Australian Government

BSBDIG307X Develop Intermediate Digital Cyber Security Skills

DRAFT

Release: 1

BSBDIG307X Develop Intermediate Digital Cyber Security Skills

Modification History

Release	Comments
1	This unit of competency was first released in BSB Business Services Training Package Release 9.0.

Unit outcomes

This unit describes the skills and knowledge required to apply workplace cyber security procedures in workplace contexts. It applies to learners across all industries, who recognise threats, protect sensitive information, and support workplace security culture as part of their day-to-day work.

The primary purpose of this unit is to develop intermediate and employability digital capabilities that support participation in the digital workplace and underpin further vocational training. It is delivered with limited supervision, using varied workplace tasks of moderate complexity, at an intermediate level.

Learners develop capability across five competence areas:

- Cyber security threat awareness
- Workplace security protocols
- Data protection
- Incident response participation
- Security culture contribution.

Licensing/Regulatory Information

No licensing, legislative or certification requirements apply to this unit at the time of publication.

Knowledge

On successful completion of this unit, learners will have intermediate knowledge of:

- Common workplace cyber security threats (including but not limited to AI-enhanced threats, phishing and social engineering) and their potential impact on organisational operations
- Workplace security procedures and protocols used to protect digital systems, devices, and information in routine workplace contexts
- Workplace requirements for protecting sensitive information including but not limited to access controls, secure storage methods, and appropriate data handling procedures
- Workplace procedures for reporting security concerns, escalating incidents and participating in incident response activities

© Commonwealth of Australia, 2026 Future Skills Organisation

- Approaches for supporting workplace cyber security awareness and promoting secure workplace practices.

Skills

On successful completion of this unit, learners will have skills to:

- Recognise common workplace cyber security threats and suspicious activities
- Apply workplace security procedures and protocols to protect digital systems, devices, and information
- Protect sensitive workplace information by applying access controls, appropriate data handling procedures and using secure storage methods
- Report security concerns and incidents through appropriate workplace channels
- Support workplace security awareness by sharing security knowledge with colleagues.

Application of Knowledge & Skills

Learners apply their knowledge and skills with limited supervision, following established workplace frameworks and procedures.

This applies to varied workplace cyber security tasks of moderate complexity, adapting approaches to different contexts while working within organisational guidelines.

Learners will follow:

- Established workplace frameworks and procedures for cyber security
- Escalation processes when encountering unfamiliar situations, ethical considerations, or requirements beyond established procedures.

Learners are responsible for:

- Making informed decisions about threat identification, security procedures and incident reporting within defined parameters.

Learners are accountable for:

- The quality and effectiveness of their own cyber security practices, including selecting appropriate security procedures and protocols to achieve workplace outcomes within defined parameters, and supporting others with routine security tasks.

Pre-requisite unit(s)

No pre-requisite units

Competency field(s)

Digital Competence

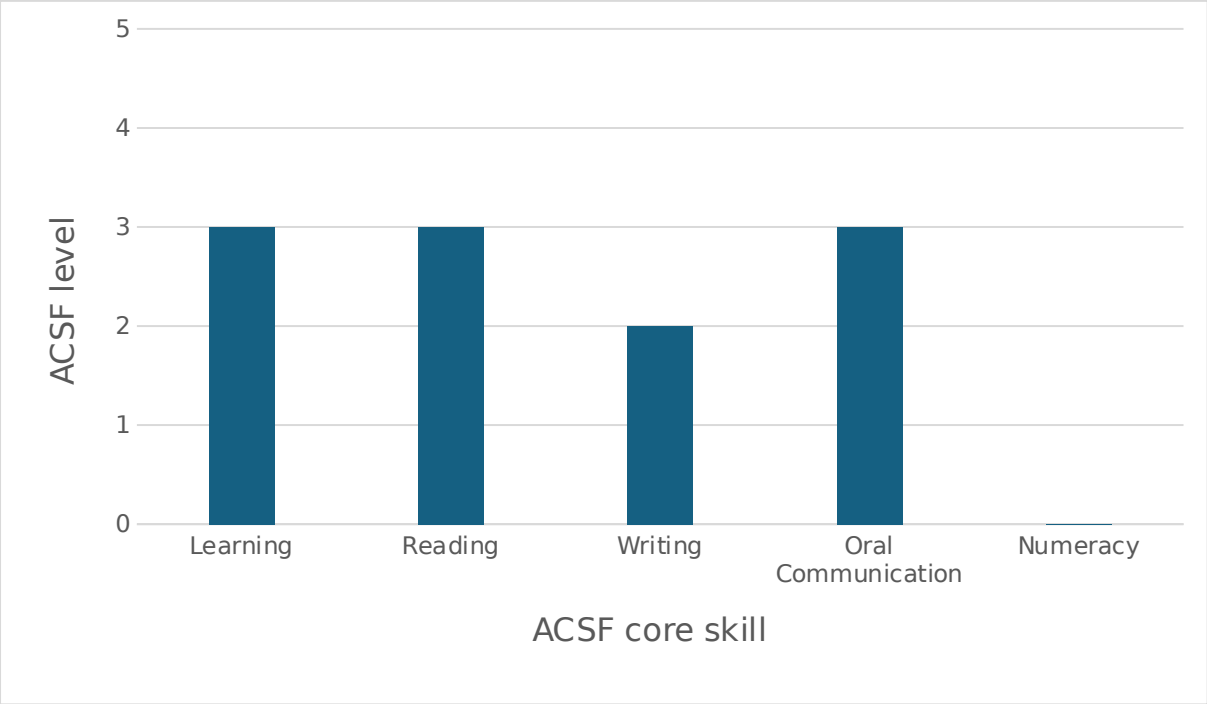
Unit sector(s)

Digital Capability

© Commonwealth of Australia, 2026 Future Skills Organisation

Foundation skills

The foundation skills in this unit are outlined below



Core Skills	ACSF Indicators and Performance Features
Learning	Plans, implements and adjusts processes and applies strategies in less familiar contexts. Taking responsibility for routine learning, reflecting on actions and outcomes, and beginning to transfer principles to new situations.
Reading	Evaluates and integrates information across familiar and some unfamiliar texts. Understanding texts that require integrating a number of ideas, with some inference, and beginning to consider the validity of a source.
Writing	Conveys meaning on familiar topics using familiar text types. At least two familiar text types, such as an email message, and factual information in notes or lists.
Oral Communication	Establishes and maintains spoken communication in familiar and some unfamiliar contexts. Using structure and register for a range of purposes, including explaining, instructing and problem solving in everyday situations.
Numeracy	No ACSF level assigned.

© Commonwealth of Australia, 2026 Future Skills Organisation

Range of conditions

N/A

DRAFT

© Commonwealth of Australia, 2026 Future Skills Organisation

Assessment Requirements for BSBDIG307X Develop Intermediate Digital Cyber Security Skills

Performance Evidence

Learners must demonstrate ability to:

- Recognise and respond to at least two different common workplace cyber security threats using established procedures
- Apply workplace security procedures to protect digital systems, devices and information for a workplace task
- Apply appropriate access controls, secure storage methods and data handling procedures to protect sensitive workplace information for a workplace task
- Report at least one security concern and incident through appropriate workplace channels and participate in response activities
- Contribute to a workplace security awareness activity or share security knowledge with at least one colleague to support a positive workplace security culture.

Knowledge Evidence

Learners must demonstrate intermediate knowledge of:

- The nature of common workplace cyber security threats, including AI-enhanced threats, and their potential impact on organisational operations
- The role of workplace security procedures and protocols in protecting digital systems, devices and information
- The requirements for protecting sensitive workplace information, including access controls, secure storage and data handling procedures
- The steps and decision points involved in reporting, escalating and participating in workplace incident response
- The contribution of individual security awareness practices to a positive workplace cyber security culture.

Assessment Conditions

N/A

Mandatory Workplace Requirements

Assessment of performance evidence may be in a workplace setting or an environment that accurately represents a real workplace.

Unit Mapping Information

Previous Code and Title	Equivalence	Comments
	Newly created	This unit has been created to

© Commonwealth of Australia, 2026 Future Skills Organisation

		address a skill or task required by industry that is not covered by an existing unit of competency

Links

Companion volumes, including implementation guides, are found on the national training register - https://training.gov.au/training/details/BSB.

DRAFT

© Commonwealth of Australia, 2026 Future Skills Organisation