# Assessment event 2 of 2: Project

## Criteria

### Unit code and name

Cluster | Workplace Security

BSBXCS404 | Contribute to cyber security risk management

ICTICT443 | Work collaboratively in the ICT industry

ICTICT451 | Comply with IP, ethics and privacy policies in ICT environments

### Qualification/Course code and name

Select your Qualification/Course code and name from the dropdown.

ICT40120 | Certificate IV in Information Technology

## Student details

Student name

Student number

Version: 20231218

Date created: 18 December 2023

© TAFE NSW 2023  
RTO Provider Number 90003 | CRICOS Provider Code: 00591E

This assessment can be found in the TAFE NSW [Learning Bank](https://share.tafensw.edu.au/share/logon.do?.page=searching.do?in%3DC1b145167-45e0-41ec-9f64-92af668e3e54%26q%3D%26type%3Dstandard%26sort%3Drank%26dr%3DAFTER%26page%3D1).

The content in this document is copyright © TAFE NSW 2023 and should not be reproduced without the permission of TAFE NSW. Information contained in this document is correct at time of printing: 09 January 2024. For current information please refer to our website or your teacher or assessor as appropriate.

## Assessment instructions

Table 1 Assessment instructions

| Assessment details | Instructions |
| --- | --- |
| **Assessment event overview** | The objective of this assessment is to assess your knowledge and performance in complying with organisational policies, contributing to cyber security risk management and working collaboratively in the ICT industry.  This assessment is in 4 parts:   * Part 1: Establish organisational requirements * Part 2: Risk management * Part 3: Consultation * Part 4: Evaluation   And is supported by:   * Submission checklists * Assessment checklists * An observation checklist * Assessment feedback * [Cl\_WorkplaceSecurity\_AE\_Pro2of2\_Appx\_RiskRegister](https://share.tafensw.edu.au/share/items/2a1ffaf1-acc5-4fa2-abf9-e6bd6cb16dd8/0/?attachment.uuid=00c6c451-cb8e-4b85-b04b-44cee0992750) * Simulated organisation, [Gelos Enterprises](https://share.tafensw.edu.au/share/items/d0b458dc-3922-409d-b1fe-9a2f785f4a38/0/?attachment.uuid=5f1677bf-8296-4137-ae33-8b9e30bad1ab)   **Note**: This assessment may contain links to external resources. Access to the long URL is provided via the External resources – Links and URLs section located at the end of this document. |
| **Unit assessment guide** | Refer to the unit assessment guide (UAG) before attempting this assessment event. The UAG contains information including assessment requirements and how to achieve a satisfactory result. |
| **Submission instructions** | When you complete this assessment:   * read the checklist at the end of the assessment to make sure you have completed everything * keep a copy of all the electronic and hardcopy assessments you submit to TAFE NSW * make sure you have completed the assessment declaration before you submit. |

## Task instructions

The assessor will use the criteria outlined in the following tasks to determine if you have satisfactorily completed this assessment event. Follow these instructions to ensure you demonstrate the required knowledge and skills.

Read all instructions carefully and complete all requirements of the assessment. In addition, refer to the checklist that your assessor will use to assess your performance and record your results.

## Part 1: Establish organisational requirements

In this part, you will develop ICT policies, procedures and protocols that meet organisational requirements.

In this assessment, you are a Gelos Enterprises ICT team member working on projects in a virtual environment.

### Task 1: Organisational requirements

**Scenario**

You have been asked to review the Gelos Enterprises policies, procedures and protocols that apply to ICT work teams that work collaboratively with internal departments and external consultants in a virtual environment.

In this task, you will describe and communicate current organisational policies and procedures at the simulated organisation, Gelos Enterprises.

1. **Access and review** the following Gelos Enterprises policies and procedures:

* [Digital Communications Policy and Procedure](https://share.tafensw.edu.au/share/items/5f1cec7b-1d03-446a-85b7-edb42692c34e/0/?attachment.uuid=9a63a882-33e8-4b99-bb8d-95a66a12d6ca) (pdf)
* [Cyber security policy and procedure](https://share.tafensw.edu.au/share/items/5f1cec7b-1d03-446a-85b7-edb42692c34e/0/?attachment.uuid=5cbd245c-a069-4c70-9109-929db6a93dd9) (pdf).

1. **Identify** theorganisation’sexpectations of the ICT team when working collaboratively with internal departments and external consultants in a virtual environment. Describe at least **3** requirements for **each** area of work.

Table 2 Requirements and expectations of work team

| Area of work | Requirements and expectations of team working with internal and external collaborators in a virtual environment |
| --- | --- |
| **Privacy** |  |
| **Ethics** |  |
| **Cyber security safety** |  |

1. **Draft a Teams Chat message** for new members of the ICT Team about the organisation's expectations and requirements. Write your message in accordance with the Gelos Digital Communications Policy and Procedure. Include the following in the message:
2. Where team members can find information about privacy, ethics and cyber security.
3. Sources of advice and support at Gelos Enterprises.
4. How to report a cyber security breach.

Your response should be between 80 and 120 words.

### Task 2: Develop intellectual property policies and procedures

In this task, you will evaluate Intellectual Property (IP) requirements at Gelos Enterprises and assist with developing a clause in the IP policy and procedure.

1. **Access** and review the Gelos Enterprises’ [Intellectual Pr](https://share.tafensw.edu.au/share/items/5f1cec7b-1d03-446a-85b7-edb42692c34e/0/?attachment.uuid=1ab93cf6-0eed-498a-95a5-585a22042d54)operty Policy (pdf).
2. **Outline** the meaning of IP relevant to the ICT industry.
3. **Describe** **3** different types of IP that apply to an ICT team at Gelos Enterprises with an example of each. Your answer should be between 60 and 80 words.
4. **Explain** at least **4** Gelosorganisational policies, procedures and processes that protect IP and the privacy of confidential information. Your answer should be between 70 and 90 words.
5. **Evaluate** whether the current Gelos Enterprises’ IP policy and procedure helps to prevent IP and privacy infringements during collaborations with internal departments and external contractors in a virtual environment. Your answer should be between 50 and 70 words.
6. **Outline** **2** responsibilities in your role as an ICT team member when you identify a risk of an IP infringement. Your answer should be between 50 and 70 words.
7. Your manager asks you to assist in maintaining the IP policy and procedures. **Develop** **a new clause** for the Gelos Enterprises’ Intellectual Property Policy to reduce the IP risks associated with sharing project knowledge with internal departments and external consultants in a virtual environment.

#### Clause 6.2.1 Information sharing protocol

##### Purpose

[Describe what the sub-clause is about, what it aims to achieve and why.]

##### Procedure

[Describe the steps to follow to share project information and knowledge collaboratively in a virtual environment in a way that protects Gelos Enterprises’ IP.]

### Task 3: Team collaboration protocols

In this task, you will assist in developing policies, procedures and protocols for the ICT team to work collaboratively in a virtual environment.

1. **Compare 2 tools/technologies** used to support teams to work collaboratively in a virtual environment.

Table 3 Comparison of team collaboration tools

| Criteria | MS Teams | Name of the second tool: |
| --- | --- | --- |
| **Description** |  |  |
| **Pros** |  |  |
| **Cons** |  |  |

1. **Reflect** on your experiences working collaboratively in a virtual environment. Determine **3** areas to improve protocols and describe how they will enhance collaboration.
2. Your manager has drafted a new Clause 3.9 - Online team collaboration to maintain the currency of the Gelos Enterprises’ [Digital Communications Policy and Procedure](https://share.tafensw.edu.au/share/items/5f1cec7b-1d03-446a-85b7-edb42692c34e/0/?attachment.uuid=9a63a882-33e8-4b99-bb8d-95a66a12d6ca) (pdf). **Develop** **at least 2 protocols** for each part of the clause based on the information you have gathered in Tasks 1 and 2. **Write** the clause using clear and specific language and industry-related terminology.

#### Clause 3.9 Online team collaboration

**All staff** must follow the following protocols when collaborating with others using MS Teams in an online environment.

##### Working collaboratively (2 protocols)

##### Ethical behaviour (2 protocols)

##### Privacy of Gelos' information and knowledge (2 protocols)

##### Cyber security (2 protocols)

##### Responsibilities

Table 4 Responsibilities

|  |  |
| --- | --- |
| Staff member | Responsibilities |
| **Chief Technical Officer** |  |
| **Management team** |  |

1. **Write an email** to your manager using the template provided. Include the following information:

* a greeting
* a summary of your draft policy
* the opportunities for Gelos by improving the protocols
* the potential risks for Gelos of no change.

**Email template**

**From:** [insert email address or name of person sending the email]

**Sent:** [insert date and time]

**To:** [insert receiver’s email address or name]

**CC:** [insert receiver’s email address or name]

**Subject:** [insert email subject]

Dear [insert name]

[insert email body here]

Kind regards,

[insert sender’s name]

## Submission checklist

Submit the following for marking:

Part 1, Assessment event 2 of 2: Project

## Part 2: Risk management

In this part, you will contribute to developing and implementing risk management strategies that control cyber security risks and document the response option applied to each risk.

### Before you begin

* Access and interpret the Gelos Enterprises’ [ICT Risk Management policy](https://share.tafensw.edu.au/share/items/5f1cec7b-1d03-446a-85b7-edb42692c34e/0/?attachment.uuid=d03451a2-9997-461e-89e9-ef2e283fcd1f) (pdf).
* Download [Cl\_WorkplaceSecurity\_AE\_Pro2of2\_Appx\_RiskRegister](https://share.tafensw.edu.au/share/items/2a1ffaf1-acc5-4fa2-abf9-e6bd6cb16dd8/0/?attachment.uuid=00c6c451-cb8e-4b85-b04b-44cee0992750). The Risk Register has 4 sections to complete:

1. Risk management approaches.
2. Identify risks.
3. Risk analysis.
4. Risk treatment.

### Task 1: Update risk management strategies

In this task, you will implement an action from the current risk register and update risk management strategies with new information.

1. **Access and read** Clause 3.1 Risk management approaches from the Gelos Enterprises’ [ICT Risk Manag](https://share.tafensw.edu.au/share/items/5f1cec7b-1d03-446a-85b7-edb42692c34e/0/?attachment.uuid=d03451a2-9997-461e-89e9-ef2e283fcd1f)ement policy (pdf).
2. **Access and view** the video, [IT risk management techniques](https://www.linkedin.com/learning/it-and-cybersecurity-risk-management-essential-training/it-risk-management-techniques-14515284?u=57684225) [LinkedIn Learning, 6:39 min].
3. In **Section 1** of the Risk Register, **amend** the risk management approaches with the industry procedure for treating risk based on the ACAT approach.

### Task 2: Risk Register

In this task, you will identify cyber security risks and maintain a risk register for your manager.

1. **Risk identification**

In **Section 2** of the Risk Register, **review** the 3 non-compliance incidents and potential cyber security risks associated with using MS Teams for online collaboration.

1. **Explain** why each incident is a cyber security risk.
2. **Describe** the potential vulnerabilities of assets that could be affected by this risk, such as those related to IP, ethics and privacy.
3. **Risk analysis**

In **Section 3** of the Risk Register, use your industry knowledge and the information in the Gelos Enterprises’ [ICT Risk Management Policy](https://share.tafensw.edu.au/share/items/5f1cec7b-1d03-446a-85b7-edb42692c34e/0/?attachment.uuid=d03451a2-9997-461e-89e9-ef2e283fcd1f) (pdf) to complete the following:

1. **Describe** the 3 risks.
2. **Analyse the likelihood** of each risk occurring from Rare to Almost certain.
3. **Analyse the impact** on the business or the consequence if the risk does occur from Insignificant to Extreme.
4. **Evaluate the risk** by mapping the likelihood of the risk against the impact of the risk in the risk matrix in the Gelos Enterprises’ [ICT Risk Management P](https://share.tafensw.edu.au/share/items/5f1cec7b-1d03-446a-85b7-edb42692c34e/0/?attachment.uuid=d03451a2-9997-461e-89e9-ef2e283fcd1f)olicy (pdf) to determine the level of risk from Low to Extreme.
5. **Prioritise the risks** from 1 to 3 based on the level of risk.
6. **Risk management**

In **Section 4** of the Risk Register, complete the following for the **2** highest severity cyber security risks.

1. **Select** the risk control option from Avoid, Control, Accept and Transfer.
2. **Describe** at least **2** specific cyber security response strategies or actions for each risk consistent with Gelos Enterprises’ policies and procedures.
3. **List** the personnel responsible for the implementation of risk controls, including yourself.
4. **Identify benchmarks** to track the effectiveness of each risk management strategy.

## Submission checklist

Submit the following for marking:

Cl\_WorkplaceSecurity\_AE\_Pro2of2\_Appx\_RiskRegister.

## Part 3 Consultation

In this part, you will prepare a meeting agenda and consult with stakeholders about using MS Teams and the protocols for team collaboration and cyber security.

### Before you begin

**Organise** at least **2** people, such as peers, work colleagues or friends, to represent one Gelos ICT team member and one external consultant team member in a consultation meeting. The people representing the team members will:

* be 18 years or over
* be able to participate in a consultation in a virtual environment
* be able to understand and provide meaningful feedback on the agenda items
* have access to a computer or other device with MS Teams, a camera and a microphone.

### Task 1: Consultation meeting agenda

In this task, you will prepare an agenda to help you facilitate the consultation meeting in Task 2.

1. **Download** the Gelos Enterprises’ [Meeting Agenda Template (dotx)](https://share.tafensw.edu.au/share/items/02285ff1-cfb2-4af4-b402-fdc23bf4bf11/0/?attachment.uuid=dd52677e-b030-47e7-82ee-117224ece8c3).
2. **Read** the Task 2 consultation meeting instructions.
3. **Incorporate** the Task 2 meeting instructions as agenda items in the template.

### Task 2: Consultation meeting

In this task, you will consult with stakeholders about using MS Teams and the protocols for team collaboration and cyber security. You have been allocated up to 20 minutes for your consultation.

Read the list of criteria provided in the **Observation Checklist** (at the end of this document) to understand what skills you need to demonstrate. This Checklist outlines the Performance Criteria and Performance Evidence your Teacher/Assessor will be assessing you on as they observe you complete the assessment task.

**The consultation must take place in MS Teams.**

Your Assessor may directly observe you facilitate the consultation online, or you may submit a recording of the consultation as video evidence.

If you are submitting the consultation as video evidence, follow the [V](https://share.tafensw.edu.au/share/items/744af7d4-a241-45e2-adb0-0e13f2fe4950/0/?attachment.uuid=01c3c87a-4599-48c2-91f0-68a00b5bbb4c)ideo recording instructions (pdf). These instructions include useful tips, links to resources, and a demonstration video.

#### Facilitate the consultation

1. **Welcome** the participants and explain the **purpose and context** of the consultation.
2. **Summarise** the online protocols you developed in Part 1, Task 3.3: Team collaboration protocols.
3. **Explain** that you will monitor compliance with the protocols during the online consultation meeting.
4. **Facilitate a group discussion,** includingseeking and responding to feedback about the team collaboration protocols.
5. **Communicate** the potential risks and proposed risk management strategies related to team collaboration from Part 2, Task 2.3: Risk management.
6. **Facilitate a group discussion,** includingseeking and responding to feedback about the effectiveness of your proposed cyber security strategies.
7. **Collaborate** with the meeting participants to determine and agree on a practical process for team members to warn Gelos Enterprises of potential new cyber security risks. Summarise the agreed strategy.
8. **Review** compliance with the team collaboration and cyber security protocols during the consultation. Discuss any modifications to behaviour that are needed.
9. **Close** the meeting.

## Submission checklist

Submit the following for marking:

Part 3, Task 1: Gelos Enterprises’ Meeting agenda template, including:

* Link to the recording of the consultation, where not directly observed by the TAFE Assessor. This is the link to the recording: [Video link].

## Part 4: Evaluation

**Scenario**

Your new protocols were implemented 3 months ago.

- Clause 6.2.1 Information sharing protocol

- Clause 3.9 Online team collaboration.

The ICT Security Senior Manager has asked you to review 2 instances of non-compliance and recommend actions.

In this part, you will review compliance with workplace protocols for working collaboratively and contribute to the development of non-compliance incident recommendations.

### Before you begin

Access and read the following:

* Gelos Enterprises’ [Cyber Security Policy and Procedure](https://share.tafensw.edu.au/share/items/5f1cec7b-1d03-446a-85b7-edb42692c34e/0/?attachment.uuid=5cbd245c-a069-4c70-9109-929db6a93dd9) (pdf)
* Gelos Enterprises’ [Intellectual Property Policy](https://share.tafensw.edu.au/share/items/5f1cec7b-1d03-446a-85b7-edb42692c34e/0/?attachment.uuid=1ab93cf6-0eed-498a-95a5-585a22042d54) (pdf)
* Gelos Enterprises’ [Digital Communications Policy and Procedure](https://share.tafensw.edu.au/share/items/5f1cec7b-1d03-446a-85b7-edb42692c34e/0/?attachment.uuid=9a63a882-33e8-4b99-bb8d-95a66a12d6ca) (pdf)

### Task 1: Incident 1

In this task, you will complete an **Incident Response Plan** in response to an incident report.

1. **Read** Part A - Incident report.
2. **Complete** Part B - Risk analysis.
3. **Complete** Part C – Action plan.
4. **Complete** Part D - Improvements.

#### Incident Response Plan: Incident 1

##### Incident report

Table 5 Incident report

| Details of incident | Description |
| --- | --- |
| Full name reporter | Charlie Young |
| Location | ICT Projects Team, Level 1 |
| Email address | charlie.young@gelosmail.com.au |
| Phone | X5811 |
| Detailed description | A Gelos Enterprises’ team member has shared access to a computer code that they developed for the ICT team with an external contractor on MS Teams. |

##### Risk analysis

Type of incident e.g., cyber security, privacy, ethics, intellectual property.

Name/s of relevant Gelos Enterprises policy procedure or protocol.

Specific area of non-compliance.

Incident classification i.e., Very high, high, medium, or low.

##### Action plan

Recommend at least **2** actions to respond to the non-compliance incident.

Table 6 Action plan

| **Actions required to resolve the incident** | **Resources required to resolve the incident** | **Job title of person/s responsible for each action** | **Expected resolution time i.e., immediate, today, this week, this month** | **Systems or services that may be affected during the response process** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |

##### Improvement

Determine why the current protocols were not effective.

Propose an improvement to future work protocols in virtual environments.

### Task 2: Incident 2

In this task, you will complete an **Incident Response Plan** in response to an incident report.

1. **Read** Part A - Incident report.
2. **Complete** Part B - Risk analysis.
3. **Complete** Part C – Action plan.
4. **Complete** Part D - Improvements.

#### Incident Response Plan: Incident 2

##### Incident report

Table 7 Incident report

| Details of incident | Description |
| --- | --- |
| Full name reporter | Charlie Young |
| Location | ICT Projects Team, Level 1 |
| Email address | charlie.young@gelosmail.com.au |
| Phone | X5811 |
| Detailed description | A Gelos team member was given a link in an MS Teams chat to an unfamiliar, overseas source of information about cyber security. The team member quickly opened the link before discussing it with their colleagues and subsequently realised there was a potential risk of infection from malware. |

##### Risk analysis

Type of incident e.g., cyber security, privacy, ethics, intellectual property.

Name/s of relevant Gelos Enterprises policy procedure or protocol.

Specific area of non-compliance.

Incident classification i.e., Very high, high, medium, or low.

##### Action plan

Recommend at least **2** actions to respond to the non-compliance incident.

Table 8 Action plan

| **Actions required to resolve the incident** | **Resources required to resolve the incident** | **Job title of person/s responsible for each action** | **Expected resolution time i.e., immediate, today, this week, this month** | **Systems or services that may be affected during the response process** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |

##### Improvement

Determine why the current protocols were not effective.

Propose an improvement to future work protocols in virtual environments.

## Submission checklist

Submit the following for marking:

This completed Assessment event 2 of 2: Project

## Checklist

The assessment checklists lists the **requirements for each task** in this assessment as outlined in the student's assessment instructions. The assessor will use the checklists to ensure **all** required tasks have been completed and submitted and provide feedback for each task.

Note that S = Satisfactory and U/S = Unsatisfactory.

A second attempt is required where the first attempt is unsatisfactory.

### Part 1: Establish organisational requirements

Table 9 Checklist

| Task number | Did the student do the following? | S | U/S | S | U/S | Assessor comments |
| --- | --- | --- | --- | --- | --- | --- |
| 1.1 | Locate, access and extract information from existing organisational policies to complete tasks |  |  |  |  | Date: |
| 1.2 | Demonstrate knowledge of key policies, procedures and protocols  Describe at least 3 requirements and protocols for ways of working, including privacy, ethics, and cyber security safety |  |  |  |  |  |
| 1.3 | Draft a message for relevant personnel to share information using language required for audience needs  Provide support and advice on information sources for ethics, privacy and cyber security  Explain how personnel report a breach |  |  |  |  |  |
| 2.1 | Locate, access and extract information from existing organisational policies to complete tasks |  |  |  |  |  |
| 2.2 | Outline the meaning of intellectual property (IP) |  |  |  |  |  |
| 2.3 | Describe 3 different types of IP that apply to an ICT team at Gelos Enterprises with an example of each |  |  |  |  |  |
| 2.4 | Evaluate at least 3 different types of IP within an organisation |  |  |  |  |  |
| 2.5 | Evaluate whether implemented IP policy and procedures help prevent IP and privacy infringements |  |  |  |  |  |
| 2.6 | Identify own role in protecting and fulfilling the requirements of the organisation's IP policy and procedures when an IP infringement is identified |  |  |  |  |  |
| 2.7 | Assist with the development of an organisational IP policy and procedure clause  Develop a protocol to share knowledge collaboratively by applying risk management strategy |  |  |  |  |  |
| 3.1 | Identify, review, and compare 2 communication tools and technology to support teams working collaboratively in virtual environments  Demonstrate knowledge of virtual platforms |  |  |  |  |  |
| 3.2 | Determine 3 areas to improve team protocols for working collaboratively in a virtual environment |  |  |  |  |  |
| 3.3 | Develop 2 protocols for teams working collaboratively in virtual environments that help achieve team objectives  Assist with the development of protocols for ethics and privacy and cyber security  Determine roles and responsibilities of team members |  |  |  |  |  |
| 3.4 | Write an email summarising the draft policy  Communicate potential risks and opportunities for improvement of virtual collaboration, IP, ethics, privacy and cyber security protocols |  |  |  |  |  |

### Part 2: Risk management

Table 10 Checklist

| Task number | Did the student do the following? | S | U/S | S | U/S | Assessor comments |
| --- | --- | --- | --- | --- | --- | --- |
| 1.1 | Locate, access and extract information from existing organisational policies to complete tasks |  |  |  |  | Date: |
| 1.2 | Access current industry-specific information |  |  |  |  |  |
| 1.3 | Update risk management strategies with new information from video  Maintain risk register with an update |  |  |  |  |  |
| 2.1 | Review potential risks and non-compliance incidents  Report on why incidents are a risk and the potential vulnerabilities of assets that could be affected by this risk, such as those that relate to IP, ethics and privacy |  |  |  |  |  |
| 2.2 | Contribute to organisational risk assessment and identification process  Describe 3 risks  Analyse the likelihood and impact of each risk  Evaluate and prioritises the risk |  |  |  |  |  |
| 2.3 | Contribute to developing risk management strategies that control identified risks  Assist in developing suitable cyber security response options  List the personnel responsible for implementation, including self  Identify benchmarks to track the effectiveness of each risk management strategy |  |  |  |  |  |

### Part 3: Consultation

Table 11 Checklist

| Task number | Did the student do the following? | S | U/S | S | U/S | Assessor comments |
| --- | --- | --- | --- | --- | --- | --- |
| 1.1 | Download the GE agenda template |  |  |  |  | Date: |
| 1.2 | Read Task 2 consultation meeting instructions |  |  |  |  |  |
| 1.3 | Incorporate the Task 2 meeting instructions as agenda items in the template  Plan and implement a range of tasks directly related to own role  Submit agenda |  |  |  |  |  |
| 2 | *Refer to the Observation Checklist* |  |  |  |  |  |

### Part 4: Evaluation

Table 12 Checklist

| Task number | Did the student do the following? | S | U/S | S | U/S | Assessor comments |
| --- | --- | --- | --- | --- | --- | --- |
| 1.1 | Read an incident report and prepare and manage an Incident Response Plan appropriate to the scenario |  |  |  |  | Date: |
| 1.2 | Review compliance with IP and cyber security protocols to work collaboratively in a virtual environment  Report on areas of potential risk |  |  |  |  |  |
| 1.3 | Contribute to the development of non-compliance incident recommendations  Respond intuitively to problems requiring immediate attention, drawing on experience to devise solutions |  |  |  |  |  |
| 1.4 | Support evaluation of the effectiveness of implemented strategies  Determine improvements to future work protocols |  |  |  |  |  |
| 2.1 | Read an incident report and prepare and manage an Incident Response Plan appropriate to the scenario |  |  |  |  |  |
| 2.2 | Review compliance with IP and cyber security protocols to work collaboratively in a virtual environment  Report on areas of potential risk |  |  |  |  |  |
| 2.3 | Contribute to the development of non-compliance incident recommendations  Respond intuitively to problems requiring immediate attention, drawing on experience to devise solutions |  |  |  |  |  |
| 2.4 | Support evaluation of the effectiveness of implemented strategies  Determine improvements to future work protocols |  |  |  |  |  |

## Observation checklist

The assessor will use this checklist to assess your performance whilst observing you complete Part 3. Use this observation checklist to understand what skills you need to demonstrate.

The observation checklist lists the observable criteria for Part 3. You must meet all the criteria.

Note that S = Satisfactory and U/S = Unsatisfactory. A second attempt is required when the first attempt is unsatisfactory.

### Part 3 Consultation

Table 13 Checklist

| Task number | Did the student do the following? | S | U/S | S | U/S | Assessor comments |
| --- | --- | --- | --- | --- | --- | --- |
| 2.1 | Welcome the consultation meeting participants  Explain the purpose and context of the consultation |  |  |  |  | Date: |
| 2.2 | Summarise the online protocols you developed previously  Share knowledge and information with others using a digitally based technology and application  Provide information using language and terminology required for the audience |  |  |  |  |  |
| 2.3 | Explain that compliance with the protocols will be monitored during the online consultation meeting  Use appropriate technology platforms to assist with cyber security risk management |  |  |  |  |  |
| 2.4 | Facilitate a group discussion about the strategies for the virtual environment protocols  Seek and respond to feedback on team communication processes  Use listening and questioning techniques and project-specific terminology to liaise with team members, present information and obtain feedback |  |  |  |  |  |
| 2.5 | Communicate the potential risks and proposed risk management strategies related to team collaboration  Consult with stakeholders to determine the scope of risk management  Provide information using language and terminology required for the audience |  |  |  |  |  |
| 2.6 | Facilitate a group discussion about the effectiveness of the cyber security strategies  Seek and respond to feedback  Present options for risk management strategies for approval  Ask open and closed probing questions and actively listen to clarify consultations |  |  |  |  |  |
| 2.7 | Collaborate with the meeting participants to determine and agree on a practical process for team members to warn Gelos Enterprises of potential new cyber security risks  Summarise the agreed strategy  Assist in establishing feedback processes that provide warning of potential new risks according to organisational requirements  Collaborate with others to achieve joint outcomes, playing an active role in facilitating group interaction, influencing direction and occasionally taking a leadership role  Work collaboratively with interdisciplinary teams to develop cyber risk management strategies |  |  |  |  |  |
| 2.8 | Review compliance with the team collaboration and cyber security protocols during the consultation  Discuss any modifications to behaviour that are needed  Monitor whether participants are abiding by organisational IP, ethics and privacy policy and procedures  Contribute to monitoring cyber security risk |  |  |  |  |  |
| 2.9 | Close the meeting |  |  |  |  |  |

## Additional evidence for verification of assessment

Assessors may ask questions to clarify your understanding during the assessment event.

You may be asked questions:

* to clarify your understanding (for example, ‘Why did you select that particular piece of equipment?’)
* to capture contingencies that may form part of the demonstration (for example, dealing with faults or unexpected events)
* to prevent a work, health and safety incident.

If questions are required during the assessment event, these questions and your responses will be recorded in this table.

Table 14 Additional evidence

| Questions asked by assessor | Student responses |
| --- | --- |
|  |  |
|  |  |
|  |  |

### Additional ad hoc question/s asked by the Assessor

Additional ad hoc questions may be asked by the assessor during or after the assessment event. This section provides the assessor opportunity to record these questions and your responses.

1. Assessor question (as required):

[Record your additional questions here]

Student response (as required):

[Record the student response/s]

1. Assessor question/s (as required):

[Record your additional questions here]

Student response/s (as required):

[Record the student response/s]

1. Assessor question/s (as required):

[Record your additional questions here]

Student response/s (as required):

[Record the student response/s]

## External resources – Links and URLs

Long URLs and permalinks are provided for access to content when the assessment is not used digitally, for example, not clickable.

Table 15 Long URLs

| Resource Name | Long URL |
| --- | --- |
| The Learning Bank | https://share.tafensw.edu.au/share/home.do |
| Research and referencing skills | https://tafensw.libguides.com/research/referencing |
| Gelos Enterprises | https://share.tafensw.edu.au/share/items/d0b458dc-3922-409d-b1fe-9a2f785f4a38/0/?attachment.uuid=5f1677bf-8296-4137-ae33-8b9e30bad1ab |
| Gelos Enterprises’ Meeting Agenda Template (dotx) | https://share.tafensw.edu.au/share/items/02285ff1-cfb2-4af4-b402-fdc23bf4bf11/0/?attachment.uuid=dd52677e-b030-47e7-82ee-117224ece8c3 |
| TAFE NSW Assessment Guidelines (pdf) | https://share.tafensw.edu.au/share/items/d36df03f-9651-4d43-8c9d-a299699e8585/0/?attachment.uuid=30e52f91-8a9f-4df1-bf7f-91168307cfb9 |
| Gelos Enterprises’ Digital Communications Policy and Procedure | https://share.tafensw.edu.au/share/items/5f1cec7b-1d03-446a-85b7-edb42692c34e/0/?attachment.uuid=9a63a882-33e8-4b99-bb8d-95a66a12d6ca |
| Gelos Enterprises’ Cyber security policy and procedure | https://share.tafensw.edu.au/share/items/5f1cec7b-1d03-446a-85b7-edb42692c34e/0/?attachment.uuid=5cbd245c-a069-4c70-9109-929db6a93dd9 |
| Gelos Enterprises’ Intellectual Property Policy | https://share.tafensw.edu.au/share/items/5f1cec7b-1d03-446a-85b7-edb42692c34e/0/?attachment.uuid=1ab93cf6-0eed-498a-95a5-585a22042d54 |
| Gelos Enterprises’ ICT Risk Management Policy | https://share.tafensw.edu.au/share/items/5f1cec7b-1d03-446a-85b7-edb42692c34e/0/?attachment.uuid=d03451a2-9997-461e-89e9-ef2e283fcd1f |
| LinkedIn Learning, IT risk management techniques (video) | https://www.linkedin.com/learning/it-and-cybersecurity-risk-management-essential-training/it-risk-management-techniques-14515284?u=57684225 |
| Video recording instructions | https://share.tafensw.edu.au/share/items/744af7d4-a241-45e2-adb0-0e13f2fe4950/0/?attachment.uuid=01c3c87a-4599-48c2-91f0-68a00b5bbb4c |

This page is not required for online assessment submissions.

### Student assessment declaration

This assessment is my original work and has not been:

* copied from any source without proper referencing
* written for me by any other person except where such collaboration has been approved by a teacher or assessor.

Student signature and date

### Reasonable adjustment

Reasonable adjustment was in place for this assessment event.

If so, please provide details of any reasonable adjustment strategies that were implemented:

[Insert reasonable adjustment strategies]

### Assessment outcome

Satisfactory  Unsatisfactory

Comments

[Insert comments]

Assessor name, signature and date

Student acknowledgement of assessment outcome

[Would you like to make any comments about this assessment?]

Student name, signature and date