Australian Government

BSBDIG507X Develop Highly Advanced Digital Cyber Security Skills

DRAFT

Release: 1

BSBDIG507X Develop Highly 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 manage cyber security across diverse organisational contexts.

The primary purpose of this unit is to develop highly advanced digital capabilities that support strategic leadership across diverse workplace contexts and underpin further professional development. Learners apply these capabilities across all industries in complex workplace tasks at a highly advanced level.

Learners develop highly advanced capability across four competence areas:

- Security awareness and threat recognition
- Data security and privacy
- Incident response and communication
- Security culture and policy.

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 highly advanced knowledge of:

- Emerging developments in cyber security technologies and threat intelligence
- Methods for implementing and maintaining threat management systems
- Ethical and proportionate application of cyber security practices and technologies
- Legislative and regulatory frameworks relating to cyber security
- Emerging developments in data security solutions
- Methods for implementing data security approaches
- Legislative and regulatory frameworks relating to data protection and privacy
- Methods for implementing incident response frameworks
- Approaches for building cyber security capability in others.

© Commonwealth of Australia, 2026 Future Skills Organisation

Skills

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

- Critically evaluate cyber security technologies, threat intelligence and evolving threat landscapes to inform workplace decisions
- Develop and apply integrated threat management approaches that draw on security intelligence and emerging technologies
- Analyse developments in data security, privacy governance and regulatory compliance, applying this analysis to complex workplace practice
- Design and apply data security frameworks incorporating privacy governance and compliance mechanisms
- Take responsibility for the quality of incident response practice within a team or work area, including communication protocols and recovery approaches
- Contribute specialist expertise to improving incident response maturity and resilience
- Assess security culture models, governance frameworks and capability-building approaches, applying this analysis to complex workplace situations
- Apply and contribute to security culture and governance frameworks that embed accountability
- Provide expert advice and mentoring to build another person's advanced capability in cyber security practice.

Application of Knowledge & Skills

Learners work independently and with significant self-direction across varied workplace contexts, applying specialist expertise to cyber security practices.

This applies to complex workplace cyber security challenges requiring application of frameworks and integration of cyber security considerations with organisational risk management and compliance requirements, data security and privacy governance frameworks, and legislative and regulatory requirements relating to cyber security and data protection.

Learners will follow:

- Organisational policies and frameworks for cyber security, data security and privacy governance, contributing to their implementation.

Learners are responsible for:

- Making judgement-based decisions about cyber security approaches, threat management practices, incident response frameworks and capability development approaches, within established organisational frameworks
- Exercising judgement on threat severity, ethical considerations and proportionate application of security technologies
- Determining when specialist expertise, legal or regulatory advice, or senior consultation is required.

Learners are accountable for:

© Commonwealth of Australia, 2026 Future Skills Organisation

- Leading cyber security initiatives in the workplace, the selection of cyber security approaches and the application of threat management practices
- Contributions to organisational policies for data security, privacy and incident response, and the application of governance frameworks and organisational systems in their own work and in building capability in others.

Pre-requisite unit(s)

No pre-requisite units

Competency field(s)

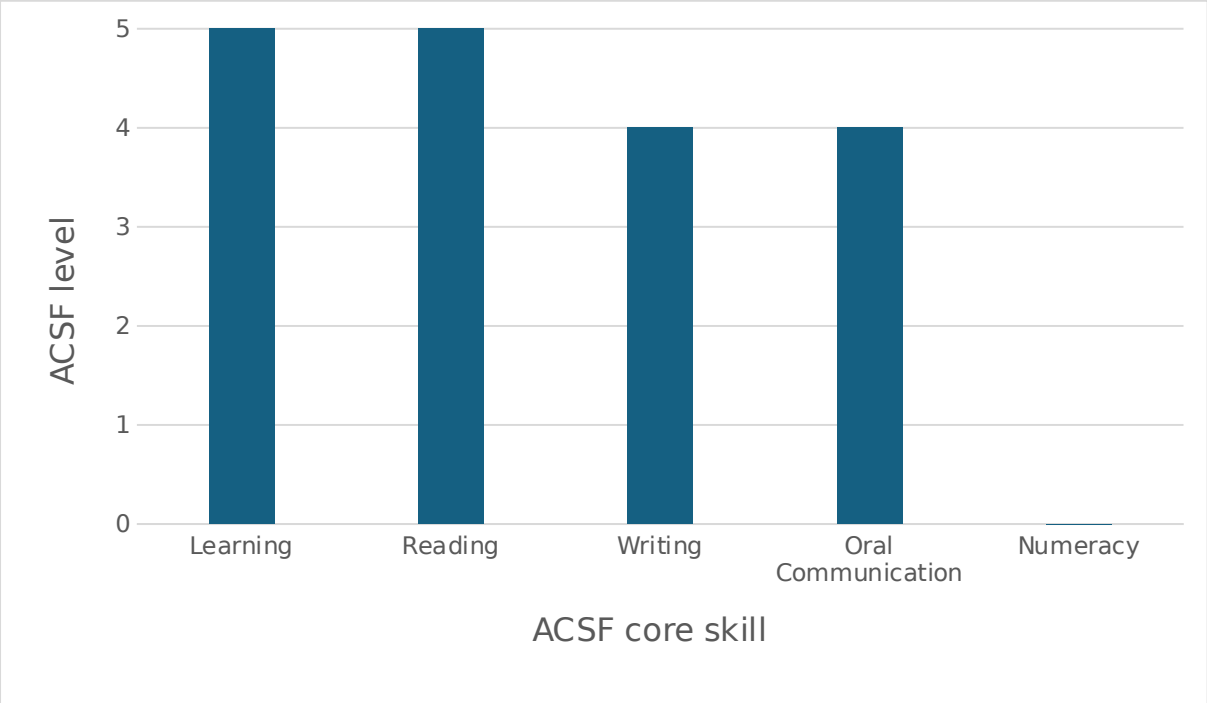
Digital Competence

Unit sector(s)

Digital Capability

Foundation skills

The foundation skills in this unit are outlined below



Core Skills	ACSF Indicators and Performance Features
Learning	Self-directs learning, drawing on a broad and expanding repertoire of strategies. Self-directing learning in highly challenging contexts, critically evaluating information from a wide variety of sources, and using structured approaches to currency and critical reflection.

© Commonwealth of Australia, 2026 Future Skills Organisation

Reading	Organises, evaluates and critiques ideas and information across complex texts. Understanding highly complex, technically dense texts; selecting, synthesising and critically evaluating evidence and arguments; evaluating credibility and relevance against criteria.
Writing	Communicates complex relationships between ideas, matching style to purpose and audience. 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. 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	No ACSF level assigned.

Range of conditions

N/A

DRAFT

© Commonwealth of Australia, 2026 Future Skills Organisation

Assessment Requirements for BSBDIG507X Develop Highly Advanced Digital Cyber Security Skills

Performance Evidence

Learners must demonstrate ability to:

- Address a complex or evolving cyber security threat by developing and applying integrated threat management approaches that draw on security intelligence and emerging technologies
- Resolve a complex data security or privacy compliance issue by developing and applying data security frameworks incorporating governance and compliance mechanisms
- Take responsibility for the quality of incident response practice within a team or work area, including communication protocols and recovery approaches, and contribute to improving incident response maturity and resilience
- Evaluate security culture models, governance frameworks or capability-building approaches as they apply to a complex workplace situation, and provide expert advice or mentoring to build another person's cyber security capability.

Knowledge Evidence

Learners must demonstrate highly advanced knowledge of:

- Emerging developments in cyber security technologies and threat intelligence, methods for implementing threat management systems, ethical and proportionate application of security technologies, and associated legislative and regulatory frameworks
- Emerging developments in data security solutions, methods for implementing data security approaches, and associated legislative and regulatory frameworks for data protection and privacy
- Methods for implementing incident response frameworks in workplace contexts
- Approaches for building organisational cyber security capability and 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

DRAFT

		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