



Australian Government

TLIX0009X Employ digital supply chain risk management practices

Release: 1

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.

Application

This unit of competency describes the skills and knowledge required to employ contemporary risk management practices in digital supply chain environments. It includes identifying digital supply chain risks, developing digital supply chain risk management plans, implementing digital supply chain practices and reviewing digital supply chain risk management practices.

Supply chain risk management practices typically focus on identifying, measuring and analysing risks to minimise negative impacts. Risk management and risk control in a digital supply chain, whilst built on standard risk planning strategies, will specifically aim to address cyber security in relation to third parties and the provision of rapid organisational responses to unplanned events.

The unit is applicable to those with management or team leadership responsibilities within a supply chain.

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

Pre-requisite Unit

Not applicable

Competency Field

Supply chain

Unit Sector

X - Logistics

Elements and Performance Criteria

ELEMENTS

Elements describe the essential outcomes.

PERFORMANCE CRITERIA

Performance criteria describe the performance needed to demonstrate achievement of the element.

- | | |
|--|--|
| 1 Identify digital supply chain risks | <ul style="list-style-type: none">1.1 Risks, including vulnerabilities in the digital supply chain, are identified and mapped1.2 Cyber security risks related to third parties in the digital supply chain are identified1.3 Digital supply chain risks are prioritised for severity of impact1.4 Responsibility and level of authority for monitoring risk management practices in the digital supply chain is confirmed |
| 2 Develop digital supply chain risk management plan | <ul style="list-style-type: none">2.1 Digital supply chain risk management plan is developed and communicated to stakeholders2.2 Digital supply chain risk management system is developed, in accordance with the risk management plan2.3 Digital supply chain risk management policies, procedures, processes and practices are developed, in consultation with stakeholders2.4 Reporting mechanisms are established, in accordance with the risk management plan |
| 3 Implement digital supply chain risk management practices | <ul style="list-style-type: none">3.1 Risk mitigation is undertaken, in accordance with risk management procedures3.2 Digital supply chain dashboard metrics are used to assess risks, identify causes and inform stakeholders3.3 Risks to the technical integrity of the digital supply chain are reported, in accordance with risk management procedures3.4 Responses to unplanned digital supply chain events are managed, in accordance with risk management procedures |
| 4 Review and report on digital supply chain risk management practices | <ul style="list-style-type: none">4.1 Digital supply chain risk outcomes, including cyber security, are assessed and the effectiveness of risk mitigation is reviewed, in consultation with stakeholders4.2 Continuous monitoring and assessment of digital |

supply chain data related to risk management practices is reviewed

- 4.3** Report on digital supply chain risk management practices is prepared and presented to approved stakeholders
- 4.4** Continuous improvement actions that support risk management practices are documented

Foundation Skills

Foundation skills essential to performance are explicit in the performance criteria of this unit of competency.

Range of Conditions

Range is restricted to essential operating conditions and any other variables essential to the work environment.

Non-essential conditions may be found in the Companion Volume Implementation Guide.

Unit Mapping Information

This is a new unit. There is no equivalent unit.

Links

Companion Volume Implementation Guides are found in VETNet -
<https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=df441c6e-213d-43e3-874c-0b3f7036d851>

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>