



BSBXCS403

# Contribute to cyber security threat assessments

Assessment 3 of 4

Role Play



## Assessment Instructions

### Task overview

Read each question carefully before typing your response in the space provided.

### Additional resources and supporting documents

To complete this assessment, you will need:

- Learning Resources
- CBSA Communication Policy and Procedures



## Assessment Information

### Submission

You are entitled to three [3] attempts to complete this assessment satisfactorily. Incomplete assessments will not be marked and will count as one of your three attempts.

All questions must be responded to correctly to be assessed as satisfactory for this assessment.

Answers must be typed into the space provided and submitted electronically via the LMS. Hand-written assessments will not be accepted unless previously arranged with your assessor.

### Reasonable adjustment

Students may request a reasonable adjustment for assessment tasks.

Reasonable adjustment usually involves varying:

- the processes for conducting the assessment [e.g. allowing additional time]
- the evidence gathering techniques [e.g. oral rather than written questioning, use of a scribe, modifications to equipment]

However, the evidence collected must allow the student to demonstrate all requirements of the unit.

Refer to the Student Handbook or contact your Trainer for further information.



Please consider the environment before printing this assessment.

### Case Study

You have been tasked by your manager, Con Kafatos, to present the Cybersecurity Risk Assessment and Action Plan you have developed to him and Tina Yates, an IT Technician in your department at CBSA. The aim of this presentation is so that you can present the documents you have developed previously for feedback and improvement.

### Task 1

You will present the following documents that you have developed to the consultation participants (Con Kafatos and Tina Yates), asking for their feedback and possible improvements:

- Cybersecurity Threat Risk Assessment Template
- Action Plan Template
- You must comply with CBSA's Communication Policy and Procedures during the consultation session.
- Take notes of suggestions for improvement received during the meeting, as you will need these to complete the following tasks.
- The role play must be a maximum of 10-15 minutes.

During the role play, your Assessor will be looking to see that you demonstrate the following:

- Communicate findings of the assessment of business impact to staff in the Information Technology department at CBSA.
- Ask open and closed probing questions and actively listen to clarify information.
- Present the cybersecurity review insights and the related potential risk impacts on the workplace to the Information Technology department staff at CBSA.

Communicate review outcomes and cybersecurity improvements required as per the Action Plan.

**Assessor instructions:** The purpose of this task is to observe the student's skills in a simulated environment. The student must demonstrate the following skills:

- Communicate findings of the assessment of business impact to staff in the Information Technology department at CBSA.
- Ask open and closed probing questions and actively listen to clarify information.
- Present the cybersecurity review insights and the related potential risk impacts on the workplace to the Information Technology department staff at CBSA.
- Communicate review outcomes and cybersecurity improvements required as per the Action Plan.

### Role play instructions

In this task, you will participate in a role/play meeting with **two (2) others**. These may be sourced using one of the following options:

- peers to who you are already working within the industry your qualification relates to.
- fellow students who will play the role of the stakeholders. Please contact your fellow students via the Discussion Forum and coordinate your role play with them directly.

The role play/meeting must not exceed **15 minutes** in duration and must address all elements of the Observation Checklist below.

If you are unable to find participants to play the role of the other team members, contact your assessor via the Discussion Forum, who will discuss options for pairing up with other students to complete this task.

### **Option 1: Peer participants**

Should you complete this task with your peers, you must fully brief all participants, providing them with the context of the role play/meeting, a role outline to play and a copy of the observation checklist so that they can prepare for the recording.

Peers will need to state their name and job title at the start of the recording to inform consent.

### **Option 2: Fellow student participants**

Fellow students participating in the recording must be provided with context to their role and responsibilities in the session and have reviewed the assessment activity and observation checklist so that they can prepare for the recording.

Students will need to state their name and that they are a student [as their job title] at the start of the recording to inform consent.

### **Participants' briefing instructions:**

#### **Role 1: Con Kafatos**

*You are playing the role of Con Kafatos, the IT Manager. Con requested this consultation session to understand what the student has developed as part of his instructions to identify cybersecurity threats, their risks, and the control measures to combat these threats/risks.*

*During the role play, you must be accommodating to the students' presented information but should ask clarifying questions if you don't understand the presented information. You can also offer suggestions on what improvements can be made if you determine any during the student's presentation.*

*Example questions to ask can include variations of the following:*

*Can you please provide more detail on the email phishing threat event?*

*What made you select these threat events as opposed to other threat events?*

*What other control measures might apply to the email phishing threat event?*

#### **Role 2: Tina Yates**

*You are playing the role of Tina Yates, the IT Technician at CBSA. You are a co-worker of the student and work in the Information Technology department with them. You have been requested to attend the consultation session by the other role-play participant, Con Kafatos, the IT Manager, for your input.*

*During the role play, you must be accommodating to the students' presented information but should ask clarifying questions if you don't understand the information. You can also suggest improvements if you determine any during the student's presentation.*

*Example questions to ask can include variations of the following:*

*Why did you give the email phishing threat event a moderate risk rating?*

*Do you think the timeline for the action task 'staff training on email phishing and password update' in the Action Plan is achievable, or should more time be allowed?*

## Recording instructions

Your role play must be recorded with all participants captured in a virtual room using a system such as Zoom, Skype or Teams.

Consent to participate in the recording must be captured for all participants at the start of the meeting. This is achieved by the student reading the following statement at the start of the recording, with all participants replying with their name and job title to inform consent.

*"This session/presentation is being recorded for assessment purposes for my course with Swinburne Open Education. This session will be recorded and submitted through my course online learning platform to my Assessor for grading. All participant/s in this session indicate their consent to be included in this recording by stating their name and job title."*

The time taken to capture consent at the start of the recording does not count towards the recording time limit.

Include this recording as part of your assessment submission.

## ASSESSOR OBSERVATION CHECKLIST

Students are required to upload a video of themselves and **two (2) others** engaged in a short meeting.

The participants must be fully briefed as outlined in the role play instructions.

The meeting should be a maximum of **15 minutes**.

Students must demonstrate each of the performance criteria outlined in the observation checklist below.

ACTIVITY	SATISFACTORY YES / NO	ASSESSOR COMMENTS
<b>Task checklist</b>		
<ul style="list-style-type: none"> <li>The student consulted with stakeholders to inform decision making.</li> </ul>		<p><i>The student led the stakeholder consultation meeting, ensuring they:</i></p> <ul style="list-style-type: none"> <li><i>displayed effective communication skills, including</i></li> </ul>

			<p><i>positive verbal and non-verbal communication skills, such as maintaining eye contact, acknowledging questions, etc.</i></p> <ul style="list-style-type: none"> <li>▪ <i>used active listening to respond appropriately to stakeholder queries during the consultation</i></li> <li>▪ <i>implemented a collaborative environment where two-way communication occurred between all stakeholders.</i></li> </ul>
<ul style="list-style-type: none"> <li>• The student presented insights from the cybersecurity review to the Information Technology department staff at CBSA and the related potential risk impacts on the workplace.</li> </ul>			<p><i>The student covered all threat events providing a breakdown of each event, the description and the risk rating assigned to each threat event.</i></p>
<ul style="list-style-type: none"> <li>• The student communicated review outcomes and cybersecurity improvements required as per the Action Plan.</li> </ul>			<ul style="list-style-type: none"> <li>▪ <i>The student outlined all the actions in the Action Plan they developed, including:</i></li> <li>▪ <i>the name of each task, why it is required</i></li> <li>▪ <i>the responsibility assigned to each task</i></li> <li>▪ <i>the timeline for each task</i></li> <li>▪ <i>the resources for each task.</i></li> </ul>
<ul style="list-style-type: none"> <li>• The student uses questioning skills during the consultation session to clarify information and their understanding.</li> </ul>			<p><i>The student actively participates in the stakeholder consultation, asking clarifying and probing questions to help clarify their understanding of the information being communicated.</i></p> <ul style="list-style-type: none"> <li>▪ <i>The student responds to any questions asked by the participants providing relevant information to address the questions and displaying sufficient knowledge of cybersecurity.</i></li> </ul>

**Assessment checklist:**

Students must have completed all questions within this assessment before submitting. This includes:

1	Task 1 - Role Play	<input type="checkbox"/>
---	--------------------	--------------------------



**Congratulations you have reached the end of Assessment 3!**

© RTO Advice Group Pty. Ltd. as trustee for RTO Trust (ABN 88 135 497 867) t/a Eduworks Resources 2022  
Reproduced and modified under license by UP Education Online Pty Ltd.

**© UP Education Online Pty Ltd 2021**

Except as permitted by the copyright law applicable to you, you may not reproduce or communicate any of the content on this website, including files downloadable from this website, without the permission of the copyright owner.