# Case Study Assessment

## Criteria

### Unit code, name and release number

ICTICT424 - Address cyber security requirements (1)

### Qualification/Course code, name and release number

ICT40118 - Certificate IV in Information Technology (1)

## Student details

### Student number

### Student name

## Assessment Declaration

* This assessment is my original work and no part of it has been copied from any other source except where due acknowledgement is made.
* No part of this assessment has been written for me by any other person except where such collaboration has been authorised by the assessor concerned.
* I understand that plagiarism is the presentation of the work, idea or creation of another person as though it is your own. Plagiarism occurs when the origin of the material used is not appropriately cited. No part of this assessment is plagiarised.

### Student signature and Date

Version: *201911127*

Date created: *10 August 2018*

Date modified: *05/03/2021*

For queries, please contact:

*Technology and Business Services SkillsPoint*

*Ultimo*

© 2019 TAFE NSW, Sydney  
RTO Provider Number 90003 | CRICOS Provider Code: 00591E

This assessment can be found in the: [Learning Bank](https://share.tafensw.edu.au/share/access/searching.do?doc=%3Cxml%2F%3E&in=P7ac4831b-430a-4b8d-8b56-f7b32ed5b9cf&q=&type=standard&sort=rank&dr=AFTER)

The contents in this document is copyright © TAFE NSW 2019, and should not be reproduced without the permission of the TAFE NSW. Information contained in this document is correct at time of printing: 5 March 2021. For current information please refer to our website or your teacher as appropriate.

## Assessment instructions

Table 1 Assessment instructions

| Assessment details | Instructions |
| --- | --- |
| **Assessment overview** | The objective of this assessment is to assess your knowledge and performance as would be required to determine the cyber security requirements of an organisation and use a range of resources to protect valuable assets. |
| **Assessment Event number** | 2 of 2 |
| **Instructions for this assessment** | This is a case study assessment and it will be assessing you on your knowledge and performance of skills required by the unit.  This assessment is in 5 parts:   1. Case study scenario 2. Investigation and consultation (includes role-plays) 3. Solution implementation 4. Post Implementation and consultation (includes role-plays) 5. Assessment feedback |
| **Submission instructions** | On completion of this assessment, you are required to upload it or hand it to your trainer for marking.  Ensure you have written your name at the bottom of each page of this assessment.  It is important that you keep a copy of all electronic and hardcopy assessments submitted to TAFE and complete the assessment declaration when submitting the assessment. |
| **What do I need to do to achieve a satisfactory result?** | To achieve a satisfactory result for this assessment all questions must be answered correctly. |
| **What do I need to provide?** | Computer with internet access  Office Software (e.g. MS Office with Word and Excel or similar)  Optional:   * Smart mobile device such as a phone or tablet   + iOS iPad or iPhone   + Android phone or tablet * Mobile internet or wireless network access   If a student doesn’t have a smart phone or tablet, please talk to your teacher about using a device from their inventory. |
| **What the assessor will provide?** | Computer with internet access  Access to the Learning Management System (LMS)  TAFE email account access  Documents:   * ICTICT424\_SR\_1of2 * ICTICT424\_SR\_2of2   Optional if students require them:   * Smart devices capable of using MDM e.g.   + Smart phone (either iOS or Android)   + Tablets (either iOS or Android)   + Unproxied Internet access |
| **Due date and time allowed** | These tasks can be completed unsupervised except the meetings for the following questions:   * Part 2 Q1 (a) * Part 2 Q7 * Part 4 Q1 * Part 4 Q4   Indicative time to complete:  Part 2: 1 hr  Part 3: 1 hr  Part 4: 1 hr  **Total: 3 hrs** |
| **Assessment feedback, review or appeals** | Appeals are addressed in accordance with Every Students Guide to Assessment. |

## Specific task instructions

The instructions and the criteria in the case studies below will be used by the assessor to determine whether the student has satisfactorily completed each Case Study Scenario. Use these instructions and criteria to ensure you demonstrate the required knowledge.

## Part 1: Case Study Scenario

To complete this part of the assessment, the student will be required to read the Case Study Scenario below.

Once the student has read the information, they are required to complete their written responses to questions in parts 2 to 4 in the spaces provided in this document. Please ensure they take note of the volume of response requirement where indicated.

Once completed the student will need to submit this assessment to the assessor for marking.

**Case Study Scenario:**

Smith & Jones have recently added wireless access points to the network as part of their move and started equiping staff with laptops, mobiles and tablets so they can move between the office, clients and courts as required.

Their website and public facing information is located on another network, but their clients and staff are also requesting the ability to connect their devices to the wireless network to access the internet. Staff would like to access the network resources from their laptops, mobiles and tablets.

The IT Manager (Mrs Janet Twomey) has asked your organisation to assist Smith & Jones with their cybersecurity analysis as they are considereing the effects that the wireless network has had to their security posture and what this means with staff being issued smart phones, laptops and tablets.

Recently one staff member lost their mobile and there were concerns of the data and access that this device had on it. They have not been able to find the device, but their largest concern is to ensure the data on the devices is unavailabe to the person who potentially has it if this happens in the future.

They are also interested in ensuring that staff mobiles and tablets are audited for unauthorised applications and blocking installation or useage of apps if possible.

You have been employed as part of the team to complete the task of determining the risks that these devices add to the network, advise a solution and perform some tests to ensure your solution minimises risks to the organisation.

## Part 2: Research and Investigation

To complete this part of the assessment, you will be required to analyse and research information based on the scenario in *ICTICT424\_SR\_1of2*.

1. You must identify and document valuable assets to create a register for the organisation.
   1. **Role-play to analyse the assets of the organisation.** You have been requested to identify the assets of the organisation and the risk appetite of the organisation. To do so you need to ask the organisation representative (one of your fellow students) some questions and confirm the assets (as per ICTICT424\_SR\_1of2) you are aware of and ensure you are able to identify the valuable assets of the organisation.  
        
      Your client does not understand technical terminology very well so you will need to make sure you use language and communication skills that are appropriate for your client and context.

Your assessor will use the observation checklist below to record the outcomes of this assessment. You should use the marking criteria in the checklist as a guide for what you will be assessed on.

#### Role-play

This task should take approximately 5 to 10 minutes.

Use this Checklist to understand what skills you need to demonstrate in the practical task demonstration. The Checklist lists the assessment criteria used to determine whether you have successfully completed this assessment event. All the criteria must be met. Your demonstration will be used as part of the overall evidence requirements of the unit. The assessor may ask questions while the demonstration is taking place or if appropriate directly after the task/activity has been completed.

Table – Meeting checklist

| Task # | Task/Activity Performed | S | U/S | Assessor Comments (Describe the student’s ability in demonstrating the required skills and knowledge) |
| --- | --- | --- | --- | --- |
| Identifies the valuable assets of the organisation | |  |  |  |
| Identifies the risk appetite for the organisation. | |  |  |  |
| Used listening skills to respond appropriately. | |  |  |  |
| Responds to client questions using suitable language. | |  |  |  |
| Questioning techniques to confirm understanding of clients. | |  |  |  |

* 1. **Document the assets.**  
     After the meeting record at least one of each type of the assets you have identified in the assets register (ICTICT424\_SR\_2of2). You must include at least one (1) mobile device (e.g. phone or tablet) in the list of assets.  *You can use your phone in this with the purchase date, warranty and life expectancy based on your experience and assumptions.* *Any missing information can be assumed by you from the supporting resources or based on personal experience and research.*



1. Now that you have identified the valuable assets you must asses the threats to these assets and the likelihood and impact of those threats to get a risk rating. This will help the organisation to identify the assets that require the most protection.

The threat that the organisation is most worried about is losing information and infection due to malware or intruders.

* 1. Using the table below, assess the threats and the risks to some of these assets identified by using the threat/likelihood/impact risk assessment table (table 3). You must justify your reasoning.   
     You must include a mobile device (e.g. phone or tablet) in the list of assets.

Table - Threat table

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Asset | Threat | Likelihood | Impact | Risk Rating | Comment |
| Data Base system | Unauthorised access | Low | High | Medium | If data base is compromised customer imformation could be leaked causing harm for customers |
| Customer imformation | Personal data released | Medium | High | High | Privacy and security breaches can cause huge impacts to the companies integrity. |
| Computer | Stolen | High | High | Critical | Data can be stolen unless precautions are taken such as remote authorisation |
| Mobile device | Malicious application | High | Medium | High | Imformation can be stolen without precautions such as no jail broken devices or regulating apps that can be installed. |

Table - Rating table

|  |  |  |  |
| --- | --- | --- | --- |
|  | Low Impact | Medium Impact | High Impact |
| High Likelihood | Medium | High | Critical |
| Medium Likelihood | Low | Medium | High |
| Low Likelihood | Negligible | Low | Medum |

* 1. What asset is at the highest risks? Why do you think this is the case? (50-100 words).

Computer being stolen as they would have access to customer and private information which could seriously effect consumer confidence and integrity of the business. Another risk could be holding the information at ransom so they thief black mails you into paying a price set by the thief to give your device back.

1. For each threat and asset in question 2 analyse and document the cyber security contols required to deal with each. You must include a strategy for mobile devices.   
   Note: The organisation has advised you that they have anti-virus software on all their PC’s but it is not installed on any of their servers or mobile devices.

Table - Mitigation

|  |  |  |
| --- | --- | --- |
| Asset | Threat | Requirements |
| Data Base system | Unauthorised access |  |
| Customer imformation | Personal data released | Ensure passwords and data is encrypted to minimise chance of information being released |
| Computer | Stolen | Ensure remote authentification is enabled so that the data can be locked remotely |
| Mobile device | Malicious application | Makes sure devices are following company BYOD protocol |

1. Based on the BYOD policy (as per ICTICT424\_SR\_1of2), identify security gaps that exist and ways to enhance cyber security for Smith & Jones . (50-100 words).

The ability to install and enrol the supplied devices should be able to be controlled by an admin

Installing or removing applications

The ability to remote wipe if required

The ability to remote lock the devices

Passwords/passcodes can be longer, may be changed on a regular basis

Two-Factor authentication can be employed

1. You must advise the organisation about some controls that can be used to help address the cyber security gaps in the BYOD policy, especially regarding mobile phones and tablets. Provide a description of the control and justify why it fits the gap. (50-100 words). Provide links or references.

Reducing permissions on each mobile device so that certain information cannot be accessed if there is a potential that this data to cause a threat if the device is compromised by an external or internal threat. This will limit the effect of a possible privacy within our organisation.

1. The organisation has advised that they would like to ensure that they can check the devices the organisation issues to their staff and address the cybersecurity gaps by controlling the device to some degree.

Provide a comparison via email to the manager advising them of mobile device management solutions that will meet their needs, what you believe is a higher priority and your recommendation. Include the free Comodo MDM solution as found at <https://dm.comodo.com/free-mdm> in your comparison.   
(150-200 words). Provide links or reference

Mobile device management solution

1. You must have a meeting with an organisation representative (one of your fellow students) to seek feedback on the controls you have advised and agree what you are going to implement as part of the solution. Note that the chosen MDM solution will be Comodo MDM solution as available at <https://dm.comodo.com/free-mdm>.   
   Record details of the meeting here.

#### Role-play

This task should take approximately 5 to 10 minutes.

Use this Checklist to understand what skills you need to demonstrate in the practical task demonstration. The Checklist lists the assessment criteria used to determine whether you have successfully completed this assessment event. All the criteria must be met. Your demonstration will be used as part of the overall evidence requirements of the unit. The assessor may ask questions while the demonstration is taking place or if appropriate directly after the task/activity has been completed.

Table - Meeting Checklist

| Task # | Task/Activity Performed | S | U/S | Assessor Comments (Describe the student’s ability in demonstrating the required skills and knowledge) |
| --- | --- | --- | --- | --- |
| Asked for feedback ensuring organisation representative understood the solution and provides feedback on the suitability of the solution. | |  |  |  |
| Agreed to implement particular controls. | |  |  |  |
| Used listening skills to respond appropriately. | |  |  |  |
| Responds to client questions using suitable language. | |  |  |  |
| Questioning techniques to confirm understanding of clients. | |  |  |  |

1. If the security policies and solution was not successful, advise the organisation what legislative requirements from Australia they would need to consider. Provide an explanation of what they need to know. (50-100 words). Provide links or references.

## Part 3: Solution implementation

To complete this part of the assessment, you will be required to setup an MDM solution as provided by Comodo.

1. Set up the Comodo MDM free security app via <https://dm.comodo.com/free-mdm>  
   You will need to use your tafe email address to set it up.  
   Provide a screenshot of the setup.

1. When registering for this service you will need to choose a URL prefix. Please use a sensible one such as tafe-<firstname-lastname> where <your-name> is replaced with your first and last names. Eg if your name is Tom Jones make the prefix tafe-tom-jones.  
   Copy/paste or screenshot the URL you used.

1. Enrol your device and show that it is in the enrolled device list.  
   (We suggest you use your mobile – but if you have issues with using your device please consult your teacher.)  
   Provide a screenshot showing your device enrolled in the website dashboard

1. Send a test message.  
   Test the message system by sending a test text message. Provide a screenshot from the phone. (*You may need to email this to yourself.*)

1. Develop a guide showing what needs to be done by:
   1. an admin to setup an Android or Apple device
   2. a user to setup an Android or Apple device

## Part 4: Post implementation and consultation

Now that you have completed installing the MDM solution you need to complete some post-installation tasks.

1. Organise a meeting with an organisation representative (one of your fellow students) to discuss the control you have implemented and gather feedback about what controls they have found meets the requirements and what controls, if any, don’t meet their requirements.  
   Record details of the meeting here.

#### Role-play

This task should take approximately 5 to 10 minutes.

Use this Checklist to understand what skills you need to demonstrate in the practical task demonstration. The Checklist lists the assessment criteria used to determine whether you have successfully completed this assessment event. All the criteria must be met. Your demonstration will be used as part of the overall evidence requirements of the unit. The assessor may ask questions while the demonstration is taking place or if appropriate directly after the task/activity has been completed.

Table - Meeting Checklist

| Task # | Task/Activity Performed | S | U/S | Assessor Comments (Describe the student’s ability in demonstrating the required skills and knowledge) |
| --- | --- | --- | --- | --- |
| Asked for feedback ensuring organisation representative understood the solution and provides information on the suitability of the solution and any issues. | |  |  |  |
| Identified any issues with the solution and any differences between the proposed solution and the implementation. | |  |  |  |
| Used listening skills to respond appropriately. | |  |  |  |
| Responds to client questions using suitable language. | |  |  |  |
| Questioning techniques to confirm understanding of clients. | |  |  |  |

1. Considering the asset register you completed in Part 2 question 1(b), is it still current after Part 3? What assets now needs to be added to this register? (25-75 words).  
   You must add at least 2 new assets to the register.

1. Provide a description of how the threats and risks in Part 2 question 2 above have now changed? (25-75 words).

1. After you added a device to the mobile device management system, a routine check by the organisation and your team has found devices have potential security issues that the first analysis didn’t take into account including that BYOD devices may be insecure due to passwords/passcodes not being used and insecure apps as well as guests using the WIFI network who are not part of the MDM solution may have insecure devices.   
   In a team (with one person playing the role of the organisation representative) have a meeting to discuss:
   1. What controls you can identify may be applicable;
   2. determine which controls you can use in the Comodo MDM solution;
   3. agree on which controls you will use that may reduce or eliminate the security gaps.

Record details of the meeting here.

#### Role-play

This task should take approximately 5 to 10 minutes.

Use this Checklist to understand what skills you need to demonstrate in the practical task demonstration. The Checklist lists the assessment criteria used to determine whether you have successfully completed this assessment event. All the criteria must be met. Your demonstration will be used as part of the overall evidence requirements of the unit. The assessor may ask questions while the demonstration is taking place or if appropriate directly after the task/activity has been completed.

Table - Meeting Checklist

| Task # | Task/Activity Performed | S | U/S | Assessor Comments (Describe the student’s ability in demonstrating the required skills and knowledge) |
| --- | --- | --- | --- | --- |
| Identifies controls which address the new gaps. | |  |  |  |
| Discussed and determined which controls are possible in the Comodo MDM solution | |  |  |  |
| Agrees with controls to address the new gaps. | |  |  |  |
| Used listening skills to respond appropriately. | |  |  |  |
| Responds to questions using suitable language. | |  |  |  |
| Questioning techniques to confirm understanding of solutions. | |  |  |  |

1. Now that you have determined that some application may need to be blocked or removed from the devices you are tasked with doing this in the Comodo MDM solution. To assist with the organisation doing this themselves you are required to block and remove specific applications and provide the documentation showing them how to do it themselves.   
   On the dashboard, block an application from working.
2. Provide a description showing how to block an application and a screenshot showing the application blocked.

Provide a description showing how to remove an application and a screenshot showing the application removed.

1. Provide a screenshot from the mobile device showing the application being blocked. *(You may need to email this to yourself to record and document actions.)*

Provide a screenshot from the mobile device showing the application the application being removed. *(You may need to email this to yourself to record and document actions.)*

NOTE: Once these exercises have been completed you will need to unenroll it from the MDM solution and remove the MDM application from your mobile device.

## Part 5: Assessment Feedback

*NOTE: This section* ***must*** *have the assessor signature and student signature to complete the feedback.*

### Assessment outcome

Satisfactory

Unsatisfactory

### Assessor Feedback

Was the assessment event successfully completed?

If no, was the resubmission/re-assessment successfully completed?

Was reasonable adjustment in place for this assessment event?  
*If yes, ensure it is detailed on the assessment document.*

Comments:

### Assessor name, signature and date:

### Student acknowledgement of assessment outcome

Would you like to make any comments about this assessment?

### Student name, signature and date

***NOTE: Make sure you have written your name at the bottom of each page of your submission before attaching the cover sheet and submitting to your assessor for marking.***