



Australian Government

Department of Education, Employment and Workplace Relations

PSPSEC601A Define information systems framework

Revision Number: 3

PSPSEC601A Define information systems framework

Modification History

Release	TP Version	Comments
3	PSP12V1	Unit descriptor edited.
2	PSP04V4.2.	Layout adjusted. No changes to content.
1	PSP04V4.1	Primary release.

Unit Descriptor

This unit covers the process of identifying and establishing the information system security framework for an organisation or a business unit at functional level.

It includes establishing the organisational context, determining principal areas of risk, determining information system requirements, establishing and obtaining approval for the framework.

In practice, defining an information systems framework may overlap with other generalist or specialist public sector work activities such as managing compliance with legislation and ethics requirements, managing risk, networking, implementing policy, managing change. No licensing, legislative, regulatory or certification requirements apply to this unit at the time of endorsement.

Application of the Unit

Not applicable.

Licensing/Regulatory Information

Not applicable.

Pre-Requisites

Not applicable.

Employability Skills Information

This unit contains employability skills.

Elements and Performance Criteria Pre-Content

Elements are the essential outcomes of the unit of competency. Together, performance criteria specify the requirements for competent performance. Text in ***bold italics*** is explained in the Range Statement following.

Elements and Performance Criteria

ELEMENT

PERFORMANCE CRITERIA

- | | |
|--|--|
| 1. Establish the organisational context | <ul style="list-style-type: none">1.1 Legislative and regulatory requirements for the organisation are identified and documented in accordance with organisational policy and procedures.1.2 Legislation is analysed for any security implications for information management, and the outcomes are documented.1.3 The organisation's purpose and function are reviewed for compliance requirements.1.4 The broad social context in which the organisation operates is analysed to determine community expectations. |
| 2. Determine the principal areas of risk requiring information strategy | <ul style="list-style-type: none">2.1 Existing risk analyses for organisation's functions are reviewed and updated.2.2 Regulatory requirements and legal liabilities are reviewed and documented for their impact on the information systems framework.2.3 Risks and liabilities to be managed by information systems are determined and documented informing the development of the framework. |
| 3. Determine the information system requirements for each business function | <ul style="list-style-type: none">3.1 Risks, liabilities and regulatory requirements are determined and analysed against each business function.3.2 The determined requirements for each business function are documented and communicated as evidence to be captured as records.3.3 Information system specifications are formulated from the evidence requirements in accordance with the organisation's technologies, standards and protocols.3.4 Information security requirements are determined for each business function.3.5 Specifications for information systems security measures are determined consistent with government guidelines and standards. |
| 4. Establish information systems framework for organisation | <ul style="list-style-type: none">4.1 Overview of responsibilities for information management within the organisation is developed and communicated.4.2 Responsibilities and authorities in relation to regulatory requirements are defined in accordance with jurisdictional and organisational standards.4.3 Information management responsibilities and rights for each business function are defined.4.4 Identified risks and liabilities managed by information systems are integrated with the definition of responsibilities for each function.4.5 Levels of accountability and responsibility within the framework are defined, assigned and documented for each function. |

ELEMENT**PERFORMANCE CRITERIA**

- 4.6 Security procedures for information systems are formulated and documented.
5. **Obtain approval for framework**
- 5.1 The completed and documented framework of areas of risk, regulatory requirements, records specifications, security requirements and information management responsibilities are communicated to the ***appropriate person(s)*** for review and endorsement.
- 5.2 A review process is established and appropriate persons are charged with ***maintaining*** the currency of the organisation's information systems framework.

Required Skills and Knowledge

This section describes the essential skills and knowledge and their level, required for this unit.

Skill requirements

Look for evidence that confirms skills in:

- applying legislation, regulations and policies relating to government information systems security
- analysing process functions and problems
- preparing, compiling and writing complex documents and reports
- communicating complex relationships and processes effectively to users and management
- documenting complex relationships and processes
- identifying and viewing component parts as integral elements of the whole system
- using tools and techniques to solve problems
- analysing and interpreting legal, regulatory and security requirements and organisation policies and procedures
- analysing and synthesizing documentation, verbally delivered information, and observed behaviours
- consulting with stakeholders to elicit relevant information for analysis
- responding to diversity, including gender and disability
- applying procedures relating to occupational health and safety and environment in the context of government information systems security

Knowledge requirements

Look for evidence that confirms knowledge and understanding of:

- legislation, regulations, policies, procedures and guidelines relating to government information system security
- sources of information about jurisdictional requirements for information systems
- functions and structures in the organisation
- policies and strategies that apply across the jurisdiction
- information management principles and processes
- information security requirements
- equal employment opportunity, equity and diversity principles
- public sector legislation such as occupational health and safety and environment in the context of government information systems security

Evidence Guide

The Evidence Guide specifies the evidence required to demonstrate achievement in the unit of competency as a whole. It must be read in conjunction with the Unit descriptor, Performance Criteria, the Range Statement and the Assessment Guidelines for the Public Sector Training Package.

Units to be assessed together

- *Pre-requisite* units that must be achieved prior to this unit: *Nil*
- *Co-requisite* units that must be assessed with this unit: *Nil*
- *Co-assessed units* that may be assessed with this unit to increase the efficiency and realism of the assessment process include, but are not limited to:
 - PSPETHC601B Maintain and enhance confidence in public service
 - PSPGOV601B Apply government systems
 - PSPGOV602B Establish and maintain strategic networks
 - PSPLEGN601B Manage compliance with legislation in the public sector
 - PSPMNGT604B Manage change
 - PSPMNGT608B Manage risk
 - PSPPOL603A Manage policy implementation
 - PSPSEC602A Manage security awareness

Overview of evidence requirements

In addition to integrated demonstration of the elements and their related performance criteria, look for evidence that confirms:

- the knowledge requirements of this unit
- the skill requirements of this unit
- application of the Employability Skills as they relate to this unit (see Employability Summaries in Qualifications Framework)
- information systems frameworks defined (or re-defined) in a range of (3 or more) contexts (or occasions, over time)

Resources required to carry out assessment

These resources include:

- legislation, policy, procedures and protocols relating to information systems frameworks
- case studies and workplace scenarios to capture the range of situations likely to be encountered when defining information systems frameworks

Where and how to assess evidence

Valid assessment of this unit requires:

- a workplace environment or one that closely resembles normal work practice and replicates the range of conditions likely to be encountered when defining information systems

frameworks, including coping with difficulties, irregularities and breakdowns in routine

- information systems frameworks defined (or re-defined) in a range of (3 or more) contexts (or occasions, over time)

Assessment methods should reflect workplace demands, such as literacy, and the needs of particular groups, such as:

- people with disabilities
- people from culturally and linguistically diverse backgrounds
- Aboriginal and Torres Strait Islander people
- women
- young people
- older people
- people in rural and remote locations

Assessment methods suitable for valid and reliable assessment of this competency may include, but are not limited to, a combination of 2 or more of:

- portfolios
- questioning
- scenarios
- authenticated evidence from the workplace and/or training courses, such as risk management plan, organisational flowchart

For consistency of assessment

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

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 ***bold italics*** in the Performance Criteria is explained here.

Legislative and regulatory requirements may include:

- income tax
- superannuation
- goods and services tax
- occupational health and safety
- industrial relations
- freedom of information
- privacy
- statutory access

Analysis of the broad legal and social context of an organisation may identify:

- the legal framework which regulates an organisation's operations
- the internal and external stakeholders whose interests must be taken into account
- the social and ethical standards the community expects it should meet
- codes of ethics, codes of professional conduct

Regulatory requirements may be documented in:

- codes of practice
- regulations or rules
- technical standards
- international or national standards

Specifications for information systems security may include:

- standard level of protection
- enhanced level of protection
- certification and accreditation of information technology and telecommunications systems
- information technology audit trails
- logical access controls

Responsibilities may be assigned to:

- business unit managers or organisational groupings responsible for discrete functions, processes or projects which generate information
- individual employees who carry out the business activities which create information
- managers who may be responsible for establishing overall policy and procedures based on organisational requirements, standards and compliances

- Standards** that apply may include:
- system administrators who may be responsible for the reliability and continuing operation of systems which generate records
 - Protective Security Policy Framework
 - fraud control standards
 - Australian Government Information Security Manual (ISM)
 - AS/NZS 4390.2 Australian Standard in Records Management Part 2, Clause 5
 - ISO DIS 15489 - Draft International Standard on Records Management
 - AS 3674 - Storage of Microfilm (of all types for various purposes)
 - AS 1203 Microfilming of Engineering Documents
 - AS 2840 Microfilming Newspapers for Archival Purposes
 - AS 4003 Permanent Paper
- Appropriate person for approvals** may be:
- senior manager for each business function
 - agency security adviser
 - management team
 - reference body appointed by management
- Maintenance of the framework** includes:
- responsibility for ensuring the maintenance of adequate security measures for information systems and their data

Unit Sector(s)

Not applicable.

Competency field

Government Security Management.