



BSBXCS403

Contribute to cyber security threat assessments

Assessment 4 of 4

Project



Assessment Instructions

Task overview

This assessment task is divided into three (3) tasks. 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 Email Template



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 purpose of this assessment, you will play the role of Tan Yamamoto (Software Developer in the IT team at Complete Business Solutions Australia CBSA).

You have been tasked by Con Kafatos, head of IT, to update documentation based on consultation feedback received. Read Con's Email below:



To: Tan Yamamoto
From: Con Kafatos (con.kafatos@cbsa.com.au)
Date/time: Monday 11:46 a.m.
Subject: Update Cybersecurity Documentation

Good morning Tan,

Thanks for conducting the stakeholder consultation session the other day.

Based on the consultation feedback received, I want you to update the following documentation to finalise them:

- Cybersecurity Threat Risk Assessment Template
- Action Plan Template

Please use a different font colour or track changes so I can clearly see what you have updated in each document.

Kind Regards,

Con Kafatos

Information Technology Manager

300 Fictional Way, Sydney, NSW 2000

Phone: 1800 111 222

www.cbsa.com.au



Task 1

Update the following documentation based on consultation feedback received in the previous assessment task:

- Cybersecurity Threat Risk Assessment Template
- Action Plan Template

As per the email from Con, you must make sure you use a different font colour or track changes so that the changes you have made are clearly identifiable.

Save and submit your updated documents using the following naming conventions:

- <Student Number> Cybersecurity Threat Risk Assessment – UPDATED
- <Student Number> Action Plan - UPDATED

Assessor instructions: The purpose of this task is to assess the student's ability to assist in integrating feedback to finalise threat assessment.

The documents must be updated based on improvements provided during the consultation session.

Updates must be easily determinable using a different colour font or track changes.

Case Study

You have been tasked by Con Kafatos, head of IT, to develop a Cybersecurity Security Audit Checklist using the template supplied. Read Con's Email below:



To: Tan Yamamoto
From: Con Kafatos (con.kafatos@cbsa.com.au)
Date/time: Tuesday 8:05 a.m.
Subject: Develop a Cybersecurity Security Audit Checklist
Attachment: Cybersecurity Security Audit Checklist Template.docx

Good morning Tan,

Thanks for finalising the cybersecurity documentation based on the consultation feedback received.

To assist the IT department in its cybersecurity audit processes, I would like you to develop a Cybersecurity Security Audit Checklist to be used for an upcoming audit.

Please use the template attached to this email.

Kind Regards,

Con Kafatos

Information Technology Manager

300 Fictional Way, Sydney, NSW 2000

Phone: 1800 111 222

www.cbsa.com.au



Task 2

Develop a Cybersecurity Security Audit Checklist using the template supplied, ensuring the following:

- Document CBSA's existing cybersecurity policies and procedures.
- Document eight audit questions that can be used to evaluate the effectiveness of the cybersecurity protection measures implemented by CBSA.
- Document a benchmark that each question must meet. This can be a simple yes/no benchmark, a number that must be met [zero issues, for example], or another benchmark that can determine the success or not of each question.

Assessor instructions: The purpose of this task is to assess the student's ability to:

- identify relevant organisational data security/protection policies and procedures
- contribute to organisation-wide cyber security audits.

The student:

- Document CBSA's existing cybersecurity policies and procedures. This must be the Information Technology Policy and Procedures at a minimum, as this is the only data security/protection that CBSA currently has.

The student may list other policies that are related to cybersecurity operations, such as Risk Management Policy and Procedures or Privacy Policy, but these are not specifically required for the purpose of this task.

- Document eight audit questions related to cybersecurity with appropriate benchmarks for each. Questions will vary, but they must be related to cybersecurity and allow an outcome to be determined. Each question must have an appropriate benchmark that is measurable and must be consistent with the examples in the sample Cybersecurity Security Audit Checklist provided.

A sample answer is provided below.

CYBERSECURITY SECURITY AUDIT CHECKLIST			
Auditor			
Audit Date			
CBSA Cybersecurity Policies and Procedures			
<i>IM005 – Information Technology Policy and Procedures</i>			
Audit Question	Benchmark	Compliant (Y/N)	Notes
1. <i>Do backups of the organisation's data occur regularly?</i>	<i>Yes/No</i>		
2. <i>Is anti-malware installed and up to date on all organisation computers?</i>	<i>Yes/No</i>		
3. <i>Does regular cybersecurity awareness training occur?</i>	<i>Yes/No</i>		
4. <i>How many security breaches occurred within the last three months?</i>	<i><= 0</i>		
5. <i>Is there a disaster recovery plan?</i>	<i>Yes/No</i>		
6. <i>Are all devices protected from the internet by a firewall?</i>	<i>Yes/No</i>		
7. <i>Do all users have a strong password?</i>	<i>Yes/No</i>		
8. <i>Are all operating systems and applications up to date?</i>	<i>Yes/No</i>		

Case Study

You have been tasked by Con Kafatos, head of IT, to develop an email using the CBSA Email Template. Read Con's Email below:



To: Tan Yamamoto
From: Con Kafatos (con.kafatos@cbsa.com.au)
Date/time: Wednesday 10:00 a.m.
Subject: Distribute Cybersecurity Documentation

Good morning Tan,

Thank you for developing the Cybersecurity Security Audit Checklist.

Please distribute the following finalised documentation to all members of CBSA's Information Technology department for review:

- Cybersecurity Threat Risk Assessment Template
- Action Plan Template
- Cybersecurity Security Audit Checklist

Kind Regards,

Con Kafatos

Information Technology Manager

300 Fictional Way, Sydney, NSW 2000

Phone: 1800 111 222

www.cbsa.com.au



Task 3

Develop an email using the CBSA Email Template provided in your resources, including the following:

- Specify the people who will receive the email.
- Specify that the email is being sent by yourself.
- Specify the date and time that the email was developed.
- Specify the subject line.
- Specify the documents that will be attached to the email.
- Specify an opening, body and closing section of the email.

Save and submit your email using the following naming convention:

<Student Number> Email

Assessor instructions: The purpose of this task is to assess the student's ability to distribute final threat assessment according to organisational policies and procedures.

The student must develop an email using the correct template that:

- *specifies that it is being delivered to Con Kafatos, Sally Fischer and Tina Yates*
- *specifies that the student is sending it*
- *specifies the date and time it was sent*
- *specifies a relevant subject line, for example, Cybersecurity Documentation for Review or similar*
- *specifies that the following documents are attached:*
 - *Cybersecurity Threat Risk Assessment Template*
 - *Action Plan Template*
 - *Cybersecurity Security Audit Checklist*
- *contains a body relevant to the task instructions.*

A sample email has been provided.

To:	<i>Con Kafatos, Sally Fischer, Tina Yates</i>
From:	<i>Tan Yamamoto (tan.yamamoto@cbsa.com.au)</i>
CC:	
BCC:	
Date/time:	<i>XX/XX20XX X:X a.m./p.m.</i>
Subject:	<i>Cybersecurity Documentation for Review</i>
Attachments:	<i>Cybersecurity Threat Risk Assessment Template.docx, Action Plan Template.docx, Cybersecurity Security Audit Checklist.docx</i>

Hello Con, Sally, and Tina,

I have attached the following cybersecurity documents that I have developed for your review and feedback:

- *Cybersecurity Threat Risk Assessment Template*
- *Action Plan Template*
- *Cybersecurity Security Audit Checklist*


Please let me know if you have any queries about this documentation.

Kind Regards,

Tan Yamamoto

Systems Administrator

300 Fictional Way, Sydney, NSW 2000
Phone: 1800 111 222
www.cbsa.com.au



Assessment checklist:

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

1	Task 1 <ul style="list-style-type: none">• Updated Cybersecurity Threat Risk Assessment Template• Updated Action Plan Template	<input type="checkbox"/> <input type="checkbox"/>
2	Task 2 <ul style="list-style-type: none">▪ Cybersecurity Audit Checklist	<input type="checkbox"/>
3	Taks 3 <ul style="list-style-type: none">▪ Email	<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.