Australian Government

# BSBDIG407X Develop Advanced Digital Cyber Security Skills

DRAFT

**Release: 1**

# BSBDIG407X Develop Advanced 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 cyber security practices and security initiatives across diverse workplace contexts.

The primary purpose of this unit is to develop advanced digital capabilities that support specialised application across diverse workplace contexts and underpin further vocational training. Learners apply these capabilities across all industries in complex, non-routine workplace tasks at an advanced level.

Learners develop advanced capability across five competence areas:

- Cyber security threat assessment
- Security implementation
- Data protection and privacy
- Incident response coordination
- Security culture development.

## 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 advanced knowledge of:

- The use of emerging technologies used in cyber attacks and cyber security
- Approaches for identifying, analysing and evaluating cyber security threats and vulnerabilities in workplace contexts
- Methods for implementing security measures and maintaining secure systems
- Data protection and privacy requirements (including security controls, access management and compliance considerations)
- Incident response procedures, recovery processes and stakeholder communication approaches
- Strategies for promoting security awareness and building organisational security culture.

DRAFT


© Commonwealth of Australia, 2026 Future Skills Organisation

## Skills

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

- Identify and analyse cyber security threats and vulnerabilities in workplace contexts, evaluating risk levels using appropriate methods
- Determine and implement protective practices to maintain secure environments, monitoring their effectiveness through systematic checking
- Coordinate data protection initiatives using appropriate security controls, maintaining privacy standards across systems and processes
- Manage access controls and compliance requirements
- Implement and coordinate incident response and recovery activities during security events
- Coach a colleague to strengthen incident management capability
- Promote security awareness and mitigation strategies in workplace contexts
- Contribute to initiatives that build organisational security culture.

## Application of Knowledge & Skills

Learners work independently within established workplace frameworks and procedures, applying judgement to identify, assess and respond to cyber security threats, implement and monitor security measures, manage incident response activities, and promote security awareness and organisational security culture across varied workplace contexts.

This applies to non-routine workplace cyber security tasks requiring analysis and evaluation across diverse organisational contexts, including situations with multiple variables and stakeholder considerations.

Learners will follow:

- Established workplace frameworks and procedures for cyber security threat identification, response and awareness promotion
- Escalation to specialist security expertise or organisational policy guidance when matters fall outside established frameworks, including emerging threats, AI-enabled cyber risks and stakeholder communication during security events

Learners are responsible for:

- Making informed decisions about threat identification, security measure implementation, data protection requirements, incident response approaches and security culture initiatives across varied contexts, and exercising judgement on emerging threats, AI-enabled cyber risks and stakeholder communication during security events

Learners are accountable for:

- The selection and application of cyber security measures and protective practices, and the verification of outputs from AI-supported security activities


© Commonwealth of Australia, 2026 Future Skills Organisation

- The quality of cyber security outputs in their own work and in supporting and guiding the work of others.

## Pre-requisite unit(s)

No pre-requisite units

## Competency field(s)

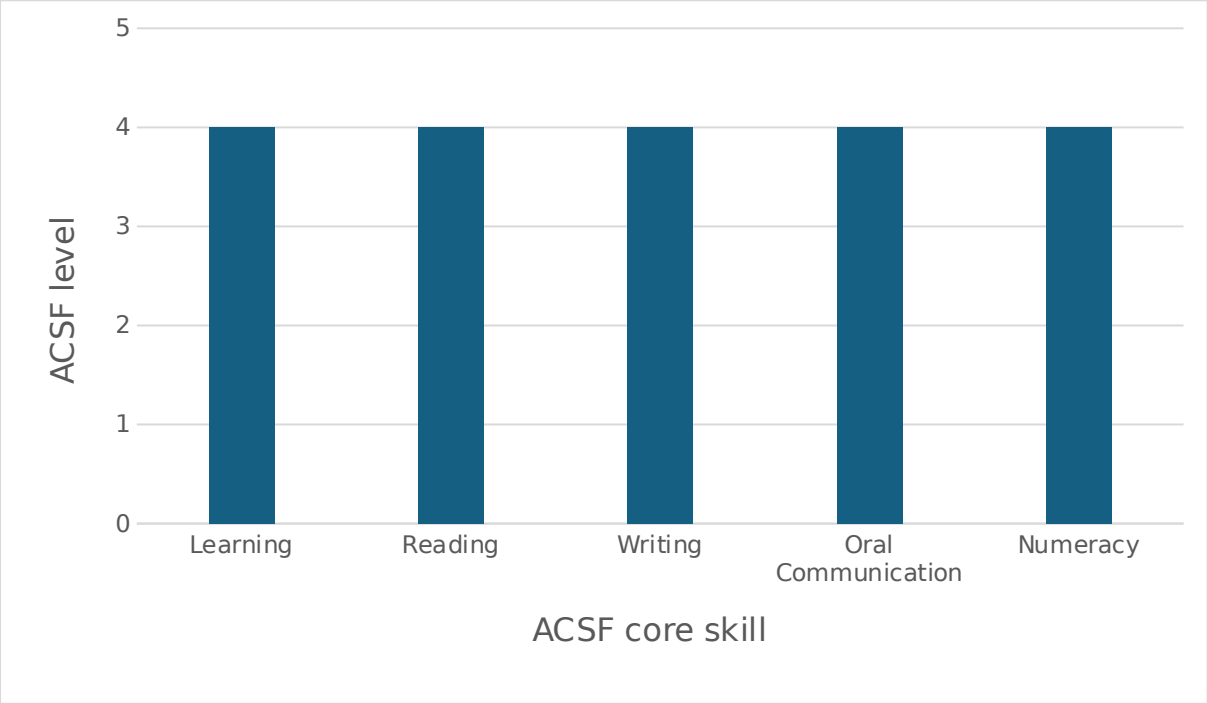
Digital Competence

## Unit sector(s)

Digital Capability

## Foundation skills

The foundation skills in this unit are outlined below




| Core Skills | ACSF Indicators and Performance Features |
|---|---|
| Learning | Designs, reflects on and redesigns approaches, adapting strategies to new contexts.<br>Self-directing learning in an expanding range of contexts and using formal approaches to maintain currency in a specialised field. |
| Reading | Interprets and critically analyses complex texts.<br>Understanding texts with complex structures and some technical specificity, synthesising information from several sources, and |


© Commonwealth of Australia, 2026 Future Skills Organisation

| | |
|---|---|
| | beginning to evaluate credibility and relevance as a routine part of reading. |
| Writing | Communicates complex relationships between ideas, matching style to purpose and audience.<br>Control of text types such as reports and procedures, writing for a range of purposes and integrating information from several sources. |
| Oral Communication | Shows flexibility, choosing structures and strategies across a range of contexts.<br>Complex oral exchanges such as exploring issues, problem solving and reconciling points of view, with control of oral genres such as reports and discussions. |
| Numeracy | Extracts and evaluates embedded mathematical information.<br>Extracting and interpreting information embedded in non-routine texts, including rates, routine formulae and statistical data in complex tables. |

## Range of conditions

N/A

DRAFT


© Commonwealth of Australia, 2026 Future Skills Organisation

# Assessment Requirements for BSBDIG407X Develop Advanced Digital Cyber Security Skills

## Performance Evidence

Learners must demonstrate ability to:

- Identify and assess at least three different cyber security threats in a workplace context, evaluating risk levels and advising a colleague on appropriate protective responses
- Implement, monitor and systematically review security measures across workplace systems to maintain a secure environment
- Protect workplace data and maintain privacy standards, ensuring compliance and coordinating data protection initiatives
- Coordinate a cyber security incident response and recovery activity, communicating with stakeholders during the security event and reviewing outcomes to identify improvements to incident management capability
- Contribute to a programme or initiative that builds sustainable cyber security awareness and culture in a workplace context.

## Knowledge Evidence

Learners must demonstrate advanced knowledge of:

- Emerging technologies used in cyber attacks and cyber security, and approaches for identifying, analysing and evaluating cyber security threats and vulnerabilities in workplace contexts
- Methods for implementing security measures and maintaining secure systems
- Data protection and privacy requirements, including security controls, access management and compliance considerations.
- Incident response procedures, recovery processes and stakeholder communication approaches
- Strategies for promoting security awareness and building organisational 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 |
|---|---|---|

DRAFT



© Commonwealth of Australia, 2026 Future Skills Organisation

| | | |
|---|---|---|
| | Newly created | This unit has been created to 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