



BSBXCS404

Contribute to cyber security risk management

Assessment 4 of 5

Role Play

ASSESSOR GUIDE



Assessment Instructions

Task overview

Read the instructions 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

For the purposes of this task, you will play the role of Tan Yamamoto [Software Developer] at CBSA.

You have been tasked by your manager, Con Kafatos, to present the cybersecurity risk assessment and action plan you have developed to himself 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 can only complete this assessment task after you have completed the in the previous assessment task, where you developed the necessary documentation you will need to present in this consultation meeting with the stakeholders.

You are to 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.

If the role play participants identify improvements to your risk assessment or action plan template, you are to update these documents in line with the agreed improvements.

You must comply with **CBSA Communication Policy and Procedures** during the consultation session.

The role play will be approximately 10–15 minutes.

During the role play, your assessor will be looking to see that you can:

- consult with stakeholders to determine the scope of risk management appropriate to the organisation and industry
- present options for risk management strategies for approval within the scope of own role review relevant critical cyber risk management strategies appropriate to the level of risk present insights from cybersecurity review to required personnel and potential related impacts on the workplace
- communicate review outcomes and cybersecurity improvement requirements according to organisational policies and procedures
- document approved risk management strategies
- update risk management strategies with new information as required.
- submit the updated documents using the following naming convention:

<Student Number> Updated <insert name of the document>

Examples:

<Student Number> Updated Action Plan

<Student Number> Updated Cybersecurity Threat Risk Assessment

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:

- stakeholder consultation to determine the scope of risk management actions

- presenting risk management strategies options, insights and impacts
- reviewing cyber risk management strategies
- updating risk management strategies based on consultation feedback

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 virus threat event?

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

What other control measures might apply to the virus 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, your department's 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 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:

Why did you give the virus threat event a risk rating of high?

Is the timeline for the action task [install anti-malware software in the Action Plan] 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
Task checklist		
<ul style="list-style-type: none"> The student consulted with stakeholders to determine the scope of risk management actions. 		<p><i>The student led the stakeholder consultation meeting, ensuring they:</i></p> <ul style="list-style-type: none"> <i>Displayed effective communication skills, including both positive verbal and non-verbal communication skills, such as maintaining eye contact, acknowledging questions asked, etc.</i> <i>Used active listening to respond appropriately to stakeholder queries during the consultation.</i> <i>Implemented a collaborative environment where two-way communication occurred between all stakeholders.</i>
<ul style="list-style-type: none"> The student presented risk management strategies options, insights and impacts from the cybersecurity review to the Information Technology department staff at CBSA and the related potential risk impacts on the workplace. 		<ul style="list-style-type: none"> <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>
<ul style="list-style-type: none"> The student communicated review outcomes and cybersecurity risk management strategies required as per the Action Plan. 		<p><i>The student outlined all the actions in the Action Plan they developed, including:</i></p> <ul style="list-style-type: none"> <i>the name of each task, why it is required</i> <i>the responsibility assigned to each task</i> <i>the timeline for each task</i> <i>the resources for each task.</i>
<ul style="list-style-type: none"> The student updated the cybersecurity documentation if updates were agreed upon during the consultation session. 		<p><i>The student must update any of the following documents if an agreement is reached during the consultation on any appropriate improvements:</i></p> <ul style="list-style-type: none"> <i>Cybersecurity Threat Risk Assessment Template</i> <i>Action Plan Template.</i>

Assessment checklist:

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

1	Rola Play	<input type="checkbox"/>
2	Updated Documents	<input type="checkbox"/>



Congratulations you have reached the end of Assessment 4!

© 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.