RTO No. 31652 | CRICOS 03500M

INFORMATION TECHNOLOGY

ICTNWK502

Implement Secure Encryption Technologies

Assessment Tool 3 of 3: Practical Project

PRINT CLEARLY - Please fill out the following using Black Only.

Qualification	ICT60615 Advanced Diploma of Telecommunication		
Student name			
Student number			
Student email			
Assessor name	Ansel Thomas		
Assessment due date			
Submission date	Attempt 1 Date:	Attempt 2 Date:	Attempt 3 Date:
Result for attempt (S or NS)	Date marked: ☐ Satisfactory ☐ Not Satisfactory	Date marked: ☐ Satisfactory ☐ Not Satisfactory	Date marked: ☐ Satisfactory ☐ Not Satisfactory

Note: If you have not signed the student declaration on the next page your submission will not be accepted.

Student declaration of authenticity

Before you submit this Assessment Tool you must declare that the work is your own. Read the text below. Sign the declaration if you agree with all the statements.

I declare:

- This assessment is my own work, based on my own study and research and no part of it has been copied from any other source, except where due acknowledgement/reference has been made. (Plagiarism is not permitted in any form)
- A late submission fee of $100 per unit of competency will apply before my submission will be marked if my submission is made past the due time and date.
- If this assessment is based on teamwork, as authorised by the assessor, I have not submitted the same final version of any assessment material as another student.
- I have not previously submitted this assessment or any part of this assessment for this or any other course/unit unless required to do so in a resubmission.
- I have kept a copy of my assessment.
- I give permission for my assessment to be reproduced, communicated, compared and archived for the purposes of detecting plagiarism or collusion and to fulfil Vibe College's requirements as an RTO.
- Any assessment marked as unsatisfactory will require me to undergo reassessment; reassessment may involve different assessment to that originally undertaken.
- I have read and understand the policies and procedures relating to assessment as outlined in the Vibe College Student Handbook (or the International Student Handbook) and the Student Assessment Guide.

 Signed: **Dated:**

Note: If you are completing this document electronically, use either a scanned and cropped jpg image of your signature or type your name in the space above.

For documents submitted through Moodle, the inclusion of this declaration with any form of signature, however presented, with your submission, indicates that you understand and agree the declaration is true.

If you are completing this Assessment Tool as self-marking questions on Moodle, you will be required to agree to an electronic statement of authenticity at the beginning of the Knowledge questions before being able to proceed.

Copyright

Version Control & History

Version	Summary of modifications made
Version 1.1 Sept 2019	New Assessment Tool Created

Purpose

This Assessment Tool assesses your ability to determine, Implement and monitor Encryption Methods.

Location

For the simulated work environments, you are to assume that you have been employed by Binary Digital Pty Ltd.

Resources supplied to you.

- ICTNWK502 Learner Guide
- ICTNWK502 PowerPoint
- Moodle Access

Resources you will need.

- Computer Access
- Internet Access

How to submit this Assessment Tool?

What?	A copy of this Assessment Tool, named correctly and completed with your responses. Remember to fill in the cover sheet before submission.
When?	Your assessor will advise the due date and time for this assessment.
Where?	Upload to the submission link for Assessment Tool 3 of 3 in Moodle. If your assessor advises not to use Moodle, you may hand in your printed copy of this Assessment Tool however you MUST keep a copy.

What must you do to achieve Satisfactory for this Assessment Tool?

This Assessment Tool is the second of 3 assessments for this Unit of Competency.

You must achieve a Satisfactory result for each of the 3 Assessment Tools to achieve an overall mark of Competent for this Unit of Competency.

You are permitted 3 attempts at this assessment.

Instructions

1. Make a copy of this document. Name it **ICTNWK502_YourStudentID_ [Your Name] _AT 3 of 3_submission1** (if your first attempt, submission2 if your second etc.)

2. Complete the cover sheet and sign the declaration of authenticity. Your submission **will be rejected unless** both are completed. Rejection may mean a delay in your submission and the imposition of a late fee which must be paid before your work will be marked.

3. Complete all sections below where you are asked to provide answers. Grey texts are to be deleted.

4. You need to submit this document when you have completed all sections. You need to upload the document to Moodle by clicking on the link named ICTNWK502_AT 3 of 3_Submission link. You MUST keep the original of this document somewhere safe.

Assessment Task-1

Question 1: Explain each of the following symmetric key algorithms in 50-100 and list at least two (2) usages for each of symmetric key algorithms.

1) AES
2) DES
3) Triple DES
4) Blowfish

<Write Your Response Here>			
Assessor Feedback	**S**	**NS**	**Feedback (MUST be provided if NS is selected)**
	☐	☐	

Question 2: Explain each of the below mention encryption types in 80-150 words:

1. Public Key
2. Secret Key
3. Hash key

<Write Your Response Here>

Assessor Feedback	S	NS	Feedback (MUST be provided if NS is selected)
	☐	☐	

Question 3:   Explain the functioning of "Digital signatures" in 100-150 words.

<Write Your Response Here>

Assessor Feedback	S	NS	Feedback (MUST be provided if NS is selected)
	☐	☐	

Question4:   Explain two (2) features of digital signatures. Write 100-150 for each function.

<Write Your Response Here>			
Assessor Feedback	**S**	**NS**	**Feedback (MUST be provided if NS is selected)**
	☐	☐	

Question5:   Answer the below questions related to timestamp.

5A) Explain two (2) functions of timestamp. Explain each in 50-100 words.

5B) Summarize two features of timestamp.

<Write Your Response Here>			
Assessor Feedback	**S**	**NS**	**Feedback (MUST be provided if NS is selected)**
	☐	☐	

Question6: What do you understand by the term "Encryption strength"? Explain in 50-100 words.

<Write Your Response Here>			
Assessor Feedback	**S**	**NS**	**Feedback (MUST be provided if NS is selected)**
	☐	☐	

Question7: Explain each of following terms in 50-150 words.

1. Message digest 5 (MD5)
2. Secure hash algorithm (SHA)
3. Public key infrastructure (PKI)
4. Pretty good privacy (PGP)
5. GNU privacy guard (GnuPG)

<Write Your Response Here>			
Assessor Feedback	**S**	**NS**	**Feedback (MUST be provided if NS is selected)**
	☐	☐	

Question8:   Explain the importance of reviewing helpdesk records to troubleshoot encryption issues. Explain in 40-80 words.

<Write Your Response Here>			
Assessor Feedback	**S**	**NS**	**Feedback (MUST be provided if NS is selected)**
	☐	☐	

Question 9: What important information will you collect by reviewing system logs for encryption issues and compromises. Write your response un 50-100 words.

<Write Your Response Here>

Assessor Feedback	S	NS	Feedback (MUST be provided if NS is selected)
	☐	☐	

Question10: Explain each the following security threat in 50-100 words.

1. Eavesdropping
2. Data Interception
3. Data corruption
4. Data falsification
5. Authentication issues.

<Write Your Response Here>

Assessor Feedback	S	NS	Feedback (MUST be provided if NS is selected)
	☐	☐	

Question11: Explain the term "Transmission Control Protocol" and its application in 150-200 words.

<Write Your Response Here>

Assessor Feedback	S	NS	Feedback (MUST be provided if NS is selected)
	☐	☐	

Question12: Explain the following terms. (Each in 50-150 words).

1. Wired Equivalent Privacy (WEP)
2. Wi-Fi Protected access (WPA)
3. Wi-Fi Protected access 2 (WPA2)

<Write Your Response Here>

Assessor Feedback	S	NS	Feedback (MUST be provided if NS is selected)
	☐	☐	

Question 13: Explain each of the following certificate related infrastructure in 50-150 words?

1) Certificate authorities
2) Registration authorities
3) Repository services

<Write Your Response Here>

Assessor Feedback	S	NS	Feedback (MUST be provided if NS is selected)
	☐	☐	

Question14: List three (3) most common asymmetric key algorithms and summarise their usages in 40-80 words.

<Write Your Response Here>			
Assessor Feedback	**S**	**NS**	**Feedback (MUST be provided if NS is selected)**
	☐	☐	

Question 15:   What do you understand by reply attacks? Write your response in 100-150 words.

<Write Your Response Here>			
Assessor Feedback	**S**	**NS**	**Feedback (MUST be provided if NS is selected)**
	☐	☐	

Question 16:   List and explain five (5) security problems and challenges arise due to organisational issues?

<Write Your Response Here>			
Assessor Feedback	**S**	**NS**	**Feedback (MUST be provided if NS is selected)**
	☐	☐	

Question 17:   Summarise the features and functions of access control permission in 100-200 words.

<Write Your Response Here>			
Assessor Feedback	**S**	**NS**	**Feedback (MUST be provided if NS is selected)**
	☐	☐	

Question 18:   Explain the functioning and features of the following in 100-200 words for each.

1.   Symmetrical Encryption
2.   Asymmetrical Encryption

<Write Your Response Here>			
Assessor Feedback	**S**	**NS**	**Feedback (MUST be provided if NS is selected)**
	☐	☐	

Question 19:   Summarise the features and functions of "One-way encryption"?

<Write Your Response Here>			
Assessor Feedback	**S**	**NS**	**Feedback (MUST be provided if NS is selected)**
	☐	☐	

Question 20:   List two techniques to analyse data security requirements.

<Write Your Response Here>			
Assessor Feedback	**S**	**NS**	**Feedback (MUST be provided if NS is selected)**
	☐	☐	

Question 21:   What is the essential information should include in a security plan. List any three (3).

<Write Your Response Here>			
Assessor Feedback	**S**	**NS**	**Feedback (MUST be provided if NS is selected)**
	☐	☐	

Assessment Task-2

Scenario:

"Southern Star" company is providing public, private, hybrid and community cloud services to many companies across the world and offering following services:

- IaaS (Infrastructure-as-a-Service)
- PaaS (Platform-as-a-Service)
- SaaS (Software-as-a-Service)
- Storage, Database, Information, Process, Application, Integration, Security, Management Testing-as-a-service

To provide above mentioned cloud services, "Southern Star" company has following infrastructure in their data centre.

- Eight (8) Servers out of these Six (6) are connected to network and Two (2) are kept as backup.
- Twelve (12) Network switches with 24 port support (Nine (9) Switches are connected to network are three (3) are kept as back up)
- Six (6) Routers (4 Routers are hosing NBN connection and two (2) of them are kept as back up)
- Five (5) wireless access point connected to network to provide Wi-Fi connectivity throughout data centre.
- Twenty (20) SAN (Storage area network) storage area devices to store client's data.

- Fifty (50) desktop computers

"Shan Publications" is a premium client of "Southern Star". "Shan publication" use cloud services offered by "Southern Star" to store the drafts of unpublished poems, books and blueprints of printed books. One day as they were downloading the drafts of some books to publish, they found that some of their data is missing from the server and raised the complaint about missing data to "Southern Star". As per the agreement "Southern Star" is liable for client data security and company do not want to lose their client base.

Southern Star is now investigating the problem, and one of the senior consultants (Lee) is allocated to this project. Lee is working in the company from last 10 years and has an extensive amount of experience in network, cloud and data security.

David is a general manager of the Southern star and looking after all the operation of the organisation.

Roles and responsibilities of Lee:

- Planning, implementing, and upgrading security measures and controls.
- Establishing plans and protocols to protect digital files and information systems against unauthorized access, modification and/or destruction.
- Maintaining data and monitor security access.
- Performing vulnerability testing, risk analyses and security assessments
- Conducting internal and external security audits
- Anticipating security alerts, incidents and disasters and reduce their likelihood.
- Managing network, intrusion detection and prevention systems
- Analysing security breaches to determine their root cause.
- Recommending and install appropriate tools and countermeasures.
- Defining, implementing, and maintaining corporate security policies
- Training fellow employees in security awareness and procedures
- Coordinating security plans with outside vendors

After an initial investigation of the data loss problem, Lee has found below concerns in the southern star network infrastructure:

- No data encryption service
- Data security concerns
- Data permission not planned.
- Additional hardware to manage the data.

Activity 1: (Analysing and documenting data security requirement)

After reviewing the scenario, you need to analyse the data loss problem and need to prepare a security plan including.

- Background of the security plan
- Issues identified in the network
- How to resolve each issue
- What hardware and software required
- How identified software and hardware aligned with the solutions

- How and when data backup will be prepared
- Transmission security

- Network database security

You may need to research related to security plan on the internet. You must complete below security plan as a part of the activity.

Security Plan Template

Background-
Issues identified in the network
How to resolve each issue
What hardware and software required

How identified software and hardware aligned with the solutions

Transmission Security

File Transfer:	Name	Version	Vendor
• Encryption Software Used:			
• Network Monitoring tools			
• Virus Scanning software			
• Data Transfer authentication method			
• Network Based DLP			
Email: • Service Provider			
• Password Strength Criteria			
• Domain reputation			

Network Database Security

Access Control			
Authentication			
Encryption method			
Backups			

<Write Your Response Here>

Assessor Feedback	S	NS	Feedback (MUST be provided if NS is selected)
	☐	☐	

Activity 2:

(Review encryption technologies and costs)

Note: This activity is in continuation of activity 1.

After completing the security plan, you are required to review a range of encryption software on the internet and complete below Technology cost template.

After completing the template, you are required to send email to David (Trainer/assessor) including technology cost document for approval. Email must include:

- Subject
- Body
- Explain that which option is the best and why we should use it.

Technology Cost Template

S. No	Encryption Software	Vendor	Encryption Applicability (Network/ Database)	Price	Rank (from 1 -5)	Remarks
1.						
2.						
3.						
4.						
5.						

Assessment Task- 3

Project Task:

Activity 1(Installing encryption software)

This activity is continuation of assessment task 2. You are required to participate in a practical demonstration task. You need to complete this activity in 1 to 2 hours.

Note: For This activity RTO/Assessor will provide you the following:

- A site where encryption installation may be conducted
- A live network
- Servers
- Encryption software
- Encryption tools*.*

You have received a final approval from David to start the encryption project, so you must perform the installation of encryption software and tools on the live network.

Assume yourself as "Lee" and install database encryption software and tools.

You need to install encryption software on IT Server. You need to Perform installation of database "Encryption" software by adhering below mention conditions.

    a.   Use secure protocol for data transfer
    b.   Create a digital key certificate for client and server
    c.   Use secure network protocols
    d.   Set admin password

Student must follow vendor instruction to install the software.

Your trainer and assessor will observe you during the activity and complete the performance checklist.

Activity 2: (Analysing effect of encryption on user roles)

Note: This activity is in continuation of activity 1.

Assume that Lee has implemented the encryption software successfully. As a part of his responsibilities, he needs to analyse the effect of user roles and responsibilities.

Assume yourself as Lee and you are required to analyse the effect of user roles and responsibilities in encryption and complete the following template.

Role	Description
Enterprise Administrator	
Group or Policy Administrator	
Enterprise Authenticator	
Group or Policy Authenticator	
User	

Activity 3: (Role Play - Informing users about their roles)

Note: This activity is in continuation of activity 2.

- o Time allowed for this activity is 10-15 minutes.

Assume that you are still playing the role of Lee and participate in the following role play.

The purpose of the role play is to inform users about new encryption technology and how it works. Explain the effects of new encryption technology on user responsibilities. You need to use the template that you have developed in the assessment activity 2 (Assessment task 3) to explain the effects of new encryption technology on user responsibilities for the following users:

- o Policy administrator
- o Enterprise Authenticator
- o Policy authenticator
- o User

Your trainer/assessor will act as enterprise administrator and will ask you the following questions:

1. Security limitations of all the roles

2. Explanation of the features included in the "Enterprise administrator" role

Following the role play, complete minutes of meeting template with details of what was discussed.

Minutes of Meeting

Meeting Objective:

Attendees:

Venue:

Date:

No.	Points Discussed	Actions Suggested	Target Date

Signature of attendee 1:   **Signature of attendee 2:**

Signature of attendee 3:   **Signature of attendee 4:**

Activity 4: (Analysing functioning of "Encryption software")

Assuming that you have implemented the encryption technology and tools in a live server in the previous assessment activities, you are required to monitor the encryption in this activity. You need to complete this task in 1 to 2 hours.

In this activity you need to monitor the functioning of "Encryption software" by perform following tasks in a live server.

1. Analyse the implementation of encryption technology to confirm its functioning by:
   o   Monitoring digital signature
   o   Monitoring Data Encryption Compromising Network Performance
   o   Monitoring network performance
2. Analyse helpdesk records for errors occurred and security compromises in encryption and print these records as a part of this activity.
3. Check local computer security logs for encryption issues and print it as a part of this activity.
4. You need write a note on encryption issue and security compromises included error logs and network performance issues identified in the task and submit to your trainer/assessor.

Your trainer will observe you during the activity and complete the performance checklist.

Assessors note(s)	S (Satisfactory) NS (Not Satisfactory) Add the date of simulated work observed.	
Skill, behaviour and/or task to be observed to industry standard. **Did the student …**	**Date**	**Comment** If any column is marked NS, a comment is mandatory and detailed explanation of what was observed must be given.
Prepared Business case that addresses:		
Understood company's requirements of data security	S ☐ NS ☐	
Analyse data security requirements	S ☐ NS ☐	
Prepared a data security plan include all the information maintained in the template	S ☐ NS ☐	
Conducted research on internet for encryption software	S ☐ NS ☐	
Completed attached Technology Cost Template	S ☐ NS ☐	
Sent an email to David (Trainer/assessor) for approval including: • Subject • Body	S ☐ NS ☐	

• Explain that which option is the best and why we should use it.			
Installed encryption software and tools	S ☐	NS ☐	
Followed vendor instructions for installation	S ☐	NS ☐	
Configured management services	S ☐	NS ☐	
Set admin credentials	S ☐	NS ☐	
Generate digital ID's	S ☐	NS ☐	
Define user roles in encryption	S ☐	NS ☐	
Created digital Certificate for data exchange	S ☐	NS ☐	
Use secure Network protocol	S ☐	NS ☐	
Identified the roles of Enterprise Administrator	S ☐	NS ☐	
Identified responsibilities of Group or Policy Administrator	S ☐	NS ☐	
Identified roles of Enterprise Authenticator	S ☐	NS ☐	
Identified responsibilities Group or Policy Authenticator	S ☐	NS ☐	
Identified Responsibilities of User	S ☐	NS ☐	
Document user responsibilities in the given template	S ☐	NS ☐	
Strat roleplay with greetings	S ☐	NS ☐	
Explain the User roles and responsibilities confidentially	S ☐	NS ☐	
Use simple language to explain technical terminology	S ☐	NS ☐	
Explain the roles to individuals	S ☐	NS ☐	
Body Language during Presentation including: • Eye contact • Tone • Gesture	S ☐	NS ☐	

Analyse the implementation of encryption technology to confirm its functioning by including:
   o Check digital signature
   o Check Data Encryption Compromising Network Performance
   o Check network performance
	S
	☐
		NS
		☐	

Analyse helpdesk record for errors occurred and security compromises and submitted to the trainer/assessor	S ☐	NS ☐	
Check local computer security logs for encryption issues and submitted to the trainer/assessor	S ☐	NS ☐	
Prepared a note on encryption issue and compromises included error logs and network performance issues identified in the task and submit to your trainer/assessor	S ☐	NS ☐	

Result (for use by assessor only)

Has the student signed the declaration of authenticity or this has been done through Moodle?	☐ Yes ☐ No
Has reasonable adjustment been made by the assessor in assessing the student's competency in respect of this Assessment Tool?	☐ Yes ☐ No If Yes, the assessor must specify the arrangements of the reasonable adjustment. Describe here:
Name of assessor	Ansel Thomas
Signature of assessor	
Date of marking assessment	
Overall Result for this Assessment Tool	Satisfactory ☐ Not Satisfactory ☐
If resubmission is required, provide date	Click here to enter a date.
If resubmission is required, specify requirements	Resubmission due date and time: The following must be resubmitted: