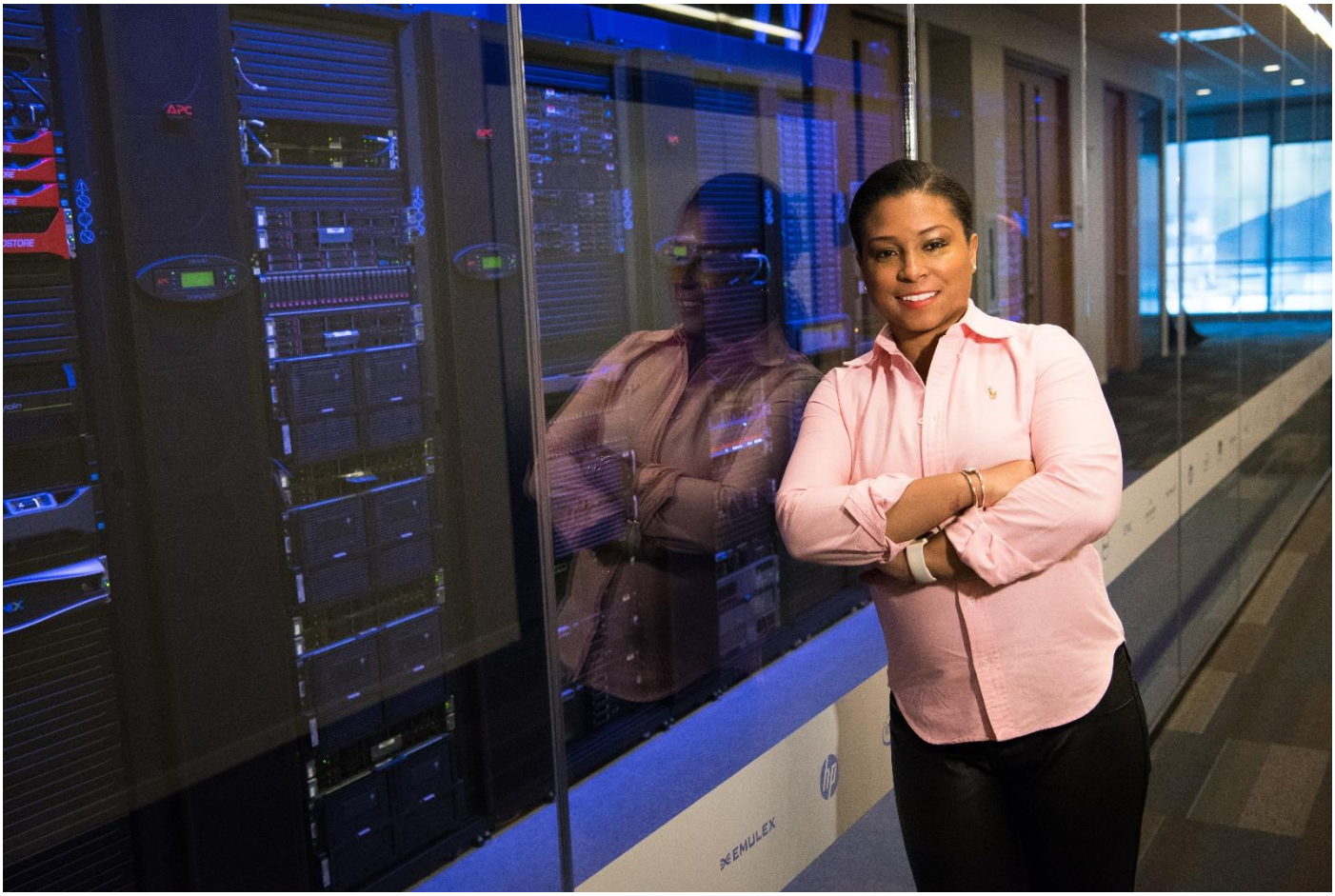


BSBXCS404

Contribute to cyber security risk management

Assessment 5 of 5

Project

ASSESSOR GUIDE

Version 1

Assessment Instructions

Task overview

This assessment task is divided into four (4) 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
- 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.

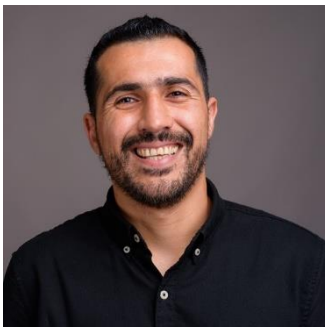
Refer to the Student Handbook or contact your Trainer for further information.

Please consider the environment before printing this assessment.

Case Study

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

You have been tasked by your manager, Con Kafatos, to communicate the approved cybersecurity risk management strategies and a feedback process that employees can use if they notice a new cybersecurity threat. Read Con's email below:



To:	Tan Yamamoto (tan.yamamoto@cbsa.com.au)
From:	Con Kafatos (con.kafatos@cbsa.com.au)
Date/time:	Monday 8:59 a.m.
Subject:	Cybersecurity Risk Management Strategies

Good morning Tan,

Thanks for conducting the stakeholder consultation session the other day.

Based on the consultation session outcomes, please communicate these to all CBSA employees by email, including attaching the following documents that you have developed:

- Cybersecurity Threat Risk Assessment Template
- Action Plan Template.

I also want you to develop and communicate a feedback process that employees can use to warn of potential cybersecurity risks that they come across in their daily work tasks in the email. The feedback process must comply with IM003 Communication Policy and Procedures, so please ensure that you mention this in the feedback process.

Kind Regards,

Con Kafatos

Information Technology Manager

300 Fictional Way, Sydney, NSW 2000

Phone: 1800 111 222

www.cbsa.com.au

Task 1

Using a word processor, develop an email using the **Email Template** provided, including:

- Specifying the people that the email will be sent to. Note you can use the 'All CBSA Employees' email group for the purpose of this task.
- Specifying that the email is being sent by yourself.
- Specifying the date and time that the email was developed.
- Specifying the subject line.

- Specifying the documents that will be attached to the email.
- Specifying an opening, body and closing section of the email, including:
- The purpose of the attached documents.
- The feedback process you want them to use if they identify a cybersecurity threat in their day-to-day work. Note that you must specify that they follow **CBSA Communication Policy and Procedures** when providing feedback.

[Approximate word count: 100 – 150 words]

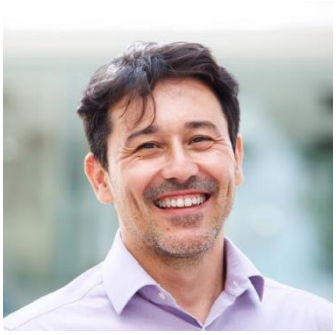
Assessor instructions: *The purpose of this task is to assess the student's ability to:*

- *communicate approved risk management strategies to stakeholders*
- assist in establishing feedback processes for new risks

More specifically:

The student must develop an email using the correct template that:
- specifies that it is being delivered to all staff members
- specifies that the student is sending it
- specifies the date and time it was sent
- specifies a relevant subject line
- specifies that the following documents are attached:
  - Cybersecurity Threat Risk Assessment Template
  - Action Plan Template.
- contains a body relevant to the task instructions, including a brief summary of what the documents cover and the cybersecurity feedback process.

A sample email is provided below.



To:	*All CBSA Employees*
From:	*Tan Yamamoto (tan.yamamoto@cbsa.com.au)*
Date/time:	*XX/XX20XX XX:XX a.m./p.m.*
Subject:	*Cybersecurity Risk Management Strategies and Feedback Process*
Attachment:	*Cybersecurity Threat Risk Assessment Template.docx, Action Plan Template.docx, Cybersecurity Security Audit Checklist.docx*

Hello all,

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

- *Cybersecurity Threat Risk Assessment Template*
- *Action Plan Template.*

These documents state the cybersecurity threats and risks you must know and the action plan designed to mitigate these.

Also, I have developed a cybersecurity feedback process as follows:

- *If you notice a new cybersecurity threat, please send an email detailing this threat to me or if this is not possible, call me as soon as you are able. Please ensure that you follow IM003 Communication Policy and Procedures at all times when providing feedback.*

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

Kind Regards,

Tan Yamamoto

Systems Administrator

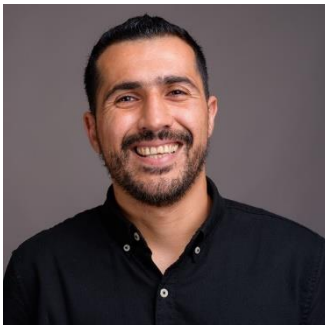
300 Fictional Way, Sydney, NSW 2000

Phone: 1800 111 222

www.cbsa.com.au

Case Study

You have been tasked by your manager, Con Kafatos, to develop benchmarks for the risk management strategies you have developed so that they can be monitored and evaluated against. Read Con's email below:



To:	Tan Yamamoto (tan.yamamoto@cbsa.com.au)
From:	Con Kafatos (con.kafatos@cbsa.com.au)
Date/time:	Wednesday 4:16 p.m.
Subject:	Documenting Risk Management Strategy Benchmarks
Attachment:	Risk Management Strategy Benchmarks Template.docx

Good afternoon Tan,

I want you to develop benchmarks for each of the control measures for the five cybersecurity threat events you have determined so that the effectiveness of the control measures for each can be monitored and evaluated.

I have attached the Risk Management Strategy Benchmarks Template that I want you to use for this task.

Kind Regards,

Con Kafatos

Information Technology Manager

300 Fictional Way, Sydney, NSW 2000

Phone: 1800 111 222

www.cbsa.com.au

Task 2

Document the Risk Management Strategy Benchmarks Template, including:

- Specifying the threat event ID number for each threat event you have identified in a previous assessment task [Assessment 3: Task 1].
- Specifying the threat event name for each threat event you have identified in a previous assessment task [Assessment 3: Task 1].
- Specifying the control measure[s] for each threat event you have identified in a previous assessment task [Assessment 3: Task 2].
- Specifying a relevant benchmark that can be used to monitor and evaluate the effectiveness of each control measure. This benchmark must be measurable. For example, it relates to a yes/no answer such as 'Did this control measure prevent the cybersecurity threat event?' or a numerical answer such as 'The number of occurrences of this threat event was less than three' or similar.

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

- identify risk management strategy benchmarks
- help evaluate the effectiveness of each risk management strategy.

More specifically, the student:

- Must match the threat event ID numbers they documented in the previous assessment task [Assessment 3: Task 1].
- Must match the threat event names they documented in the previous assessment task [[Assessment 3: Task 1].
- Must match the risk control measures they documented in the previous assessment task [Assessment 3: Task 2].
- Each benchmark provided must be measurable and suitable for the threat event control measures.

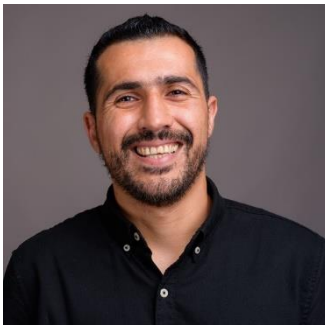
A sample risk management strategy benchmarks template is provided below.

- ***Risk Management Strategy Benchmarks Template***

Threat Event ID	Threat Event	Control Measure(s)	Benchmark
TE1	*Protocol attack*	*Develop a DDoS Response Plan*	*Does a plan exist? Yes/No*
TE2	*Inadequate operating system security*	*IT policy and procedure update*	*Has the policy been updated? Yes/No*
TE3	*Virus*	*Anti-malware software*	*Has anti-malware software been installed? Yes/No*
TE4	*IP Spoofing*	*Network monitoring software*	*Has network monitoring software been installed? Yes/No*
TE5	*Email phishing*	*Staff training on email phishing*	*Has staff training on email phishing been completed? Yes/No*

Case Study

You have been tasked by your manager, Con Kafatos, to monitor cybersecurity risk management strategies' effectiveness and address any non-compliances. Read Con's email below:



To: Tan Yamamoto (tan.yamamoto@cbsa.com.au)

From: Con Kafatos (con.kafatos@cbsa.com.au)

Date/time: Friday 12:39 p.m.

Subject: Documenting Risk Management Strategy Benchmarks

Attachment: Risk Management Strategy Benchmarks Template.docx

Good afternoon Tan,

Now that the cybersecurity risk management strategies have been in place for some time, I want you to monitor these and evaluate the effectiveness of these strategies using the attached template.

If any strategies have been ineffective or if non-compliances have occurred, please document a recommended incident response using the attached template.

Kind Regards,

Con Kafatos

Information Technology Manager

300 Fictional Way, Sydney, NSW 2000

Phone: 1800 111 222

www.cbsa.com.au

Task 3

To simulate the risk management monitoring and evaluation process, the following information must be substituted against the risk strategies you have implemented to control (the control measures) each of the five threat events you documented in the Action Plan you previously developed in sequential order. For example, the non-compliance for the third threat event must relate to the action(s) you documented in the Action Plan concerning the third event threat.

Assume that the following non-compliances have occurred during the monitoring process and have been brought to your attention:

- a cybersecurity incident relevant to the second of your five threat events
- a cybersecurity incident relevant to the third of your five threat events.

Based on this information, and using a word processor, document the **Incident Response Plan Template**, including:

- Specifying the threat event ID number for each of the five threat events you have identified in a previous assessment task (Assessment 3: Task 1).

- Specifying the threat event name for each of the five threat events you have identified in a previous assessment task (Assessment 3: Task 1).
- Specifying the control measure(s) for each threat event you have identified in a previous assessment task (Assessment 3: Task 2).
- Specifying the benchmark for each threat event control measure that you developed in the previous part.
- Specifying whether the control measures have been effective based on the benchmark outcomes. This should be 'yes' or 'no'. Based on the information provided at the start of this task, you can assume that any compliant threat events have been effective, so place a 'yes' for those threat events and a 'no' for those which have been non-compliant.

For those threat events that have been evaluated as non-compliant, you must develop a recommended incident response, including the following:

- Specifying the threat event name for those threat events that are non-compliant.
- Specifying the control measure(s) for each threat event that were implemented.
- Specifying the cybersecurity incident that occurred which caused the non-compliance. You must specify any incident that could happen, appropriate and relevant to the threat event and the control measures implemented. For example, an incident of an employee adverting their password to other people after they had received cybersecurity awareness training on this subject or an employee opening an infected email (malware) that causes the business network to become infected.
- Specifying a recommended response for each incident. This must be relevant to the threat event, existing control measures, and the incident that occurred. For example, modifying a specific policy and procedure, cybersecurity awareness training for employees, implementing a new tool to minimise the threat, escalating to the IT Manager for review and action, etc.
- Note that at least one recommendation must involve updating the action plan or other document you have developed or an existing CBSA policy and procedure. You will complete this task in the next part..

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

- monitor cyber security risk using risk management strategies
- help determine compliance of cybersecurity risk mitigation strategies
- address any cybersecurity risk mitigation strategy non-compliances
- evaluation effectiveness of each implemented risk management strategy.

More specifically, the student:

- Must match the threat event ID numbers they documented in the previous assessment task (Assessment 3: Task 1).
- Must match the threat event names they documented in the previous assessment task (Assessment 3: Task 1).
- Must match the risk control measures they documented in the previous assessment task (Assessment 3: Task 2).
- Must match the benchmarks they documented in the previous assessment part.
- Document whether each of the control measures was effective or not This must be yes for the first, fourth and fifth threat events and no for the second and third threat events.
- Must document the threat event names for the second and third threat event from the Monitoring and Evaluation section.

- Must document the control measures for the second and third threat event from the Monitoring and Evaluation section.
- Must document the relevant to the threat event and the control measures.
- Must document the recommended response in the Recommended Response column of the Incident Response section Answers will vary. Must be relevant to the threat event, the existing control measures and the incident that occurred.

A sample answer is provided below:

- ***Incident Response Plan Template***

Monitoring and Evaluation				
Threat Event ID	**Threat Event**	**Control Measure(s)**	**Benchmark**	**Effective (Y/N)**
TE1	*Protocol attack*	*Develop a DDoS Response Plan*	*Does the plan exist? Yes/No*	*Yes*
TE2	*Inadequate operating system security*	*IT policy and procedure update*	*Has the policy been updated? Yes/No*	*No*
TE3	*Virus*	*Anti-malware software*	*Has anti-malware software been installed? Yes/No*	*No*
TE4	*IP Spoofing*	*Network monitoring software*	*Has network monitoring software been installed? Yes/No*	*Yes*
TE5	*Email phishing*	*Staff training on email phishing*	*Has staff training on email phishing been completed? Yes/No*	*Yes*

Incident Response			
Threat Event	**Control Measures**	**Incident**	**Response Recommendations**
Inadequate operating system security	*IT policy and procedure update*	*Cybersecurity attack targeting security issue in the operating system which would not have occurred if the operating system had been patched*	*Update policy to clarify that operating system patching should occur as soon as a patch is available.*
Virus	*Anti-malware software*	*Installed anti-malware software did not identify and protect against virus attack*	*Evaluate various anti-malware software to determine the best solution that CBSA should implement*

Case Study

You have been tasked by your manager, Con Kafatos, to update the risk management strategies based on the results of your evaluation. Read Con's email below:

To: Tan Yamamoto (tan.yamamoto@cbsa.com.au)

From: Con Kafatos (con.kafatos@cbsa.com.au)

Date/time: Thursday 8:59 a.m.

Subject: Implementing Incident Response Recommendations

Good morning Tan,

Thanks for completing the evaluation of the risk management strategies.

Based on the incident response plan you developed, please proceed with any documentation updated tasks to implement your recommendation(s).

Kind Regards,

Con Kafatos

Information Technology Manager

300 Fictional Way, Sydney, NSW 2000

Phone: 1800 111 222

www.cbsa.com.au

Task 4

Using a word processor, update the specified documentation from your recommendations in the Incident Response Plan developed in the previous part to address the cybersecurity risk management strategy non-compliance(s).

Submit your updated documentation using the following naming conventions:

<Student Number> Updated Documentation

Assessor instructions: The purpose of this task is to assess the student's ability to update risk management strategies with new information as required.

Answers will vary. Appropriate documentation must be updated based on the recommendations in their Incident Response Plan developed in the previous assessment task.

This may include their Action Plan, CBSA Information Technology Policy & Procedures, or another document as appropriate. Accept any reasonable updates that address the documented non-compliance. For example, updating the Action Plan to implement a new action task for employee training on cybersecurity awareness if this was the cause of the non-compliance.

Assessment checklist:

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

1	Task 1 - Email	☐
2	Task 2 - Risk Management Strategy Benchmarks	☐
3	Task 3 - Incident Response Plan	☐
4	Task 4 – Updated Documentation	☐

Congratulations you have reached the end of Assessment 5!