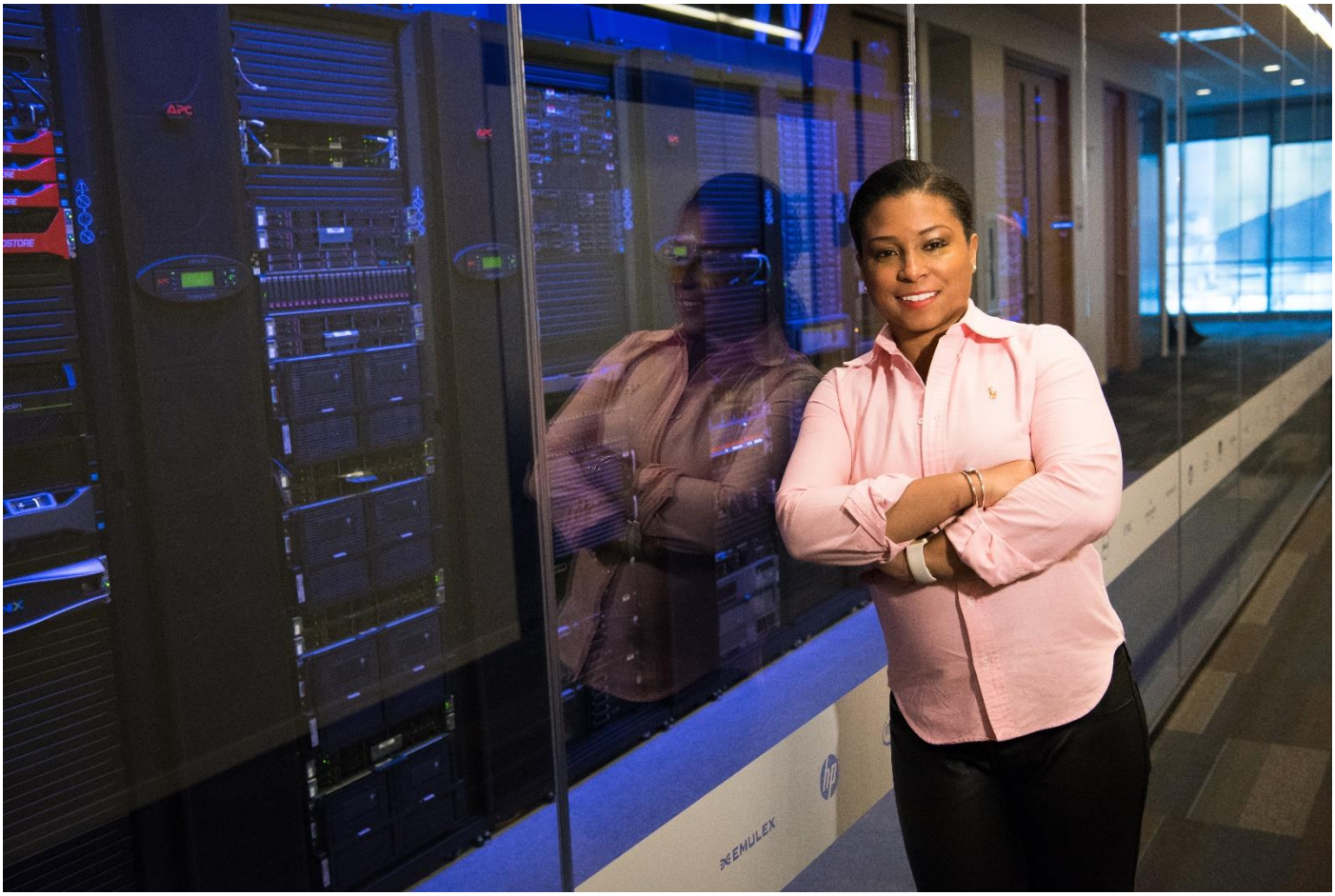


BSBXCS404

Contribute to cyber security risk management

Assessment 3 of 5

Project

ASSESSOR GUIDE

Version 1

Assessment Instructions

Task overview

This assessment task is divided into three (3) tasks. 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
- Organisational Chart
- CBSA Information Technology Policy & Procedures
- CBSA Risk Management Policy and Procedures
- CBSA Communication Policy & 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.

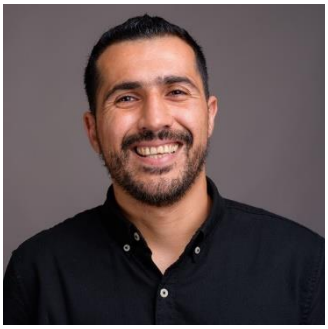
Refer to the Student Handbook or contact your Trainer for further information.

Please consider the environment before printing this assessment.

Case Study

For the purposes of this assessment, you will play the role of Tan Yamamoto (Software Developer).

You have been tasked by your manager, Con Kafatos, to undertake research using various Australian government sources of current cybersecurity risks and threats. Read Con's email below:



To:	Tan Yamamoto (tan.yamamoto@cbsa.com.au)
From:	Con Kafatos (con.kafatos@cbsa.com.au)
Date/time:	Wednesday 11:03 a.m.
Subject:	Documenting and Assessing Cybersecurity Threats and Risks
Attachments:	Cybersecurity Threat Register Template.docx, Cybersecurity Threat Event Register Template.docx

Good morning Tan,

As agreed in the consultation session, I want you to take up a new project researching possible cybersecurity risks and threats that CBSA might face in its day-to-day operations.

I have attached two templates for you to use.

Please document all the threats you find using the attached Cybersecurity Threat Register Template. Once you have done this, please determine the risks of these threats, documenting these in the attached Cybersecurity Threat Event Register Template.

Please contact me if you have any questions.

Kind Regards,

Con Kafatos

Information Technology Manager

300 Fictional Way, Sydney, NSW 2000

Phone: 1800 111 222

www.cbsa.com.au

Task 1

A. Document at least five (5) cybersecurity threats that may impact CBSA's day-to-day operations using the Cybersecurity Threat Register Template provided. For each threat, you must:
   - assign a unique cybersecurity threat ID number
   - provide a descriptive name for the cybersecurity threat
   - provide a brief description of the cybersecurity threat.

B. Document one (1) threat event for each of the five (5) threats you identified in the Cybersecurity Threat Register Template using the Threat Event Register template provided. For each threat event, you must:
   - assign a unique cybersecurity threat event ID number
   - provide a descriptive name for the cybersecurity threat event

- provide a brief description of the cybersecurity threat event
- specify the cybersecurity threat ID number from the Cybersecurity Threat Register Template that is relevant to the cybersecurity threat event.

Assessor instructions: The purpose of this task is to assess the student's ability to review and document the latest cyber security threats and trends impacting an organisation. More specifically:

- The student must complete the cybersecurity threat register as per the sample provided. It should include numbers only or a combination of numbers and letters to identify each threat uniquely. It should also contain a relevant name and a brief description of each identified threat.
- The student needs to provide five threats in total. They must be relevant to CBSA operations. In addition to those provided in the table, some examples are:
    - Insider threat: an employee or contractor within the organisation who undertakes sabotage or malicious attacks on the organisation's systems, networks, or data.
    - Internet of Things (IoT): where security gaps in using IoT software and devices are exploited.
    - Ransomware: malware that encrypts a victim's access to files or their device until a sum of money is paid to remove this encryption.
    - Wi-Fi security vulnerabilities: where security gaps in the use of Wi-Fi within the organisation are exploited.
    - Note that other cybersecurity threat names exist that are not listed above or which might have variations of their names. For example, virus or trojan horse instead of malware. Accept name variations of the list above or other cybersecurity threats not listed. Sample responses have been provided in the table.
- The student must complete the cybersecurity threat event register as per the sample provided. It should include numbers only or a combination of numbers and letters to identify each threat uniquely. It should also contain a relevant name and a brief description of each identified threat.
- The cybersecurity threat ID must be correctly associated with its Threat Event ID between the cybersecurity threat register template and the cybersecurity threat event register template, as shown in the sample.

Sample answers are provided below:

- ***Cybersecurity Threat Register Template***

ID	Threat	Description
T1	*Distributed Denial of Service (DDoS)*	*A malicious attack designed to disrupt the normal traffic of an organisation's network or website by trying to overwhelm it with significant Internet traffic.*
T2	*Inadequate patch management*	*Information technology staff aren't implementing a scheduled patch update of software when improvements to this software have been made, leading to potential security gaps.*
T3	*Malware*	*Malicious software designed to harm or infect devices, services, or networks.*
T4	*Man-in-the-middle (MitM)*	*An attack designed to intercept communications between two parties by positioning themselves somewhere between the two parties' communication methods.*

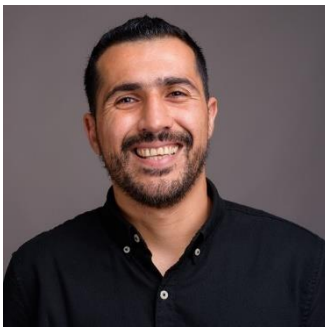
T5	*Phishing*	*A malicious attack where targets are contacted by email, text or phone by the attacker pretending to be a legitimate organisation so that they can gain personal information or gain access to organisational networks and systems.*

- ***Cybersecurity Threat Event Register Template***

Threat Event ID	Threat Event	Description	Threat ID
TE1	*Protocol attack*	*Floods the network traffic with SYN packets.*	*T1*
TE2	*Inadequate operating system security*	*Operating system doesn't have the latest security patches installed.*	*T2*
TE3	*Virus*	*Modifies a file by inserting code into the file.*	*T3*
TE4	*IP Spoofing*	*Intercept of communication by changing the IP headers of a TCP packet.*	*T4*
TE5	*Email phishing*	*An email that prompts a call to action to negate some issue that the user will face unless they click on a link in the email.*	*T5*

Case Study

You have been tasked by your manager, Con Kafatos, to undertake a risk assessment of the identified cybersecurity threats. Read Con's email below:



To:	Tan Yamamoto (tan.yamamoto@cbsa.com.au)
From:	Con Kafatos (con.kafatos@cbsa.com.au)
Date/time:	Friday 2:36 p.m.
Subject:	Cybersecurity Threats Risk Assessment
Attachment:	Cybersecurity Threat Risk Assessment Template.docx

Good afternoon Tan,

Thanks for identifying and documenting cybersecurity threats that CBSA might encounter.

Please undertake a risk assessment of these identified cybersecurity threats using the attached template, including reviewing current cyber security practices that CBSA implements (by reviewing our policies and procedures) and recommending at least one cybersecurity control measure that we can use to control each cybersecurity threat.

Kind Regards,

Con Kafatos

Information Technology Manager

300 Fictional Way, Sydney, NSW 2000

Phone: 1800 111 222

www.cbsa.com.au

Task 2

Undertake research to:

- determine recommended protection measures against all the identified cybersecurity threats in Task 1
- review the following CBSA's policies and procedures relating to IT to determine current cyber security practices using an internet browser:
    - **CBSA Information Technology Policy & Procedures**
    - **CBSA Risk Management Policy and Procedures**
    - **CBSA Communication Policy & Procedures**

Then undertake a risk assessment of each cybersecurity threat and document your assessment using the supplied Cybersecurity Threat Risk Assessment Template, ensuring that you:

- document the threat event ID number and the event name for each threat you have identified in Task 1
- use the Risk Rating Matrix in **CBSA Risk Management Policy and Procedures** to determine and document the risk rating for each threat based on the likelihood and consequence of each threat

- document [1] one risk control measure for each cybersecurity threat.

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

- review relevant critical cyber risk management strategies appropriate to the level of risk
- assist in developing suitable cyber security response options according to organisational policies and procedures
- document approved risk management strategies
- contribute to developing and implementing risk management strategies that control two different identified cyber security risks and document the response option applied to each risk.

More specifically, the student:

- Must match the threat event ID numbers they documented in the previous part.
- Must match the threat event names they documented in the previous part.
- Must assign a risk rating that is specified in the Risk Management policy and procedure ranging from very low, low, moderate, high, and critical.
- A sample table has been provided.
- Control measures will vary and will be dependent on the threats documented in the previous part. Sample control measure for each threat event has been provided.

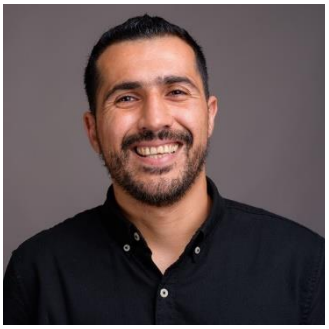
A sample answer is provided below:

- ***Cybersecurity Threat Risk Assessment Template***

Threat Event ID	Threat Event	Threat Risk Rating	Recommended Control Measure(s)
TE1	*Protocol attack*	*Moderate*	*Develop a DDoS Response Plan*
TE2	*Inadequate operating system security*	*Low*	*IT policy and procedure update*
TE3	*Virus*	*High*	*Anti-malware software*
TE4	*IP Spoofing*	*Low*	*Network monitoring software*
TE5	*Email phishing*	*Moderate*	*Staff training on email phishing*

Case Study

You have been tasked by your manager, Con Kafatos, to develop an Action Plan using the Action Plan Template supplied. Read Con's email below:



To:	Tan Yamamoto (tan.yamamoto@cbsa.com.au)
From:	Con Kafatos (con.kafatos@cbsa.com.au)
Date/time:	Tuesday 10:10 a.m.
Subject:	Develop an action plan
Attachment:	Action Plan Template.docx

Good morning Tan,

Thanks for completing the risk assessment of possible cybersecurity risks.

Please develop an action plan to implement the recommended control measures in a coordinated manner. Use the template I have attached to this email, and I will review it.

Please ensure that you include the following tasks in the action plan in addition to the actions for your recommended control measures:

- communicating cybersecurity risk management strategies
- establishing a feedback process on cybersecurity risks
- monitoring and evaluating the effectiveness of cybersecurity risk management strategies.

Kind Regards,

Con Kafatos

Information Technology Manager

300 Fictional Way, Sydney, NSW 2000

Phone: 1800 111 222

www.cbsa.com.au

Task 3

Using a word processor, develop an Action Plan using the Action Plan Template supplied, ensuring that you:

- Document actions that need to be implemented to control each cybersecurity threat.
- Document who will be responsible for each task (you can assign yourself or any staff member in the **CBSA Organisational Chart** as appropriate), a timeline for each task's completion and the resources needed for each (specific people, CBSA departments, specific software, etc.).
- As per the email from Con, you must make sure you have three further actions: communicating strategies, establishing feedback processes, and monitoring/evaluating the effectiveness of risk management strategies. You will undertake these three actions in later assessment tasks.

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

- assist in developing suitable cyber security response options according to organisational policies and procedures
- document approved risk management strategies
- contribute to developing and implementing risk management strategies that control two different identified cyber security risks and document the response option applied to each risk.

More specifically:

- The student must cover all the control measures identified in the previous tasks and include action tasks for:
    - communicating cybersecurity risk management strategies
    - establishing a feedback process on cybersecurity risks
    - monitoring and evaluating the effectiveness of cybersecurity risk management strategies.
- Responsibility: it must be either the student or an appropriate staff member from the CBSA organisation chart.
- The student must provide a date in the future for each action as per the sample.
- The student must provided a specific resource, if applicable, for each action as per the sample. For example, specific people, CBSA departments, specific software, etc.

A sample answer is provided below:

- ***Action Plan Template***

Action	Responsibility	Timeline	Resources
Develop a DDoS Response Plan	*Tina Yates*	*XX/XX/20XX*	
Update IT policy and procedures	*Tan Yamamoto*	*XX/XX/20XX*	*IT policy and procedures*
Install anti-malware software	*Tina Yates*	*XX/XX/20XX*	*Anti-malware software*
Install network monitoring software	*Tina Yates*	*XX/XX/20XX*	*Network monitoring software*
Staff training on email phishing and password update	*Tan Yamamoto*	*XX/XX/20XX*	*Training room, existing policies*
Communicating cybersecurity risk management strategies	*Tan Yamamoto*	*XX/XX/20XX*	
Establishing a feedback process on cybersecurity risks	*Tan Yamamoto*	*XX/XX/20XX*	
Monitoring and evaluating the effectiveness of cybersecurity risk management strategies	*Tan Yamamoto*	*XX/XX/20XX*	

Assessment checklist:

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

1	Task 1 • Cybersecurity Threat Register • Cybersecurity Threat Event Register	☐ ☐
2	Task 2 - Cybersecurity Threat Risk Assessment	☐
3	Task 3 - Action Plan	☐

Congratulations you have reached the end of Assessment 3!