Unit code	BSBXXX131
Unit title	Develop Highly Advanced Digital Cyber Security Skills
Unit outcomes	This unit describes the skills and knowledge required to drive cyber security initiatives and drive organisational transformation. Learners develop highly advanced capability across four competence (C) areas: C1. Security awareness and threat recognition C2. Data security and privacy C3. Incident response and communication C4. Security culture and governance. No licensing, legislative or certification requirements apply to this unit at the time of publication.
Knowledge (K)	Required knowledge includes: K1. emerging developments in cyber security technologies, threat intelligence and data security solutions K2. methods for designing threat management systems, data security strategies and incident response frameworks K3. ethical cyber security practices and proportionate application of security technologies K4. approaches for building cyber security capability in others K5. legislative and regulatory frameworks relating to cyber security, data protection and privacy.
Skills (S)	Required skills include: S1. Stay informed about cyber security technologies, threat intelligence and evolving threat landscapes. S2. Design and implement integrated threat management ecosystems. S3. Stay informed about developments in data security, privacy governance and regulatory compliance. S4. Develop and oversee data security frameworks incorporating privacy governance and compliance mechanisms. S5. Establish organisation-wide incident response frameworks incorporating communication protocols and recovery strategies. S6. Lead initiatives that enhance incident response maturity, resilience and continuous improvement. S7. Stay informed about security culture models, governance frameworks and capability-building strategies. S8. Design and manage security culture and governance frameworks that embed accountability and enhance capability.

	S9. Support and develop others to build advanced capability in workplace cyber security practices.
Application of Knowledge & Skills	At the Highly Advanced level, learners apply knowledge (K1-K5) and skills (S1-S9) with full autonomy across all competence areas (C1-C4) with the following characteristics: • Autonomy: Independently and with full accountability, exercising leadership in cyber security strategy development, policy formulation, and organisational transformation initiatives. • Accountability: Accountable for organisational cyber security capability, strategic outcomes, governance frameworks, and the development of organisational systems and practices. • Responsibility: Responsible for leading organisational cyber security initiatives, establishing governance frameworks, building organisational capability, and driving cultural change. • Context: Highly complex, strategic organisational cyber security challenges requiring systems thinking, governance expertise, and ability to integrate cyber security considerations with organisational strategy, risk management, and compliance frameworks across enterprise contexts. • Decision-Making: Make authoritative decisions on cyber security approaches and threat management strategies; establish organisational policies and governance frameworks for data security, privacy and incident response; lead strategic reviews and capability assessments; determine when external expertise, regulatory consultation, or board-level approval is required.
Assessment Requirements	
Performance evidence (PE)	Learners must demonstrate ability to: PE1. design and implement integrated threat management approaches that incorporate security intelligence and emerging technologies PE2. develop data security frameworks incorporating privacy governance and compliance mechanisms PE3. establish organisational incident response frameworks, including communication protocols and recovery strategies PE4. lead initiatives to improve incident response capability PE5. design and manage security culture and governance frameworks that enhance organisational cyber security capability and support capability development in others. Performance evidence must be demonstrated across at least two different workplace scenarios.

Knowledge evidence (KE)	Learners must demonstrate knowledge of: KE1. emerging developments in cyber security technologies, threat intelligence and data security solutions KE2. methods for designing threat management systems, data security strategies and incident response frameworks KE3. ethical cyber security practices and proportionate application of security technologies KE4. approaches for building cyber security capability in others KE5. legislative and regulatory frameworks relating to cyber security, data protection and privacy. Knowledge evidence must be demonstrated across at least two different workplace scenarios.
Assessment conditions	Assessment must occur in workplace or simulated conditions that reflect real-world environments, including access to: • enterprise-level cyber security platforms requiring governance and integration • scenarios involving complex threats and cross-functional security requirements • opportunities to design, implement and evaluate cyber security transformation initiatives • contexts requiring leadership, mentoring and capability development in others • emerging cyber security technologies requiring strategic evaluation and integration • assistive technologies where required to support diverse learner needs. Assessors must satisfy the requirements for assessors under applicable VET legislation, frameworks, and standards.
Unit Mapping Information	No equivalent unit.
Links	Link to BSB TP Companion Volume Implementation Guide.