



Australian Government

Assessment Requirements for TLIX0009X Employ digital supply chain risk management practices

Release: 1

Assessment Requirements for TLIX0009X Employ digital supply chain risk management practices

Modification History

Release 1. This is the first release of this unit of competency in the TLI Transport and Logistics Training Package.

Performance Evidence

Evidence required to demonstrate competence in this unit must be relevant to and satisfy all requirements of the elements and performance criteria on at least one occasion and includes

- analysing data
- assessing risk outcomes
- communicating with stakeholders
- determining third party cyber security risks
- developing a risk management system and risk management plan for digital supply chains
- documenting continuous improvement actions
- establishing digital supply chain risk management reporting mechanisms
- identifying risks and vulnerabilities in the digital supply chain
- implementing digital supply chain risk management practices
- managing responses to unplanned events
- monitoring and assessing digital supply chain data related to risk management practices
- preparing reports
- reporting risks to the technological integrity of the digital supply chain
- undertaking risk mitigation and reviewing its effectiveness
- using digital supply chain dashboard metrics to assess risks, identify causes and inform stakeholders
- working with risk management policies and procedures.

Knowledge Evidence

Evidence required to demonstrate competence in this unit must be relevant to and satisfy all requirements of the elements and performance criteria and includes knowledge of

- communication methods and techniques
- continuous improvement principles
- data analysis
- digital supply chain policies and procedures
- digital supply chain stakeholders
- digital supply chain technology

- principles of risk management practice
- report requirements
- responses to unplanned digital supply chain events
- risk management plans and risk mitigation
- tools, methods and techniques used for digital supply chain risk management practice
- types of digital supply chain risks including cyber threats.

Assessment Conditions

Assessors must hold credentials specified within the Standards for Registered Training Organisations current at the time of assessment.

Assessment must satisfy the Principles of Assessment and Rules of Evidence and all regulatory requirements included within the Standards for Registered Training Organisations current at the time of assessment.

Assessment must occur in workplace operational situations where it is appropriate to do so. Where this is not appropriate, assessment must occur in simulated workplace operational situations that replicate workplace conditions.

Assessment processes and techniques must be appropriate to the language, literacy and numeracy requirements of the work being performed and the needs of the candidate.

Resources for assessment must include access to a range of

- exercises, case studies or other simulations
- materials and tools including digital supply chain equipment used in industry
- documentation including organisational policies and procedures, industry standards, regulations, codes of practice, operational manuals and equipment specifications.

Links

Companion Volume Implementation Guides are found in VETNet -

<https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=df441c6e-213d-43e3-874c-0b3f7036d851>