • interstate or international clients • general public
<i>Active listening may include</i>	<ul style="list-style-type: none"> • listening for central ideas • considering how information applies to the situation/person • identifying/eliminating emotional triggers or psychological deaf spots • using techniques for staying in touch with what the speaker is saying, as thought speed outstrips speed of speech • paraphrasing • summarising • using silence to elicit additional information • using and recognising body language
<i>Specific needs may relate</i>	<ul style="list-style-type: none"> • age

<p>to</p>	<ul style="list-style-type: none"> • cultural background • disability • educational level • emotional state • ethnicity • expertise • family responsibilities • gender • interests • interpersonal approach • language • life experience • marital status • personality • physical ability • political orientation • religious belief • sexual orientation • socio-economic background • thinking/learning styles • work experience • working styles
<p><i>Legislation, code of conduct and ethics standards may include</i></p>	<ul style="list-style-type: none"> • Commonwealth and State/Territory legislation, standards and guidelines especially relating to equal employment opportunity, diversity, anti-discrimination • government policy • public sector code of ethics • national standards • the organisation's policies and practices • organisational code of conduct • international legislation/codes of behaviour

<p><i>Trust-building behaviours may include</i></p>	<ul style="list-style-type: none"> • listening • sharing • helping • encouraging • speaking frankly and directly • respecting opinions • being consistent • cooperating • acting as equals • being confident, self-assured • accentuating the positive • acting calmly under stress • acting spontaneously and authentically • being empathetic • providing fair and accurate feedback • being physically or psychologically close • freeing and allowing • being caring/friendly • accepting and tolerating most behaviours • transparent, open, above board • open to new ideas and information • verbal and non-verbal congruency • resolving conflict and interpersonal problems • empowering and building up others • treating others as individuals • (Gordon F Shea, 1999, Making the most of being mentored)
<p><i>Presentations may be</i></p>	<ul style="list-style-type: none"> • oral • formal/informal • to a small/larger group depending on the size of the workgroup • supported by graphs, charts, tables or other information • supported by electronic slideshow/presentation
<p><i>Feedback may include</i></p>	<ul style="list-style-type: none"> • informal feedback during the presentation • informal feedback after the presentation • feedback from supervisor, as part of performance management

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 PSPGOV312A, candidates should provide evidence that confirms workplace 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:

PSPGOV312A – Use workplace communication strategies (Required unit)	Yes	Not Yet	Not able to comment
Responding to enquiries			
Receiving and giving directions			
Participating in meetings			
Making presentations within the workgroup			

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 required unit of competency in the PSP30504 Certificate III in Government (Security) – Personnel Security Stream 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.

<i>Occupational health and safety issues may include</i>	<ul style="list-style-type: none">• hazards relating to the physical environment• workplace stress• conflict• bullying• harassment
<i>Designated personnel may include</i>	<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
<i>Occupational health and safety legislation may include</i>	<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
<i>Contributions may include</i>	<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
<i>Participative workplace safety arrangements may include</i>	<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
<i>Hazard identification may include</i>	<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
<i>Workplace procedures may include</i>	<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

	<ul style="list-style-type: none"> allocation of responsibilities • emergency procedures • 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
<i>Controlling risks may include actions such as</i>	<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
<i>Other hazardous events may include</i>	<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 workplace safety procedures followed 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 (Required unit)	Yes	Not Yet	Not able to comment
Contributing to participative workplace safety arrangements			
Identifying hazards and controlling risks			

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

Referee Comments:

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

Signature of Referee:

Date:

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

Signature of Candidate:

Date:

PSPLEGN301B – Comply with legislation in the public sector

Introduction

This is a required unit of competency in the PSP30504 Certificate III in Government (Security) – Personnel Security Stream and covers compliance with legislation and related public sector policy guidelines and procedures. It includes identifying and complying with legislative requirements and reporting incidents of non-compliance.

Being competent in this unit means being able to:

Identify legislative requirements

This element requires:

- Information is accessed that covers the range of **legislation and guidelines** relating to the workplace and is current and comprehensive
- Key requirements of relevant pieces of legislation are identified and confirmed with senior staff
- Requirements of legislation are clarified to confirm understanding and ensure consistency of interpretation and application
- Clarification is obtained of the way various pieces of legislation are integrated to provide a legislative framework for public sector work
- Advice is obtained when apparently **conflicting legislative directives** are found

Comply with legislative requirements

This element requires:

- Work practices are carried out in accordance with the requirements of legislation relating to the work environment
- Own conduct is reviewed and feedback from others is used to confirm continuing compliance with legislative requirements

Report incidents of non-compliance

This element requires:

- Possible breaches of legislation are raised promptly with an authorised person/body in accordance with organisational procedures
- **Inadequacies in workplace procedures** which may contribute to non-compliance are raised 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: • 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: • employee relations • chief executive officer's instructions • Commissioner's instructions • public sector notices. • workplace environment: • 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: • Treasurer's instructions • contractual obligations. • transparency: • freedom of information • professional reporting • accountability • fair trading. • business and community: • 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>Conflicting legislative directives may include</p>	<ul style="list-style-type: none"> • apparent contradiction between statutes • apparent conflict between statutes and policy requirements

<i>Inadequacies in workplace procedures may include</i>	<ul style="list-style-type: none">• insufficient financial/other controls• insecure Internet/fax access• non-auditable 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 PSPLEGN301B, 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:

PSPLEGN301B – Comply with legislation in the public sector (Required unit)	Yes	Not Yet	Not able to comment
Identifying legislative requirements			
Complying with legislative requirements			
Reporting incidents of 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:

PSPSEC301A – Secure government assets

Introduction

This is a chosen required elective unit of competency in the PSP30504 Certificate III in Government (Security) – Personnel Security Stream and covers covers implementation of security requirements for the organisation's assets. It includes protecting assets from security threats, implementing access restrictions, advising third parties of security requirements and minimising security risk.

Being competent in this unit means being able to:

Protect assets from security threats

This element requires:

- **Assets** are stored and accessed in accordance with organisational policies, procedures and guidelines
- Assets are regularly checked to ensure security
- Suspicious activity is investigated and dealt with in accordance with organisational policy and procedures
- **Expert advice** is obtained as required in accordance with organisational policy and procedures

Implement access restrictions

This element requires:

- Access is **restricted** to authorised personnel
- Potential threats are identified
- Breaches are identified and reported to appropriate personnel in accordance with organisational policy and procedures
- Action is taken to deal with a breach in accordance with legislation, policy and guidelines

Advise third parties of security requirements

This element requires:

- The needs, expectations, attitudes, and current level of knowledge of **third parties** are confirmed
- Risks related to possible confrontations are identified and managed in accordance with organisational risk management and procedures
- Third parties are advised of the organisation's security requirements
- Advice is provided that is current, timely and meets the specific needs of the parties in its range, depth and form of presentation
- Feedback is obtained on the party's level of understanding, and additional information or explanation is used to clarify requirements if needed

Minimise security risk

This element requires:

- Changes in circumstance are identified and reported to appropriate personnel in accordance with organisational policy and procedures
- Documentation is completed in accordance with organisational policies, procedures and guidelines
- **Actions** are taken to reduce the likelihood of breaches reoccurring in accordance with the organisation's security plan

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>Assets may include</i>	<ul style="list-style-type: none"> • information • documents • people • property • networks • systems • intellectual property • in Australia • overseas
<i>Assets may be</i>	<ul style="list-style-type: none"> • owned • on lease • hired • owned by others
<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
<i>Access may be restricted to information that is</i>	<ul style="list-style-type: none"> • national security classified • non-national security classified • classified by third parties
<i>Third parties may include</i>	<ul style="list-style-type: none"> • other staff • contractors • members of the public • visitors to the organisation

Actions may include	<ul style="list-style-type: none">• advice to responsible officers• disciplinary• formal counselling• prosecution• referral to third parties• strengthening of security• training
----------------------------	---

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 PSPSEC301A, candidates should provide evidence that confirms securing government assets in a range of (3 or more) contexts (or occasions, over time).

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

PSPSEC301A – Secure government assets (Chosen required elective)	Yes	Not Yet	Not able to comment
Protecting assets from security threats			
Implementing access restrictions			
Advising third parties of security requirements			
Minimising security risk			

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 chosen required elective unit of competency in the PSP30504 Certificate III in Government (Security) – Personnel Security Stream 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

	<ul style="list-style-type: none"> • Security Guidelines for Australian Government IT Systems (ACSI 33) • Commonwealth Protective Security Manual
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 			
<p>Candidate's Comments and Attachment/s number as included in Portfolio of Evidence:</p>			

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 PSP30504 Certificate III in Government (Security) – Personnel Security Stream 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
<i>Securing practices may include</i>	<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

	<ul style="list-style-type: none"> • doors • safe carriage of keys
<i>Accounting for security classified information may include</i>	<ul style="list-style-type: none"> • audit • spot checks • correct notation or markings • file records • transmission records • receipts
<i>Methods of disposal may include</i>	<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 unit)	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:

PSPREG415A – Receive and validate data

Introduction

This is a required unit of competency in the PSP30504 Certificate III in Government (Security) – Personnel Security Stream 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.

<i>Information may be</i>	<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
<i>Data sources may include</i>	<ul style="list-style-type: none"> • applications • correspondence • declarations • diary entries • electronic records • email • fax records • files • graphics

	<ul style="list-style-type: none"> • incident reports • 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 (Required unit)	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:

PSPSEC401A – Undertake government security risk analysis

Introduction

This is a required unit of competency in the PSP30504 Certificate III in Government (Security) – Personnel Security Stream and covers work at an operational level, to analyse risk against the organisation's security plan. It includes establishing the security risk context; identifying, analysing and evaluating risk against the organisation's security plan; and compiling of a security risk register.

Being competent in this unit means being able to:

Establish security risk context

This element requires:

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

Identify security risk

This element requires:

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

Analyse security risk

This element requires:

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

Evaluate security risk

This element requires:

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

Compile security risk register

This element requires:

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

Range statement

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

<p>Strategic context may include</p>	<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
<p>Organisational context may include</p>	<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,

	<p>products and services such as:</p> <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
Legislation, policy and procedures may include	<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 and 2004
Security risk criteria may concern	<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
Risk may be to	<ul style="list-style-type: none"> ● personnel ● information ● property ● reputation
Sources of security risk may include	<ul style="list-style-type: none"> ● technical ● actual events ● political circumstances ● human behaviour ● environmental ● conflict ● terrorism ● internal ● external ● local ● national and 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

	<ul style="list-style-type: none"> • 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
Risk ratings may include	<ul style="list-style-type: none"> • severe • high • major • significant • moderate • low • trivial
Security risk register may include	<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 chosen elective unit of competency in the PSP30504 Certificate III in Government (Security) – Personnel Security Stream 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 and training • personnel-oriented • information-oriented • property-oriented • reputation-oriented
Legal requirements, government and organisational policy may include	<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

	<ul style="list-style-type: none"> • 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 and 2004
Strategies may include	<ul style="list-style-type: none"> • audits • incident reporting mechanisms • technical controls • systems • rosters • access controls • training
Monitoring may include	<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: • notification of major changes to business or corporate goals or plans • notification of key projects
Stakeholders may include	<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 (Chosen required elective)	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:

