# **Unit Assessment Pack (UAP) – Cover Sheet**

## **Student and Trainer/Assessor Details**

| **Student ID** |  |
| --- | --- |
| **Student name** |  |
| **Contact number** |  |
| **Email address** |  |
| **Trainer/Assessor name** |  |

## **Course and Unit Details**

| **Course code** |  |
| --- | --- |
| **Course name** |  |
| **Unit code** | ICTNWK503 |
| **Unit name** | Install and maintain valid authentication processes |

## **Assessment Submission Method**

|  |  |  |
| --- | --- | --- |
| ☐ By hand to trainer/assessor | ☐ By email to trainer/assessor | ☐Online submission via Learning Management System (LMS) |
| ☐ By Australia Post to RTO | ☐ Any other method \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (Please mention here) | |

**Student Declaration**

|  |
| --- |
| * I certify that the work submitted for this assessment pack is my own. I have clearly referenced any sources used in my submission. I understand that a false declaration is a form of malpractice; * I have kept a copy of this assessment pack and all relevant notes, attachments, and reference material that I used in the production of the assessment pack; * For the purposes of assessment, I give the trainer/assessor of this assessment the permission to:   + Reproduce this assessment and provide a copy to another member of staff; and   + Take steps to authenticate the assessment, including communicating a copy of this assessment to a checking service (which may retain a copy of the assessment on its database for future plagiarism checking).   Student signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Date: \_\_\_\_/\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

## **Assessment Plan**

To demonstrate competence in this unit, you must be assessed as satisfactory in each of the following assessment tasks.

| **Evidence recorded** | **Evidence Type/ Method of assessment** | | | **Sufficient evidence recorded/Outcome** |
| --- | --- | --- | --- | --- |
| **Unit Assessment Task 1** | Unit Knowledge Test (UKT) | | | S / NS (First Attempt)  S / NS (Second Attempt) |
| **Unit Assessment Task 2** | Unit Project (UP) | | | S / NS (First Attempt)  S / NS (Second Attempt) |
| **Unit Assessment Task 3** | Unit Project (UP) | | | S / NS (First Attempt)  S / NS (Second Attempt) |
| **Final result** | C/NYC | **Date assessed** |  | |
| **Trainer/Assessor Signature** |  | |

## **Assessment Conditions**

|  |
| --- |
| **Unit purpose/application** |

This unit describes the skills and knowledge required to design, develop, install and maintain authentication processes to reduce the vulnerability of the system.

It applies to individuals working as middle managers such as information security managers, network engineers or security analysts, who are responsible for implementing and monitoring the organisational security management system.

No licensing, legislative or certification requirements apply to this unit at the time of publication.

|  |
| --- |
| **What the student can expect to learn by studying this unit of competency** |

* Determine authentication requirements
* Configure authentication software or tools
* Apply authentication methods
* Monitor authentication system

|  |
| --- |
| **Training and assessment resources required for this unit of competency** |

The student will have access to the following:

* Learner guide
* PowerPoint presentation
* Unit Assessment Pack (UAP)
* Access to other learning materials such as textbooks

The resources required for these assessment tasks also included:

* Access to a computer, the Internet and word-processing system such as MS Word.
* A site where encryption installation may be conducted
* A live network
* Servers
* Encryption software
* Encryption tools.
* Simulated assessment environments must simulate the real-life working environment where these skills and knowledge would be performed, with all the relevant equipment and resources of that working environment.

|  |
| --- |
| **Submission instructions** |

Yourtrainer/assessor will confirm assessment submission details for each assessment task.

|  |
| --- |
| **Academic integrity, plagiarism and collusion** |

**Academic Integrity**

Academic Integrity is about the honest presentation of your academic work. It means acknowledging the work of others while developing your own insights, knowledge and ideas.

As a student, youare required to:

* undertake studies and research responsibly and with honesty and integrity
* ensure that academic work is in no way falsified
* seek permission to use the work of others, where required
* acknowledge the work of others appropriately
* take reasonable steps to ensure other students cannot copy or misuse your work.

**Plagiarism**

Plagiarism means to take and use another person's ideas and or manner of expressing them and to pass them off as your own by failing to give appropriate acknowledgement. This includes material sourced from the internet, RTO staff, other students, and from published and unpublished work.

Plagiarism occurs when you fail to acknowledge that the ideas or work of others arebeing used, which includes:

* Paraphrasing and presenting work or ideas without a reference
* Copying work either in whole or in part
* Presenting designs, codes or images as yourown work
* Using phrases and passages verbatim without quotation marks or referencing the author or web page
* Reproducing lecture notes without proper acknowledgement.

**Collusion**

Collusion means unauthorised collaboration on assessable work (written, oral or practical) with other people. This occurs when a student presents group work as their own or as the work of someone else.

Collusion may be with another RTO student or with individuals or students external to the RTO. This applies to work assessed by any educational and training body in Australia or overseas.

Collusion occurs when youwork without the authorisation of the teaching staff to:

* Work with one or more people to prepare and produce work
* Allow others to copy your work or share your answer to an assessment task
* Allow someone else to write or edit yourwork (without rto approval)
* Write or edit work for another student
* Offer to complete work or seek payment for completing academic work for other students.

Both collusion and plagiarism can occur in group work. For examples of plagiarism, collusion and academic misconduct in group work please refer to the RTO’s policy on Academic integrity, plagiarism and collusion.

Plagiarism and collusion constitute cheating. Disciplinary action will be taken against students who engage in plagiarism and collusion as outlined in RTO’s policy.

Proven involvement in plagiarism or collusion may be recorded on students’ academic file and could lead to disciplinary action.

|  |
| --- |
| **Other Important unit specific Information** |

N/A

|  |
| --- |
| **Unit outcome** |

* This unit is not graded and the student must complete and submit all requirements for the assessment task for this cluster or unit of competency to be deemed competent.
* Students will receive a 'satisfactorily completed' (S) or 'not yet satisfactorily completed (NS) result for each individual unit assessment task (UAT).
* Final unit result will be recorded as competency achieved/competent (C) or competency not yet achieved/not yet competent (NYC).

|  |
| --- |
| **Prerequisite/s** |

Nil

|  |
| --- |
| **Co-requisite/s** |

Nil

|  |
| --- |
| **Foundation Skills** |

The Foundation Skills describe those required skills (learning, oral communication, reading, writing, numeracy, digital technology and employment skills) that are essential to performance. Foundation skills essential to performance are explicit in the performance criteria of this unit of competency.

|  |
| --- |
| **Relevant Legislation** |

* Australian Human Rights Commission Act 1986
* Age Discrimination Act 2004
* Disability Discrimination Act 1992
* Racial Discrimination Act 1975
* Sex Discrimination Act 1984
* The Privacy Act 1988 (Privacy Act) and Australian Privacy Principles (APPs)
* Occupational Health and Safety Act 2004
* Work Health and Safety Act 2011

|  |
| --- |
| **Principles of assessment and rules of evidence** |

All assessment tasks will ensure that the principles of assessment and rules of evidence are adhered to.

The principles of assessment are that assessment must be valid, fair, flexible, reliable and consistent. The rules of evidence state that evidence must be sufficient, valid, current and authentic.

|  |
| --- |
| **AQF Level** |

AQF levels and the AQF levels criteria are an indication of the relative complexity and/or depth of achievement and the autonomy required to demonstrate that achievement.

All assessment tasks must ensure compliance with the requirements of AQF level and the AQF level criteria. For more information, please visit <http://www.aqf.edu.au/>

|  |
| --- |
| **Further Information** |

For further information about this unit go to[https://training.gov.au/Training/Details/ICTNWK50](https://training.gov.au/Training/Details/ICTNWK502)3

## **Additional Information**

* This information will be managed by the provisions of the Privacy Act and the Freedom of Information Act.)
* Students are required to satisfactorily complete and submit all assessment tasks that contribute to the assessment for a unit.
* Students will be provided with one more attempt to complete this Unit assessment pack (UAP) if trainer/assessor deems them not satisfactorily completed (NS) in any Unit assessment task (UAT).
* Unit Pre-Assessment Checklist (UPAC) will be reviewed by the trainer/assessor to ensure the student is ready for the assessment.
* Feedback regarding this Unit Assessment Pack (UAP) can be emailed to the [compliance](mailto:info@caqa.online) and quality assurance department/administration department in your RTO for continuously improving our assessment and student resources.

## **Feedback to student**

Feedback on students’ assessment performance is a vital element in their learning. Its purpose is to justify to students how their competency was assessed, as well as to identify and reward specific qualities in their work, to recommend aspects needing improvement, and to guide students on what steps to take.

Feedback defines for students what their trainer/assessor thinks is important for a topic or a subject. At its best, feedback should:

* Be provided for each Unit Assessment Task (UAT)
* Guide students to adapt and adjust their learning strategies
* Guide trainers/assessors to adapt and adjust teaching to accommodate students’ learning needs
* Be a pivotal feature of learning and assessment design, not an add-on ritual
* Focus on course and unit learning outcomes
* Guide students to become independent and self-reflective learners and their own critics
* Acknowledge the developmental nature of learning.

*If students have not received proper feedback, they must speak to compliance and quality assurance department/administration department in the RTO/person responsible for looking after the quality and compliance services of the RTO.*

*For more information, please refer to RTO Student Handbook.*

# **Unit Pre-Assessment Checklist (UPAC)**

# **UAT 1 – Unit Knowledge Test (UKT)**

## **Purpose of the checklist**

The pre-assessment checklist helps students determine if they are ready for assessment. The trainer/assessor must review the checklist with the student before the student attempts the assessment task. If any items of the checklist are incomplete or not clear to the student, the trainer/assessor must provide relevant information to the student to ensure they understand the requirements of the assessment task. The student must ensure they are ready for the assessment task before undertaking it.

**Section 1: Information for Students**

* Please make sure you have completed the necessary prior learning before attempting this assessment.
* Please make sure your trainer/assessor clearly explained the assessment process and tasks to be completed.
* Please make sure you understand what evidence is required to be collected and how.
* Please make sure you know your rights and the Complaints and Appeal process.
* Please make sure you discuss any special needs or reasonable adjustments to be considered during the assessment (refer to the Reasonable Adjustments Strategy Matrix and negotiate these with your trainer/assessor).
* Please make sure that you have access to a computer and the internet (if you prefer to type the answers).
* Please ensure that you have all the required resources needed to complete this Unit Assessment Task (UAT).
* Due date of this assessment task is according to your timetable.
* In exceptional (compelling and compassionate) circumstances, an extension to submit an assessment can be granted by the trainer/assessor.
* Evidence of the compelling and compassionate circumstances must be provided together with your request for an extension to submit your assessment work.
* Request for an extension to submit your assessment work must be made before the due date of this assessment task.

## **Section 2: Reasonable adjustments**

* Students with carer responsibilities, cultural or religious obligations, English as an additional language, disabilityetc. can request for reasonable adjustments.
* Please note, academic standards of the unit/course will not be lowered to accommodate the needs of any student, but there is a requirement to be flexible about the way in which it is delivered or assessed.
* The Disability Standards for Education requires institutions to take reasonable steps to enable the student with a disability to participate in education on the same basis as a student without a disability.
* Trainer/Assessor must complete the section below “Reasonable Adjustment Strategies Matrix” to ensure the explanation and correct strategy have been recorded and implemented.
* Trainer/Assessor must notify the administration/compliance and quality assurance department for any reasonable adjustments made.
* All evidence and supplementary documentation must be submitted with the assessment pack to the administration/compliance and quality assurance department.

|  |  |  |
| --- | --- | --- |
| **Reasonable Adjustment Strategies Matrix (Trainer/Assessor to complete)** | | |
| **Category** | **Possible Issue** | **Reasonable Adjustment Strategy**  **(select as applicable)** |
| 🞎 LLN | 🞎 Speaking  🞎 Reading  🞎 Writing  🞎 Confidence | 🞎 Verbal assessment  🞎 Presentations  🞎 Demonstration of a skill  🞎 Use of diagrams  🞎 Use of supporting documents such as wordlists |
| 🞎Non-English Speaking Background | 🞎 Speaking  🞎 Reading  🞎 Writing  🞎 Cultural background  🞎 Confidence | 🞎 Discuss with the student and supervisor (if applicable) whether language, literacy and numeracy are likely to impact on the assessment process  🞎 Use methods that do not require a higher level of language or literacy than is required to perform the job role  🞎 Use short sentences that do not contain large amounts of information  🞎 Clarify information by rephrasing, confirm understanding  🞎 Read any printed information to the student  🞎 Use graphics, pictures and colour coding instead of, or to support, text  🞎 Offer to write down, or have someone else write, oral responses given by the student  🞎 Ensure that the time available to complete the assessment, while meeting enterprise requirements, takes account of the student’s needs |
| 🞎Indigenous | 🞎 Knowledge and understanding  🞎 Flexibility  🞎 Services  🞎 Inappropriate training and assessment | 🞎 Culturally appropriate training  🞎 Explore understanding of concepts and practical application through oral assessment  🞎 Flexible delivery  🞎 Using group rather than individual assessments  🞎 Assessment through completion of practical tasks in the field after demonstration of skills and knowledge. |
| 🞎Age | 🞎 Educational background  🞎 Limited study skills | 🞎 Make sure font size is not too small  🞎Trainer/Assessor should refer to the student’s experience  🞎 Ensure that the time available to complete the assessment takes account of the student’s needs  🞎Provision of information or course materials in accessible format.  🞎Changes in teaching practices, e.g. wearing an FM microphone to enable a student to hear lectures  🞎Supply of specialised equipment or services, e.g. a note-taker for a student who cannot write  🞎Changes in lecture schedules and arrangements, e.g. relocating classes to an accessible venue  🞎Changes to course design, e.g. substituting an assessment task  🞎Modifications to physical environment, e.g. installing lever taps, building ramps, installing a lift |
| 🞎Educational background | 🞎 Reading  🞎 Writing  🞎 Numeracy  🞎 Limited study skills and/or learning strategies | 🞎 Discuss with the Student previous learning experience  🞎 Ensure learning and assessment methods meet the student’s individual need |
| 🞎Disability | 🞎 Speaking  🞎 Reading  🞎 Writing  🞎 Numeracy  🞎 Limited study skills and/or learning strategies | 🞎 Identify the issues  🞎 Create a climate of support  🞎 Ensure access to support that the student has agreed to  🞎 Appropriately structure the assessment  🞎Provide information or course materials in accessible format, e.g. a textbook in braille  🞎 Changes in teaching practices, e.g. wearing an FM microphone to enable a student to hear lectures  🞎 Supply of specialised equipment or services, e.g. a note- taker for a student who cannot write  🞎 Changes in lecture schedules and arrangements, e.g. relocating classes to an accessible venue  🞎Changes to course design, e.g. substituting an assessment task  🞎Modifications to physical environment, e.g. installing lever taps, building ramps, installing a lift |
|  |  |  |

| **Explanation of reasonable adjustments strategy used (If required)** |
| --- |
|  |

# **Unit Assessment Task (UAT)**

## **Assessment Task 1 - Unit Knowledge Test (UKT)**

**Assessment type:**

* Written Questions

**Assessment task description:**

* This is the first (1) unit assessment task you have to successfully complete to be deemed competent in this unit of competency.
* The Unit Knowledge Test is comprised of twenty-one(21)written questions
* You must respond to all questions and submit them to your Trainer/Assessor.
* You must answer all questions to the required level, e.g. provide the number of points, to be deemed satisfactory in this task
* You will receive your feedback within two weeks - you will be notified byyour Trainer/Assessor when results are available.

**Applicable conditions:**

* All knowledge tests are untimed and are conducted as open book tests (this means you are able to refer to your textbook during the test).
* You must read and respond to all questions.
* You may handwrite/use computers to answer the questions.
* You must complete the task independently.
* No marks or grades are allocated for this assessment task. The outcome of the task will be Satisfactory or Not Satisfactory.
* As you complete this assessment taskyou are predominately demonstrating your written skills and knowledge to your trainer/assessor.
* The trainer/assessor may ask you relevant questions on this assessment task to ensure that this is yourown work.

**Resubmissions and reattempts:**

* Where a student’s answers are deemed not satisfactory after the first attempt, a resubmission attempt will be allowed.
* You must speak to your Trainer/Assessor if you have any difficulty in completing this task and require reasonable adjustments (e.g. can be given as an oral assessment)
* For more information, please refer to your RTO Student Handbook.

**Location:**

* This assessment task may be completed in a learning management system (i.e. Moodle) or independent learning environment.
* Yourtrainer/assessor will provide you further information regarding the location for completing this assessment task.

**Instructions for answering written questions:**

* Complete a written assessment consisting of a series of questions.
* You will be required to correctly answer all the questions.
* Do not start answering questions without understanding what is required from you. Read the questions carefully and critically analyse them for a few seconds, this will help you to identify what is really needed.
* Your answers must demonstrate an understanding and application of relevant concepts, critical thinking, and good writing skills.
* Be concise to the point and write answers according to the given word-limit to each question and do not provide irrelevant information. Be careful, quantity is not quality.
* Be careful to use non-discriminatory language. The language used should not devalue, demean, or exclude individuals or groups on the basis of attributes such as gender, disability, culture, race, religion, sexual preference or age. Gender inclusive language should be used.
* When you quote, paraphrase, summarise or copy information from the sources you are using to write your answers/research yourwork, you must always acknowledge the source.

**How your trainer/assessor will assess yourwork?**

* This assessment task requires the student to answer all the questions.
* Answers must demonstrate the student’s understanding and knowledge of the unit.
* If all assessment tasks are deemed Satisfactory (S), then the unit outcome is Competent (C).
* If at least one of the assessment task is deemedNot Satisfactory (NS), then the unit outcome is Not Yet Competent (NYC).
* Once all assessment tasks allocated to this Unit of Competency have been undertaken, trainer/assessor will complete an Assessment plan to record the unit outcome. The outcome will be either Competent (C) or Not Yet Competent (NYC).
* The “Assessment Plan” is available with the Unit Assessment Pack (UAP) – Cover Sheet.

**Purpose of the assessment task:**

* The purpose of this assessment task is to assess the students’ knowledge required for the determination of the authentication requirements, its configurations, and application and monitoring on a computer network or local environment.

## **Assessment Task 1 - Unit Knowledge Test (UKT)**

**Instructions:**

* This is an individual assessment.

The purpose of this assessment task is to assess the students’ knowledge required to ensure secure file encryption is selected, implemented and monitored on a computer network or local environment.

* To make full and satisfactory responses you should consult a range of learning resources, other information such as handouts and textbooks, learners’ resources and slides.
* All questions must be answeredin order to gain competency for this assessment.
* You may attach a separate sheet if required.
* You must include the following particulars in the footer section of each page of the attached sheets:
  + Student ID or Student Name
  + Unit ID or Unit Code
  + Course ID or Course Code
  + Trainer and assessor name
  + Page numbers
* You must staple the loose sheets together along with the cover page.
* You must attach the loose sheets chronologically as per the page numbers.
* Correction fluid and tape are not permitted. Please do any corrections by striking through the incorrect words with one or two lines and rewriting the correct words.

Resources required to complete the assessment task:

* Learner guide
* PowerPoint presentation
* Unit Assessment Pack (UAP)
* Access to other learning materials such as textbooks
* Access to a computer, the Internet and word-processing system such as MS Word.

1. Explain the problems and challenges associated with the following organisational authentication issues. Write your response in 100-150 words for each.
2. Passwords
3. Smartcards
4. Biometrics
5. Resource Accounting

|  |
| --- |
| 1. ***Passwords***   ***Password-based authentication is one of the most popular approaches to authenticate a user in various enterprise applications. But there are many problems associated with the password based authentication systems and the risks associated with using passwords as an authentication mechanism for enterprise applications is not completely secure. Considering all the risks associated with password based authentication systems, there is a strong need for enterprises to switch to a stronger authentication system which provides security against the various hacking attacks and also which is more convenient and easier to the end user of the system***  ***Challenges with Password based Authentication:***   * ***Easy Password can be cracked*** * ***Random passwords can’t be remembered*** * ***Remembering multiple passwords*** * ***Problems with passwords that needs to be continuously changed*** * ***Security vs Easy of use for passwords*** * ***Shoulder Surfing Attack***   ***Reference:*** www.cioandleader.com. 2020. *Risks Of Password Based Authentication*. [online] Available at: <https://www.cioandleader.com/articles/9361/risks-of-password-based-authentication> [Accessed 7 November 2020].   1. ***Smartcards***   ***The biggest problem facing smart cards is security and the problem is two fold. The first issue is that not all smart cards are in fact secure. VISA and MasterCard developed a new standard, SET, in early 1996 in an attempt to get the entire industry on a standard of encryption. Additionally, there are standards such as DES which have been around for years, usable in all forms of encryption which are being used in smart cards. But still some smart cards are not inviolate. Mondex, a maker of banking smart cards, solves this problem by making its transactions possible only between Mondex cards. But in order for smart cards to reach their full potential, they must be able to interact with a host of interfaces. And they must do so securely.***  ***The second issue with security involves public perception of the technology. People must believe that the cards are secure. This depends to a great extent upon actual security, but people must also be convinced of it. And once people are comfortable that the card is secure, they must still be confident that Big Brother isn't somewhere collecting and analyzing all of the information gleaned from the smart cards' use.***  ***A third issue concerns who holds responsibility for the card. If the cash balance is wiped clean by a memory failure, who is liable, the person or the bank? If a transaction is not recorded, where are the lines drawn? Currently companies have begun to write out agreements in order to draw boundaries, but these will have to be ones which consumers are comfortable with in order for people to begin to use smart cards.***  ***Reference:*** Web.mit.edu. 2020. *Smart Cards: Disadvantages*. [online] Available at: <http://web.mit.edu/ecom/Spring1997/gr12/4DISADV.HTM> [Accessed 8 November 2020].   1. ***Biometrics***   ***Biometric identification is a technology that identifies and authenticates individuals based on physical characteristics. A biometric identification system includes fingerprint identification, iris and retina, facial recognition, gait, or voice. There are some problems associated with biometircs which are listed below as :***   * ***Biometrics aren’t private***   ***Biometrics seem secure on the surface. After all, you’re the only one with your ears, eyes, and fingerprint. But that doesn’t necessarily make it more secure than passwords. A password is inherently private because you are the only one who knows it. Of course hackers can acquire it by brute force attacks or phishing, but generally, people can’t access it. On the other hand, biometrics are inherently public.***   * ***Biometrics are Hackable***   ***Once a hacker has a picture of someone’s ear, eye, or finger, they can easily gain access to their accounts. While Apple’s TouchID was widely accepted as a biometric advancement, famous hacker Jan Krissler was able to beat the technology just a day after the iPhone was released. Likewise, researchers from the Chaos Computer Club created fake fingers to unlock iPhones.***   * ***Biometrics hacks may have greater Consequences***   ***Since a biometric reveals part of a user’s identity, if stolen, it can be used to falsify legal documents, passports, or criminal records, which can do more damage than a stolen credit card number.***  ***Reference:*** Howell, K., 2020. *3 Problems With Biometric Security, Including Fingerprint ID*. [online] Blog.ipswitch.com. Available at: <https://blog.ipswitch.com/3-reasons-biometrics-are-not-secure> [Accessed 8 November 2020].   1. ***Resource Accounting***   ***Confirmation, approval, and book keeping AAA is a term for a structure for wisely controlling access to PC assets, upholding arrangements, evaluating use, and giving the data important to charge for administrations. These joined procedures are viewed as vital for compelling system administration and security. As the primary procedure, confirmation gives a method for recognizing a client, commonly by having the client enter a legitimate client name and substantial watchword before get to be conceded. The procedure of verification depends on every client having an exceptional arrangement of criteria for getting entrance. The AAA server contrasts a client's confirmation certifications and other client accreditations put away in a database. On the off chance that the accreditations coordinate, the client is conceded access to the system. In the event that the qualifications are at fluctuation, verification falls flat and system get to is denied. Following confirmation, a client must pick up approval for doing certain errands.Subsequent to signing into a framework, for example, the client may attempt to issue orders. The approval procedure decides if the client has the specialist to issue such charges. Basically,approval is the way toward authorizing approaches: figuring out what writes or characteristics of exercises, assets, or administrations a client is allowed. More often than not, approval happens inside the setting of validation. When you have verified a client, they might be approved for various sorts of access or action. The last board in the AAA system is bookkeeping, which measures the assets a client expends amid get to. This can incorporate the measure of framework time or the measure of information a client has sent or potentially got amid a session.Bookkeeping is done by logging of session insights and use data and is utilized for approval control, charging, slant examination, asset usage, and scope organization exercises.*** |

1. Summarise the following Virtual Private Network issues. Write your response in 100-150 words for each issue.
2. Quality of service (QoS) considerations
3. Bandwidth
4. Dynamic security environment
5. Function and operation of VPN concepts

|  |
| --- |
| 1. ***Quality of service considerations***   ***Quality of Service (QoS) is a set of technologies that work on a network to guarantee its ability to dependably run high-priority applications and traffic under limited network capacity. QoS technologies accomplish this by providing differentiated handling and capacity allocation to specific flows in network traffic. This enables the network administrator to assign the order in which packets are handled, and the amount of bandwidth afforded to that application or traffic flow.***  ***Measurements of concern to QoS are bandwidth (throughput), latency (delay), jitter (variance in latency), and error rate. This renders QoS of particular importance to high-bandwidth, real-time traffic such as voice over IP (VoIP), video conferencing, and video-on-demand that have a high sensitivity to latency and jitter. These applications, with minimum bandwidth requirements and maximum latency limits, are called “inelastic.”***  ***The QoS mechanisms for ordering packets and allotting bandwidth are queuing and bandwidth management respectively. Before they can be implemented however, traffic must be differentiated using classification tools. The classification of traffic according to policy allows organizations to ensure the consistency and adequate availability of resources for their most important applications.***  ***Traffic can be classified crudely by port or IP, or using a more sophisticated approach such as by application or user. The latter parameters allow for more meaningful identification, and consequently, classification of the data.***  ***Next, queuing and bandwidth management tools are assigned rules to handle traffic flows specific to the classification they received upon entering the network.***  ***Reference:*** Palo Alto Networks. 2020. *What Is Quality Of Service?*. [online] Available at: <https://www.paloaltonetworks.com/cyberpedia/what-is-quality-of-service-qos> [Accessed 10 November 2020]. |
| 1. ***Bandwidth***   ***Bandwidth describes the maximum data transfer rate of a network or Internet connection. It measures how much data can be sent over a specific connection in a given amount of time. For example, a gigabit Ethernet connection has a bandwidth of 1,000 Mbps (125 megabytes per second). An Internet connection via cable modem may provide 25 Mbps of bandwidth.***  ***While bandwidth is used to describe network speeds, it does not measure how fast bits of data move from one location to another. Since data packets travel over electronic or fiber optic cables, the speed of each bit transferred is negligible. Instead, bandwidth measures how much data can flow through a specific connection at one time.***  ***When visualizing bandwidth, it may help to think of a network connection as a tube and each bit of data as a grain of sand. If you pour a large amount of sand into a skinny tube, it will take a long time for the sand to flow through it. If you pour the same amount of sand through a wide tube, the sand will finish flowing through the tube much faster. Similarly, a download will finish much faster when you have a high-bandwidth connection rather than a low-bandwidth connection.***  ***Data often flows over multiple network connections, which means the connection with the smallest bandwidth acts as a bottleneck. Generally, the Internet backbone and connections between servers have the most bandwidth, so they rarely serve as bottlenecks. Instead, the most common Internet bottleneck is your connection to your ISP.***  ***Reference:*** Techterms.com. 2020. *Bandwidth Definition*. [online] Available at: <https://techterms.com/definition/bandwidth> [Accessed 10 November 2020]. |
| 1. ***Dynamic Security Environment***   ***A dynamic virtual private network (DVPN) is an intranet enabler that complements regular Internet services by offering more networking services and resources.***  ***These networks can load balance on-the-fly allocating hardware resources more efficiently than the existing infrastructure may allow.***  ***Dynamic virtual private networks are commonly used by businesses because they offer an extra measure of security with their authentication packet encryption protocols.***  ***Dynamic virtual private networks (DVPN) are able to self-modify to recognize added nodes without the hardware and routers having to be able to identify them.***  ***DVPNs use encryption and authentication to securely package data and deliver it across local or wide area networks (WANs). The data remains encapsulated until it reaches a destination where decryption takes place. tunneling is used to reach remote networks across WANs.***  ***There is no decryption of the data at the nodes through which the data passes, where there is most risk of interception by hackers. The security of this networking mechanism is dependent upon the security of the encryption keys used at either end of the transmission.***  ***Reference:*** Techopedia.com. 2020. *What Is A Dynamic Virtual Private Network (DVPN)? - Definition From Techopedia*. [online] Available at: <https://www.techopedia.com/definition/25872/dynamic-virtual-private-network-dvpn> [Accessed 10 November 2020]. |
| 1. ***Function and Operation of VPN concepts***   ***The strain on today’s corporate networks is greater than ever before. Network managers must continually find ways to connect geographically dispersed work groups in an efficient, cost-effective manner. Increasing demands from feature-rich applications used by a widely dispersed workforce are causing businesses of all sizes to rethink their networking strategies. As companies expand their networks to link up with partners, and as the number of telecommuters and remote users continues to grow, building a distributed enterprise becomes ever more challenging. To meet this challenge, VPNs have emerged, enabling organizations to outsource network resources on a shared infrastructure. Access VPNs in particular appeal to a highly mobile work force, enabling users to connect to the corporate network whenever, wherever, or however they require.***  ***Reference:*** E-tutes.com. 2020. *Functions Of VPN - Computer Network Tutorial*. [online] Available at: <https://e-tutes.com/lesson12/functions-of-vpn/> [Accessed 10 November 2020]. |

1. Explain the adapter based authentication and use a diagram to illustrate the adapter based authentication implementation process. Write your response in 150-200 words.

|  |
| --- |
| ***Adapter-based authentication enables you to develop custom authentication logic by using a JavaScript function within a MobileFirst adapter.***  ***Adapter-based authentication is flexible and customizable. The following diagram illustrates one possible implementation. The process is illustrated and described as follows.***  ***adapter_based_authenticator***   * ***The client makes a request to the resource that is protected by adapter authentication.*** * ***MobileFirst Server checks whether the client is already authenticated. If it is, the requested data is returned.Otherwise, authentication continues.*** * ***The adapter procedure that is defined in authenticationConfig.xml as a login-function is called.*** * ***The login-function procedure is used to return a custom JSON payload to the client.*** * ***The client processes the custom JSON payload and sends its credentials to the adapter procedure used for authentication.*** * ***The adapter procedure that is used for authentication receives credentials and validates them. If validation fails, the flow returns to step 4. Otherwise, authentication continues.*** * ***The adapter procedure that is used for authentication creates a user identity and returns a success status to the client.*** * ***The client receives the success status and issues the original request.*** * ***The flow returns to step 2.***   ***Reference:*** Ibm.com. 2020. *IBM Knowledge Center*. [online] Available at: <https://www.ibm.com/support/knowledgecenter/en/SSHS8R\_7.1.0/com.ibm.worklight.dev.doc/devref/t\_adapter\_based\_authenticator.html> [Accessed 10 November 2020]. |

1. Explain biometric authentication adapters and list the six (6) types of biometric authentication. Write your answer in 150-200 words.

|  |
| --- |
| ***Biometric authentication is simply the process of verifying your identity using your measurements or other unique characteristics of your body, then logging you in a service, an app, a device and so on.***  ***Different types of biometric authentication are listed below as:***   1. ***Fingerprint***   ***Fingerprint recognition is widely considered to be one the oldest and most developed types of biometric recognition. Fingerprints are easy to capture, and can verified by comparing the unique loops, arches, and whorls in each pattern. After capturing the print, sophisticated algorithms use the image to produce a unique digital biometric template. The template is then compared to new or existing scans to either confirm or deny a match.***   1. ***Facial Recognition***   ***Facial recognition software measures the geometry of the face, including the distance between the eyes, the distance from the chin to the forehead, and multiple other points on a person’s face. After collecting the data, an advanced algorithm transforms it into an encrypted facial signature.***   1. ***Iris Recognition***   ***Physically speaking, the shape of a person’s vocal tract, including the nose, mouth, and larynx determines the sound produced. Behaviorally, the way a person says something – movement variations, tone, pace, accent, and so on – is also unique to each individual. The most important properties used for speech authentication are nasal tone, fundamental frequency, inflection, cadence. Combining data from both physical and behavioral biometrics creates a precise voiceprint.***   1. ***Retina Scan***   ***In the human eye, the iris is the colored portion in the shape of a ring. If you look closely, you will find it is made of many asymmetric thick thread-like structures. These thread-like structures are the muscles that help adjust shape of the pupil and only allow appropriate amount of light in the eye. By measuring the unique folds of these muscles, biometric authentication tools can confirm identity with incredible accuracy. Liveness detection – like requiring a user to blink for the scan – adds an additional layer of accuracy and security.***   1. ***Signature Recognition***   ***Signature recognition is one type of biometric method used to analyze the physical activity of signing by measuring special coordinates such as pen pressure, stroke order, inclination, and speed. A measurements are digitally recorded, then that information is used to automatically create a biometric profile for future authentication.***   1. ***Keystroke Dynamics***   ***Keystroke dynamics leverage the fact that people follow a definite pattern while typing on a keyboard or keypad. Their keystroke rhythm can be used to establish a biometric profile, which can be used to identify or authenticate him/her. Time taken to press each key, pause between key presses, letters typed per second/minute, and several other measures are taken to generate a keystroke profile of a user. When added with keystroke dynamics, password-based security can improve multifold without introducing any more complexity.***  ***Reference:*** NICE Systems. 2020. *Understanding The Types Of Biometrics | NICE*. [online] Available at: <https://www.nice.com/engage/blog/rta-understanding-the-types-of-biometrics-2513/> [Accessed 11 November 2020]. |

1. Summarise the following terms associated with digital certificates.
2. VeriSign
3. SSL
4. X.509

Write your answer in 100-150 words for each blow.

|  |
| --- |
| 1. ***VeriSign***   ***Verisign, a global provider of domain name registry services and internet infrastructure, enables internet navigation for many of the world’s most recognized domain names. Verisign enables the security, stability, and resiliency of key internet infrastructure and services, including providing root zone maintainer services, operating two of the 13 global internet root servers, and providing registration services and authoritative resolution for the .com and .net top-level domains, which support the majority of global e-commerce.*** |
| 1. ***SSL***   ***SSL stands for Secure Sockets Layer, a global standard security technology that enables encrypted communication between a web browser and a web server. It is utilized by millions of online businesses and individuals to decrease the risk of sensitive information (e.g., credit card numbers, usernames, passwords, emails, etc.) from being stolen or tampered with by hackers and identity thieves. In essence, SSL allows for a private “conversation” just between the two intended parties.***  ***To create this secure connection, an SSL certificate (also referred to as a “digital certificate”) is installed on a web server and serves two functions:***   * ***It authenticates the identity of the website.*** * ***It encrypts the data that’s being transmitted.***   ***Reference:*** Verisign.com. 2020. *What Is An SSL Certificate? – Verisign*. [online] Available at: <https://www.verisign.com/en\_US/website-presence/online/ssl-certificates/index.xhtml> [Accessed 11 November 2020]. |
| 1. ***X.509***   ***An X.509 certificate is a vital safeguard against malicious network impersonators. Without x.509 server authentication, man-in-the-middle attacks can be initiated by malicious access points, compromised routers, etc.***  ***X.509 is most used for SSL/TLS connections to ensure that the client (e.g., a web browser) is not fooled by a malicious impersonator pretending to be a known, trustworthy website.***  ***However, X.509 certificates secure network communications of all kinds:***   * ***Securing Internet Communication*** * ***Securing Intranet Communication*** * ***Securing email communication*** * ***Securing device communication***   ***X.509 does not define how certificate contents should be encoded to store in files. However, two commonly used encoding schemas are used to store X.509 certificates in files, DER and PEM.***  ***DER (Distinguished Encoding Rules) is a data object encoding schema that can be used to encode certificate objects. DER is the most popular file format to store X.509 certificates. DER-encoded certificates are binary files and cannot be read by text editors, but they can be processed by web browsers and some applications without any problems.***  ***PEM (Privacy Enhanced Mail) is an encrypted email encoding schema that can be used to convert DER-encoded certificates into text files.***  ***Reference:*** Yackel, R., 2020. *What Is An X.509 Certificate? | Keyfactor*. [online] Blog.keyfactor.com. Available at: <https://blog.keyfactor.com/what-is-x509-certificate> [Accessed 11 November 2020]. |

1. What are the functions and operations of the following authentication controls? Write your response in 100-150 words for each of the following.
2. Passwords
3. Personal identification numbers (PINs)
4. Smart Cards
5. Biometric devices

|  |
| --- |
| 1. ***Passwords***   ***Passwords are the most common way for your organisation and the people in it to prove identity when banking, making purchases and other transactional online activities, accessing services, using email and accessing computers themselves (via User Accounts). The use of strong passwords and their secrecy is therefore vital in order to protect the organisation's and individuals’ security and identity. The best security in the world is useless if a malicious or other unauthorised person has a legitimate user name and password. However, the generation and use of passwords can be a complex issue - and there are not hard and fast rules which necessarily apply across different business scenarios.***  ***For this reason, password protocol and control should be a key part of your organisation’s cyber and information security strategy.***  ***Passwords are commonly used in conjunction with usernames. However, on secure sites they may also be used alongside other methods of identification such as a separate PIN and/or memorable information or characters generated by an electronic token or keypad (called multi-factor authentication). In some cases, websites request entry of only certain password characters for additional security.***  ***Reference:*** Getsafeonline.org. 2020. *Get Safe Online*. [online] Available at: <https://www.getsafeonline.org/online-safety-and-security/password-protocol-and-control/> [Accessed 11 November 2020]. |
| 1. ***Personal identification numbers(PINs)***   ***A personal identification number (PIN) is a numerical code used in many electronic financial transactions. Personal identification numbers are usually issued in association with payment cards and may be required to complete a transaction. The purpose of a personal identification number (PIN) is to add additional security to the electronic transaction process.***  ***Personal identification numbers provide additional security on an account and are most commonly used with debit cards linked to a person’s bank account. When a person is issued a debit card, they are required to choose a unique personal identification number (PIN) that they will need to enter every time they wish to withdraw money from an ATM and oftentimes when they make payments at various merchant stores.***  ***As PINs are like passwords, they are also used in many other instances, such as home security and mobile phones. A PIN is basically any numerical method used to verify an individual's identity.***  ***Reference:*** Investopedia. 2020. *Personal Identification Number (PIN)*. [online] Available at: <https://www.investopedia.com/terms/p/personal-identification-number.asp> [Accessed 11 November 2020]. |
| 1. ***Smart Cards***   ***A smart card is a secure microcontroller that is typically used for generating, storing and operating on cryptographic keys. Smart card authentication provides users with smart card devices for the purpose of authentication. Users connect their smart card to a host computer. Software on the host computer interacts with the keys material and other secrets stored on the smart card to authenticate the user.***  ***In order for the smart card to operate, a user needs to unlock it with a user-PIN.Smart cards are considered a very strong form of authentication because cryptographic keys and other secrets stored on the card are very well protected both physically and logically, and are therefore extremely hard to steal.***  ***The added security provided by the smart card comes at the expense of the user experience, as smart cards need to be physically carried around by the user and inserted into the host computer every time they want to authenticate with it. Users are also limited to host devices that have the card interface software installed.Smart cards are also expensive to administrate, as they require software installation on the host computer and physical distribution to the users.***  ***Reference:*** Secret Double Octopus. 2020. *What Is Smart Card Authentication ? | Security Wiki*. [online] Available at: <https://doubleoctopus.com/security-wiki/authentication/smart-card-authentication/> [Accessed 11 November 2020]. |
| 1. ***Biometric Devices***   ***Biometric authentication is a form of security that measures and matches biometric features of a user to verify that a person trying to access a particular device is authorized to do so. Biometric features are physical and biological characteristics that are unique to an individual person and can be easily compared to authorized features saved in a database. If the biometric features of a user trying to access a device match the features of an approved user, access to the device is granted. Biometric authentication can also be installed in physical environments, controlling access points like doors and gates.***  ***Common types of biometric authentication are increasingly being built into consumer devices, especially computers and smartphone. Biometric authentication technologies are also being used by governments and private corporations in secure areas, including at military bases, in airports, and at ports of entry when crossing national borders.***  ***Reference:*** TransUnion. 2020. *Biometric Authentication | What Is Biometric Authentication?*. [online] Available at: <https://www.iovation.com/topics/biometric-authentication> [Accessed 11 November 2020]. |

1. Explain the function and operation of the following authentication protocols. Explain each in 100-150 words.
2. Secure Remote Password protocol
3. Protocol for Carrying Authentication for Network Access
4. Password-authenticated key agreement

|  |
| --- |
| 1. ***Secure Remote Password Protocol***   ***The Secure Remote Password protocol (SRP) is a cryptographically strong authentication protocol for password-based, mutual authentication over an insecure network connection. Successful SRP authentication requires both sides of the connection to have knowledge of the user’s password. In addition to password verification, the SRP protocol also performs a secure key exchange during the authentication process. This key may be used to protect network traffic via symmetric key encryption.***  ***SRP offers security and deployment advantages over other challenge-response protocols, such as Kerberos and SSL, in that it does not require trusted key servers or certificate infrastructures. Instead, small verification keys derived from each user’s password are stored and used by each SRP server application. SRP provides a near-ideal solution for many applications requiring simple and secure password authentication that does not rely on an external infrastructure.***  ***Another favorable aspect of the SRP protocol is that compromized verification keys are of little value to an attacker. Possesion of a verification key does not allow a user to be impersonated and it cannot be used to obtain the users password except by way of a computationally infeasible dictionary attack. A compromized key would, however, allow an attacker to impersonate the server side of an SRP authenticated connection. Consequently, care should be taken to prevent unauthorized access to verification keys for applications in which the client side relies on the server being genuine.***  ***Reference:*** Pythonhosted.org. 2020. *Srp — Secure Remote Password — Secure Remote Password 1.0.5 Documentation*. [online] Available at: <https://pythonhosted.org/srp/srp.html> [Accessed 11 November 2020]. |
| 1. ***Protocol for Carrying Authentication for Network Access***   ***PANA (Protocol for Carrying Authentication for Network Access) is an IP-based protocol that allows a device to authenticate itself with a network to be granted access. PANA will not define any new authentication protocol, key distribution, key agreement or key derivation protocols. For these purposes, the Extensible Authentication Protocol (EAP) will be used, and PANA will carry the EAP payload. PANA allows dynamic service provider selection, supports various authentication methods, is suitable for roaming users, and is independent from the link layer mechanisms.***  ***Architecture’s Element of PANA:***   * ***PaC (PANA Client): The PaC is the client part of the protocol. This element is located in the node that wants to reach the access network.*** * ***PAA (PANA Authentication Agent): This entity represents the server part of the PANA protocol. Its main task is the message exchange with the PaC for authenticating and authorizing it for network access. In addition, in some scenarios, the PAA entity has to do other message exchange with the AAA server in order to offer the PaC credentials to it. In this case, EAP is configured as pass-through and the AAA server is placed physically in a different place than the PAA.*** * ***AS (Authentication Server): This element contains the information needed to check the PaC's credentials. To this end this node receives the PaC's credentials from the PAA, performs a credential check, and sends a packet with the result of the credential check. If the credential check was successful, that packet contains access parameters, such as allowed bandwidth or IP configuration. At this point, a session between PAA and PaC has been established. This session has a session lifetime. When the session expires, a re-authentication process is required for the PaC to regain network access.*** * ***EP (Enforcement Point): It works as a filter of the packets which source is an authenticated PaC. Basically, an EP is a network node which drops packets according to some parameters provided as results of the authentication processes. Typically, this function is applied by a communication device as an access point or a router. When an authentication process is done successfully, a key is installed in EP and PaC, establishing a session between EP and PaC. While this session is active (hasn't expired), the PaC can access network services for which it has been authorised. When the session expires, the PaC will have to indicate this situation to the PAA in order to perform re-authentication.*** |
| 1. ***Password-authenticated key agreement***   ***In cryptography, a password-authenticated key agreement method is an interactive method for two or more parties to establish cryptographic keys based on one or more party's knowledge of a password.***  ***An important property is that an eavesdropper or man in the middle cannot obtain enough information to be able to brute force guess a password without further interactions with the parties for each (few) guesses. This means that strong security can be obtained using weak passwords.***  ***Password-authenticated key agreement generally encompasses methods such as:***   * ***Balanced password-authenticated key exchange*** * ***Augmented password-authenticated key exchange*** * ***Password-authenticated key retrieval*** * ***Multi-server methods*** * ***Multi-party methods*** |

1. Explain the following network authentication services each in 150-200 words.
2. Kerberos
3. NTLM - NT LAN Manager

|  |
| --- |
| 1. ***Kerberos***   ***Kerberos authentication is currently the default authorization technology used by Microsoft Windows, and implementations of Kerberos exist in Apple OS, FreeBSD, UNIX, and Linux.***  ***Microsoft introduced their version of Kerberos in Windows2000. It has also become a standard for websites and Single-Sign-On implementations across platforms. The Kerberos Consortium maintains Kerberos as an open-source project.***  ***Kerberos is a vast improvement on previous authorization technologies. The strong cryptography and third-party ticket authorization make it much more difficult for cybercriminals to infiltrate your network. It is not totally without flaws, and in order to defend against those flaws, you need to first understand them.***  ***Kerberos has made the internet and its denizens more secure, and enables users to do more work on the Internet and in the office without compromising safety. It uses third party verification and strong encryption capability.***  ***Reference:*** Inside Out Security. 2020. *Kerberos Authentication Explained*. [online] Available at: <https://www.varonis.com/blog/kerberos-authentication-explained/> [Accessed 11 November 2020]. |
| 1. ***NTLM - NT Lan Manager***   ***Windows NT LAN Manager (NTLM) is a challenge-response authentication protocol used to authenticate a client to a resource on an Active Directory domain. When the client requests access to a service associated with the domain, the service sends a challenge to the client, requiring that the client to perform a mathematical operation using its authentication token, and then return the result of this operation to the service. The service may validate the result or send it to the Domain Controller (DC) for validation. If the service or DC confirm that the client’s response is correct, the service allows access to the client.***  ***NTLM is a type of single sign-on (SSO) because it allows the user to provide the underlying authentication factor only once, at login.***  ***The NTLM protocol suite is implemented in a Security Support Provider (SSP), a Win32 API used by Microsoft Windows systems to perform a variety of security-related operations such as authentication. The NTLM protocol suite includes LAN Manager authentication protocol, NTLMv1, NTLMv2 and NTLM2 Session protocols.***  ***Reference:*** Secret Double Octopus. 2020. *What Is NT LAN Manager (NTLM) | Security Wiki*. [online] Available at: <https://doubleoctopus.com/security-wiki/protocol/nt-lan-manager/> [Accessed 11 November 2020]. |

1. Summarise the features of the following protocols using 150-200 words for each protocol.
2. CHAP- Challenge-Handshake Authentication Protocol
3. Challenge–Phrase authentication
4. Password Authentication Protocol (PAP)
5. RADIUS (Remote Authentication Dial-In User Service)

|  |
| --- |
| 1. ***Challenge Handshake Authentication Protocol (CHAP) is a Point-to-point protocol (PPP) authentication protocol developed by IETF (Internet Engineering Task Force). It is used at the initial startup of the link. Also, it performs periodic checkups to check if the router is still communicating with the same host. Features of CHAP are listed below:***  * ***It uses 3-way handshaking protocol (not like TCP). First, the authenticator sends a challenge packet to the peer then, the peer responds with a value using its one way hash function. The authenticator then matches the received value with its own calculated hash value. If the values match then the authentication is acknowledged otherwise, the connection will be terminated.*** * ***It uses one-way hash function called MD5.*** * ***It also authenticates periodically to check if the communication is taking place with the same device or not.*** * ***Also, it provides more security than PAP (Password Authentication Procedure) as the value used (find out by hash function) is changed variably.*** * ***CHAP requires to know the plaintext of the secret as it is never sent over the network.***   ***Reference:*** GeeksforGeeks. 2020. *Challenge Handshake Authentication Protocol (CHAP) - Geeksforgeeks*. [online] Available at: <https://www.geeksforgeeks.org/challenge-handshake-authentication-protocol-chap/> [Accessed 10 November 2020]. |
| 1. ***Challenge Phrase Authentication***   ***Challenge-response authentication is a group or family of protocols characterized by one entity sending a challenge to another entity. The second entity must respond with the appropriate answer to be authenticated.***  ***A simple example of this is password authentication. The challenge is from a server asking the client for a password to authenticate the client's identity so that the client can be served.***  ***Most smart card systems use challenge-response authentication. These systems require at least two things for authentication and entry: the smart card and the user’s password.***  ***Another challenge-response authentication example is the use of CAPTCHA, a form of reverse-Turing test for the system to determine if the client is a human or not. This is used to prevent spam and auto-registration of new accounts for a website or email.***  ***Biometric systems are another form of challenge-response authentication.***  ***In cryptography, zero-knowledge password proof and key agreement systems such as secure remote password, CRAM-MD5 and secure shell's challenge-response system based on RSA are considered to be very sophisticated challenge-response algorithms.***  ***Reference:*** Techopedia.com. 2020. *What Is Challenge-Response Authentication? - Definition From Techopedia*. [online] Available at: <https://www.techopedia.com/definition/26138/challenge-response-authentication> [Accessed 11 November 2020]. |
| 1. ***Password Authentication Protocol***   ***There are simply two methods to authenticate PPP links namely Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP).***  ***From these two authentication protocols, PAP is less secured as the password is sent in clear text and is performed only at the initial link establishment.***  ***PAP is a password Authentication Protocol used by PPP links to validate users. PAP authentication requires the calling device to enter the username and password. If the credentials match with the local database of the called device or in the remote AAA database then it is allowed to access otherwise denied.***  ***Features of PAP are:***   * ***The password is sent in a clear text*** * ***All network os supports PAP*** * ***It uses two-way handshake protocol*** * ***It is non-interactive*** * ***PAP supports both one-way authentication and two-way authentication***   ***Reference:*** GeeksforGeeks. 2020. *Password Authentication Protocol (PAP) - Geeksforgeeks*. [online] Available at: <https://www.geeksforgeeks.org/password-authentication-protocol-pap/> [Accessed 11 November 2020]. |
| 1. ***RADIUS (Remote Authentication dial-in User Service)***   ***Remote Authentication Dial-In User Service (RADIUS) is a network protocol that provides security to networks against unauthorized access. RADIUS secures a network by enabling centralized authentication of dial-in users and authorizing their access to use a network service. It manages remote user authentication, authorization and accounting (AAA).***  ***RADIUS is used by many companies to enable roaming between Internet service providers (ISPs), providing a single global set of credentials to be used on any public network. It is also used by independent or collaborating companies, which provide their own credentials to their own service users.***  ***RADIUS supports maintaining company user profiles in a central database, where all remote servers connected to the central server are able to share the information. RADIUS is most widely used by Internet service providers and business enterprises because of its ubiquitous nature and broad support. It is used to authenticate access to internal and wireless networks and other integrated email services. These networks may use modems, virtual private network ports, Web servers, digital subscriber line (DSL), etc.***  ***RADIUS performs three major functions:***   * ***Authenticates users trying to establish a connection to a network*** * ***Authorizes users to access requested network services*** * ***Accounts for the use of those services***   ***Reference:*** Techopedia.com. 2020. *What Is Remote Authentication Dial-In User Service (RADIUS)? - Definition From Techopedia*. [online] Available at: <https://www.techopedia.com/definition/4079/remote-authentication-dial-in-user-service-radius> [Accessed 11 November 2020]. |

1. What are the principles of security tokens? Write your response in 150-200 words.

|  |
| --- |
| ***In a heterogeneous environment, Web services need to authenticate service clients to control their access by using WS-Security (Web Services security). When negotiating trust between service clients and service providers, an authentication broker can provide a common access control infrastructure for a group of applications. Typically, the authentication broker issues signed security tokens which are used by clients to authenticate themselves at the service.***  ***The Security Token Service is a service for providing such an authentication broker. It issues Security Tokens based on the WS-Trust, a standardized specification of Web services based on WS-Security.***  ***This is useful, for example, to establish a trust relationship between a client and a web service, particularly if they are in different security domains. The Security Token Service is used to issue a security token, that is, a collection of claims such as name, role, and authorization code, for the client to access the service. The message receiver only must know the STS certificate for verifying the token signature to get a trusted statement of the authentication information.***  ***Reference:*** Help.talend.com. 2020. *Welcome To Talend Help Center*. [online] Available at: <https://help.talend.com/reader/rwAmGFpbp18KiKuckiP4Zw/MDauhq9nl1m0FXZX~aHp9Q> [Accessed 10 November 2020]. |

1. Briefly explain five (5) authentication options that can be analysed as per the user and enterprise requirements? Write 30-70 words for each option.

|  |
| --- |
| ***In the past few years, we’ve seen that even the biggest companies are not immune to security breaches. Big wigs like LinkedIn, Target, Home Depot and Sony Pictures have had their systems hacked into, revealing sensitive information of their owners, employees, and clients. With millions of passwords, email addresses and more having been exposed, there has been an increase in pressure on those who handle enterprise security to up their defenses.***  ***Since it is difficult to keep up with how quickly the cyber-criminals can advance their knowledge of systems, network administrators have been facing plenty of challenges and had to start implementing more sophisticated ways of authenticating users. Below we discuss common authentication methods used for network security to beat the savvy cyber-crooks:***   1. ***Biometrics for Network Security***   ***The term “biometrics” literally translates to the term “measuring life”. Biometrics also refers to using the known and documented physical attributes of a user to authenticate their identity. This is ideal since no two people share the exact same physical traits. Common biometric authentication methods include fingerprint identification, voice recognition, retinal and iris scans and face scanning and recognition. The downside to this method is that it requires specialized scanning equipment, which is not ideal for some industries.***   1. ***Token Authentication***   ***A token is a material device that is used to access secure systems. Common forms include a dongle, card or RFID chip. A token makes it more difficult for a hacker to access an account since they must have long credentials and the tangible device itself, which is much harder for a hacker to obtain.***   1. ***Transaction Authentication***   ***Transaction authentication seeks out reasonable mistakes when comparing known data about a user with the details of a current transaction. An example would be if an individual lives in the United States, but large purchases show up while logged in from an IP address overseas. A red flag is sent up, and this cause for concern requires more verification steps to ensure that the purchase is legitimate and that the user is not a victim of a cyber-crime.***   1. ***Multi-Factor Authentication***   ***MFA is an authentication design that requires two or more independent ways of verifying identity. Examples include something that the user possesses such as a telephone or other physical token, inherent factors like biometric traits or something known like a password. ATM’s are prime examples of MFAs because you need a card (physical token) and a PIN (something known) in order for the transaction to take place.***   1. ***Out-of-Band Authentication***   ***OOB utilizes totally separate channels, like mobile devices, to authenticate transactions that originated on a computer. Any transaction that requires deposits from one place to another, like a large money transfer, would generate a phone call, text or notification on an app that there is more authentication required for the transaction to be completed. With two necessary channels, it is much more difficult for a hacker to steal money.***  ***Reference:*** Alliance Technology Partners. 2020. *Common Authentication Methods Used For Network Security*. [online] Available at: <https://www.alliancetechpartners.com/common-authentication-methods-used-network-security/> [Accessed 10 November 2020]. |

1. What is the difference between the authentication and the authorisation process? Write your response in 100-150 words for each.

|  |
| --- |
| ***Both the terms are often used in conjunction with each other in terms of security, especially when it comes to gaining access to the system. Both are very crucial topics often associated with the web as key pieces of its service infrastructure. However, both the terms are very different with totally different concepts. While it’s true that they are often used in the same context with the same tool, they are completely distinct from each other.***  ***Authentication means confirming your own identity, while authorization means granting access to the system. In simple terms, authentication is the process of verifying who you are, while authorization is the process of verifying what you have access to.***   1. ***Authentication***   ***Authentication is about validating your credentials like User Name/User ID and password to verify your identity. The system determines whether you are what you say you are using your credentials. In public and private networks, the system authenticates the user identity via login passwords. Authentication is usually done by a username and password, and sometimes in conjunction with factors of authentication, which refers to the various ways to be authenticated.***  ***Authentication factors determine the various elements the system use to verify one’s identity prior to granting him access to anything from accessing a file to requesting a bank transaction. A user’s identity can be determined by what he knows, what he has, or what he is. When it comes to security, at least two or all the three authentication factors must be verified in order to grant someone access to the system.***   1. ***Authorization***   ***Authorization, on the other hand, occurs after your identity is successfully authenticated by the system, which ultimately gives you full permission to access the resources such as information, files, databases, funds, locations, almost anything. In simple terms, authorization determines your ability to access the system and up to what extent. Once your identity is verified by the system after successful authentication, you are then authorized to access the resources of the system.***  ***Authorization is the process to determine whether the authenticated user has access to the particular resources. It verifies your rights to grant you access to resources such as information, databases, files, etc. Authorization usually comes after authentication which confirms your privileges to perform. In simple terms, it’s like giving someone official permission to do something or anything.***  ***Reference:*** Khillar, S., 2020. *Difference Between Authentication And Authorization | Difference Between*. [online] Differencebetween.net. Available at: <http://www.differencebetween.net/technology/difference-between-authentication-and-authorization/> [Accessed 10 November 2020]. |

1. What is authentication realm? Write your response in 100-150 words.

|  |
| --- |
| ***An authentication realm is a grouping of authentication resources, including:***   1. ***An authentication server, which verifies a user’s identity. The system forwards credentials submitted on a sign-in page to an authentication server.*** 2. ***An authentication policy, which specifies realm security requirements that need to be met before the system submits credentials to an authentication server for verification.*** 3. ***A directory server, which is an LDAP server that provides user and group attribute information to the system for use in role mapping rules and resource policies (optional).*** 4. ***Role mapping rules, which are conditions a user must meet for the system to map a user to one or more roles. These conditions are based on information returned by the realm's directory server, the person’s username, or certificate attributes.***   ***Reference:*** Docs.pulsesecure.net. 2020. *Defining An Authentication Realm*. [online] Available at: <https://docs.pulsesecure.net/WebHelp/PCS/9.1R4/AG/Content/PCS/PCS\_AdminGuide/Defining\_an\_Authentication\_1.htm> [Accessed 10 November 2020]. |

1. Explain the creation of the authentication realm including the process of adding the users and defining the rules of the realm. Write your response in 200-250 words.

|  |
| --- |
| ***An authentication realm is a grouping of authentication resources, including:***  ***An authentication server, which verifies a user’s identity. The system forwards credentials submitted on a sign-in page to an authentication server.***  ***An authentication policy, which specifies realm security requirements that need to be met before the system submits credentials to an authentication server for verification.***  ***A directory server, which is an LDAP server that provides user and group attribute information to the system for use in role mapping rules and resource policies (optional).***  ***Role mapping rules, which are conditions a user must meet for the system to map a user to one or more roles. These conditions are based on information returned by the realm's directory server, the person’s username, or certificate attributes.***  ***Your system is preconfigured with one user realm called “Users.” This predefined realm uses the System Local authentication server, an authentication policy that requires a minimum password length of four characters, no directory server, and contains one role mapping rule that maps all users who sign in to the Users realm to the Users role. The “testuser1” account you created is part of the Users realm, because this account is created in the System Local authentication server. The “testuser2” account you created is not part of the Users realm, because you create the user account in the new “Test Server” authentication server, which is not used by the Users realm.***  ***You can view the default user authentication realm on the User Authentication Realms page.***  ***To define an authentication realm:***   1. ***In the admin console, choose User> User Realms*** 2. ***Click New*** 3. ***Enter Test Realm in the Name box*** 4. ***Select test server from authentication list*** 5. ***Click Save Changes*** 6. ***Click the role mapping tap if it is not already selected, and click new rule.*** 7. ***Enter testuser2 in the text box*** 8. ***Under ‘then assign these roles’, select test role from the available roles list and click add to move it to the selected roles box.*** 9. ***Click save changes.***   ***After completing these steps, you have finished creating an authentication realm.***  ***Reference:*** Docs.pulsesecure.net. 2020. *Defining An Authentication Realm*. [online] Available at: <https://docs.pulsesecure.net/WebHelp/PCS/9.0R1/Content/PCS/PCS\_AdminGuide\_9.0/Defining\_an\_Authentication\_1.htm> [Accessed 10 November 2020]. |

1. What is user attributes? Summarise the setup of user attributes.

Write your response in 150-200 words.

|  |
| --- |
| ***User Attributes are facts about your users taken from your site’s data that you can use to more quickly gain insight into the behavior and needs of the users who matter most to your business.***  ***Once enabled, User Attributes allow you to filter Recordings, and target feedback widgets by these values. They also allow you to lookup and delete user data by user ID making it easy to respect your user's privacy rights - which is especially important when passing personal information to Hotjar.***  ***Setup process of user attributes:***   1. ***Decide on the user attributes most relevant to your business***   ***You should start by assessing what data from your own site's database you want to send to Hotjar as User Attributes.***   1. ***Review your privacy requirements***   ***Hotjar is designed to help you anonymize data as much as possible by default, making it easy to conform with privacy legislation such as the GDPR without having to undergo too much extra work.***   1. ***Enable user attributes and implement the code using hotjar’s identify API***   ***The ability to send User Attributes to Hotjar will be disabled until you have enabled them in your User Attributes page and successfully added/written the User Attribute code.***   1. ***Start using user attributes in hotjar***   ***Once you have enabled User Attributes, and your developer has implemented the code necessary to send data to Hotjar, you will start seeing them appear in the User Attributes management page.***  ***Reference:*** Hotjar Documentation. 2020. *How To Setup User Attributes In 4 Steps*. [online] Available at: <https://help.hotjar.com/hc/en-us/articles/360038394053-How-to-Setup-User-Attributes-in-4-Steps> [Accessed 10 November 2020]. |

1. What is meant by authentication filters and what is the process for setting one up? Write your response in 50-100 words.

|  |
| --- |
| ***Authentication filters are an integral part of ASP.Net programming. These filters authenticate any type of HTTP request that is sent out of your program or computer. Authentication filters are supported by both web based API as well as MVC 5. You can set authentication tasks for individual controllers as well as actions on your file or folder. You can allow your app to support the various authentications that are conducted in different manners.***  ***You can setup the authentication filters individually for the various controllers, or you can setup the whole thing for a particular web based API. If you wish to create an authentication filter for a single controller then you will need to base out the following code along with the [IdentityBasisAuthentication] filter applied on the controller class.***  ***If you want to apply the authentication filter for a single controller action, add the action to the filter.***  ***Reference:*** Qarea.com. 2020. [online] Available at: <https://qarea.com/blog/authentication-filters-asp-net> [Accessed 10 November 2020]. |

1. Explain three (3) different types of authentication methods to be developed and distributed to users as per the business requirements? Write your response in 200-250 words.

|  |
| --- |
| ***Authentication is the process of identifying users that request access to a system, network, or device. Access control often determines user identity according to credentials like username and password. Other authentication technologies like biometrics and authentication apps are also used to authenticate user identity.***  ***Some of the authentication for users are listed below:***   1. ***Password Based Authentication***   ***Passwords are the most common methods of authentication. Passwords can be in the form of a string of letters, numbers, or special characters. To protect yourself you need to create strong passwords that include a combination of all possible options.***  ***However, passwords are prone to phishing attacks and bad hygiene that weakens effectiveness. An average person has about 25 different online accounts, but only 54% of users use different passwords across their accounts.***  ***The truth is that there are a lot of passwords to remember. As a result, many people choose convenience over security. Most people use simple passwords instead of creating reliable passwords because they are easier to remember.***  ***The bottom line is that passwords have a lot of weaknesses and are not sufficient in protecting online information. Hackers can easily guess user credentials by running through all possible combinations until they find a match.***   1. ***Multi-factor Authentication***   ***Multi-Factor Authentication (MFA) is an authentication method that requires two or more independent ways to identify a user. Examples include codes generated from the user’s smartphone, Captcha tests, fingerprints, or facial recognition.***  ***MFA authentication methods and technologies increase the confidence of users by adding multiple layers of security. MFA may be a good defense against most account hacks, but it has its own pitfalls. People may lose their phones or SIM cards and not be able to generate an authentication code.***   1. ***Certificate-based Authentication***   ***Certificate-based authentication technologies identify users, machines or devices by using digital certificates. A digital certificate is an electronic document based on the idea of a driver’s license or a passport.***  ***The certificate contains the digital identity of a user including a public key, and the digital signature of a certification authority. Digital certificates prove the ownership of a public key and issued only by a certification authority.***  ***Users provide their digital certificates when they sign in to a server. The server verifies the credibility of the digital signature and the certificate authority. The server then uses cryptography to confirm that the user has a correct private key associated with the certificate.***  ***Reference:*** ID R&D. 2020. *User Authentication Methods & Technologies To Prevent Breach*. [online] Available at: <https://www.idrnd.ai/5-authentication-methods-that-can-prevent-the-next-breach/> [Accessed 10 November 2020]. |

1. What are the responsibilities of the users on the authentication system relevant to the enterprise security plan? Write your response in 100-150 words.

|  |
| --- |
| ***The Enterprise Authentication, Authorization and Access policy describes a fully integrated method for verifying the identity of all persons in the university community, granting access to Institutional Data and securing physical devices allowed to access that data.***  ***Authentication is the mechanism that verifies that an individual is who they claim to be. Verification shall be based on one of more of the following (depending on security requirements):***   1. ***Knowledge ( e.g. password, PIN)*** 2. ***Possession (e.g. smart card, smart phone, security fob)*** 3. ***Inherence (e.g. fingerpring, retinal scan)***   ***Enterprise level directories provide the authentication infrastructure to improve the user and IT provider experience. Data in the authentication directory is fed from authoritative sources, making the data dependable and available for decisions. Central authentication makes the login process uniform for the user and allows the provider to concentrate on the specifics of their service. Enterprise authentication offers opportunities for services beyond the campus boundaries, where appropriate, for activities such as student recruiting, patient care or alumni relationship services.***  ***Some of the responsibilities of users on the authentication system relevant to the enterprise level are listed below as :***   1. ***Users should user computers and information systems in a ethical and legal manner.*** 2. ***Users agree not to duplicate or user copyrighted or proprietary software without proper authorization.*** 3. ***Users are required to acknowledge the user of NCAR resources.***   ***Reference:*** Itsecurity.uiowa.edu. 2020. *Enterprise Authentication, Authorization, And Access Policy | IT Security & Policy Office*. [online] Available at: <https://itsecurity.uiowa.edu/enterprise-authentication> [Accessed 10 November 2020]. |

1. Summarise three (3) benefits of recording and storing permission and configuration information in a secure central location. Write your response in 150-250 words.

|  |
| --- |
| ***Many companies will keep their respective departments’ files in different locations. Whether this is out of convenience or habit will vary according to circumstance. However, what can be known is this system of filing is both inefficient and time consuming. A decentralised filing system will lead to a breakdown of organised records management and will put your businesses’ confidential information at risk.***  ***A centralised filing system actively encourages cross-referencing and collaboration between departments, and increases the efficiency of your office’s information flow. Above all, it enhances file security with files all under unitary supervision and security.***   1. ***Efficient Business Operations***   ***Decentralised filing systems often precipitate time consuming file retrieval. With files situated at different locations it becomes a far more complex task for employees to retrieve files. Employees will have to spend valuable time contacting colleagues from other departments inquiring after the location of files and will have to then rummage through these often unfamiliar storage rooms.***  ***If files are all stored in one location employees are far more likely to be familiar already with their prospective hunting ground. Employees will recurrently visit this same location and will be more familiar with the organisation and indexing of these files. This remains the case with companies storing their files in one offsite location; employees will regularly use this facility to access files and will become accustomed with its procedures for file retrieval.***   1. ***Reduced Expenditure***   ***Keeping up with the maintenance of several storage locations is likely to be expensive. Companies that use decentralised filing systems are not only more likely to using inadequate locations for document storage but are probably spending more on the preservation of multiple storage sites.***  ***A centralised filing system eliminates the need for duplication of filing equipment and corresponding security measures. Furthermore, onsite and offsite centralisation both reduce precious office space expenditure. Offsite centralised storage is likely to show the greatest return on investment. Offsite specialists are able to provide you with storage space tailored to your needs and will take on the added financial burden of maintaining secure storage facilities.***   1. ***Increased Security***   ***Having files in one location is likely to promote greater information security in your workplace. Centralised filing offers only one point of access which can be easily monitored and restricted. At any one time a company is going to be holding confidential information and a decentralised filing system could jeopardise the security of customer information. A data breach of this kind could have devastating repercussions for your company’s reputation.***  ***A centralised filing system means that there needn’t be multiple copies of files around the office in different employee’s possession. The absence of multiple copies means files are more easily tracked and protected from perpetrators. A decentralised filing system often leads to document fragmentation; without realising offices might keep duplicates of the same document in several locations. With only one central location dedicated to filing, companies are more likely to arm this location with appropriate security and staff. Heightened access controls and security standardisation are also favourable outcomes of centralisation.***  ***Reference:*** Secure Data MGT. 2020. *3 Advantages Of A Centralised Filing System - Secure Data*. [online] Available at: <https://www.securedatamgt.com/blog/centralised-filing-system-advantages/> [Accessed 10 November 2020]. |

1. List five (5) tools for ongoing network monitoring using incident management and reporting processes.

|  |
| --- |
| ***Incident Management (IcM) requires you to spot unexpected disruption in IT service and organize a resolution to the problem promptly. The field of Incident Management encompasses user support and help response, so incident management software is closely tied to service desk software functions.***  ***Some of the incident management tools are listed below:***   1. ***SolarWinds Web Help Desk***   ***Leading on-premises software to manage infrastructure and process Help Desk calls. Makes discovery and management of IT assets affordable for any size organization.***   1. ***Atera***   ***A software package for managed service providers (MSPs) with user support functions and incident logging for client service reviews.***   1. ***ManageEngine ServiceDesk Plus***   ***An extended service support system that installs on Windows and Linux.***   1. ***SolarWinds Service Desk***   ***Cloud-based Service Desk and IT Asset Management platform. Includes ticket management, knowledge base, incident logging, and self-service software platforms.***   1. ***Spiceworks Help Desk***   ***Comprehensive user support system that has incident tracking software capabilities.***  ***Reference:*** Comparitech. 2020. *6 Best Incident Management Software Tools For 2020* . [online] Available at: <https://www.comparitech.com/net-admin/best-incident-management-tools/> [Accessed 10 November 2020]. |

1. List four (4) basic security requirements in relationto an enterprise security plan.

|  |
| --- |
| ***No matter what business or industry you’re in, odds are that you’ll be a target for hackers and cybercriminals at some point in time. According to recent statistics from Accenture, there are over 130 large, enterprise-scale targeted cybersecurity breaches per year. And that number is growing at a rapid rate of 27 percent per year. Some of the basic security requirements in relationto an enterprise security plan are listed below:***   1. ***Network Security***   ***First and foremost, your enterprise security policy should cover all the critical elements necessary for assuring the protection of your IT networks and systems. The network security element to your policy should be focused on defining, analyzing, and monitoring the security of your network. It should serve to provide a strong cybersecurity posture, as well as seek to address potential gaps that would-be hackers might seek to exploit.***   1. ***Application Security***   ***The next element of application security is generally designed to thwart risks that arise out of application-based vulnerabilities. This could be anything from a third-party cloud-based application, to internally developed and executed ones. Your policy needs to define strategies to address risks associated with any applications that could potentially be exploited, with all applications in your enterprise being appropriately categorized based on how critical they are (and how sensitive the data they contain is).***   1. ***Risk Management***   ***This third element is comprised of a set of activities that are aimed at lowering the level of cyber-attack risk to what your enterprise deems to be an “acceptable level.” What that is will depend on the nature of your business, systems, and data, and it’s best to work with a trusted cybersecurity partner to understand the basics of cyber risk management to determine what’s “acceptable risk in your unique circumstance.***   1. ***Compliance Management***   ***Every enterprise has a set of compliance requirements to meet based on the industry they operate in. This could be frameworks like HIPAA for healthcare, PCI-DSS for the financial industry, or GDPR for those operating in Europe. These requirements typically include legal, regulatory, and certification requirements that need to be addressed in your EISP. Legal requirements also include contractual requirements. Your policy needs to identify all legal requirements and outline a program that meets all of those needs. Compliance, in fact, should be treated as another form of risk in your policy. Compliance management is usually done by your legal team, who will need to reach out to (and work with) IT and security teams to make sure all compliance-related policies are in alignment with what’s legally required.***  ***Reference:*** RSI Security. 2020. *Key Elements Of An Enterprise Information Security Policy | RSI Security*. [online] Available at: <https://blog.rsisecurity.com/key-elements-of-an-enterprise-information-security-policy/> [Accessed 10 November 2020]. |

# **Unit Assessment Result Sheet (UARS)**

## **Assessment Task 1 – Unit Knowledge Test (UKT)**

## **Student and Trainer/Assessor Details**

|  |  |
| --- | --- |
| **Unit code** | ICTNWK503 |
| **Unit name** | Install and maintain valid authentication processes |
| **Outcome of Unit Assessment Task (UAT)** | |  | | --- | | **First attempt:** |   Outcome (please make sure to tick the correct checkbox):  Satisfactory (S) ☐ or Not Satisfactory (NS) ☐  Date: \_\_\_\_\_\_\_(day)/ \_\_\_\_\_\_\_(month)/ \_\_\_\_\_\_\_\_\_\_\_\_(year)   |  | | --- | | **Second attempt:** |   Outcome (please make sure to tick the correct checkbox):  Satisfactory (S) ☐ or Not Satisfactory (NS) ☐  Date: \_\_\_\_\_\_\_(day)/ \_\_\_\_\_\_\_(month)/ \_\_\_\_\_\_\_\_\_\_\_\_(year) |
| **Feedback to Student** | |  | | --- | | * **First attempt:** |  |  | | --- | | * **Second attempt:** | |
| **Student Declaration** | * I declare that the answers I have provided are my own work. Where I have accessed information from other sources,I have provided references and or links to my sources. * I have kept a copy of all relevant notes and reference material that I used as part of my submission. * I have provided references for all sources where the information is not my own. I understand the consequences of falsifying documentation and plagiarism. I understand how the assessment is structured. I accept that all work I submit must be verifiable as my own. * I understand that if I disagree with the assessment outcome, I can appeal the assessment process, and either re-submit additional evidence undertake gap training and or have my submission re-assessed. * All appeal options have been explained to me. |
| **Student Signature** |  |
| **Date** |  |
| **Trainer/Assessor Name** |  |
| **Trainer/Assessor Declaration** | I hold:  🗹 Vocational competencies at least to the level being delivered  🗹 Current relevant industry skills  🗹 Current knowledge and skills in VET, *and undertake*  🗹 Ongoing professional development in VET  *I declare that I have conducted an assessment of this candidate’s submission. The assessment tasks were deemed current, sufficient, valid and reliable. I declare that I have conducted a fair, valid, reliable, and flexible assessment. I have provided feedback to the above-named candidate.* |
| **Trainer/Assessor Signature** |  |
| **Date** |  |
| **Office Use Only** | Outcome of Assessment has been entered onto the Student Management System on \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (insert date)  by (insert Name) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

**Unit Pre-Assessment Checklist (UPAC)**

# **UAT 2 – Unit Project (UP)**

## **Purpose of the checklist**

The pre-assessment checklist helps students determine if they are ready for assessment. The trainer/assessor must review the checklist with the student before the student attempts the assessment task. If any items of the checklist are incomplete or not clear to the student, the trainer/assessor must provide relevant information to the student to ensure they understand the requirements of the assessment task. The student must ensure they are ready for the assessment task before undertaking it.**Section 1: Information for Students**

* Please make sure you have completed the necessary prior learning before attempting this assessment.
* Please make sure your trainer/assessor clearly explained the assessment process and tasks to be completed.
* Please make sure you understand what evidence is required to be collected and how.
* Please make sure you know your rights and the Complaints and Appeal process.
* Please make sure you discuss any special needs or reasonable adjustments to be considered during the assessment (refer to the Reasonable Adjustments Strategy Matrix and negotiate these with your trainer/assessor).
* Please make sure that you have access to a computer and the internet (if you prefer to type the answers).
* Please ensure that you have all the required resources needed to complete this Unit Assessment Task (UAT).
* Due date of this assessment task is according to your timetable.
* In exceptional (compelling and compassionate) circumstances, an extensionto submit an assessment can be granted by the trainer/assessor.
* Evidence of the compelling and compassionate circumstances must be provided together with your request for an extension to submit your assessment work.
* Request for an extension to submit your assessment work must be made before the due date of this assessment task.

## **Section 2: Reasonable adjustments**

* Students with carer responsibilities, cultural or religious obligations, English as an additional language, disabilityetc. can request for reasonable adjustments.
* Please note, academic standards of the unit/course will not be lowered to accommodate the needs of any student, but there is a requirement to be flexible about the way in which it is delivered or assessed.
* The Disability Standards for Education requires institutions to take reasonable steps to enable the student with a disability to participate in education on the same basis as a student without a disability.
* Trainer/Assessor must complete the section below “Reasonable Adjustment Strategies Matrix” to ensure the explanation and correct strategy have been recorded and implemented.
* Trainer/Assessor must notify the administration/compliance and quality assurance department for any reasonable adjustments made.
* All evidence and supplementary documentation must be submitted with the assessment pack to the administration/compliance and quality assurance department.

|  |  |  |
| --- | --- | --- |
| **Reasonable Adjustment Strategies Matrix (Trainer/Assessor to complete)** | | |
| **Category** | **Possible Issue** | **Reasonable Adjustment Strategy**  **(select as applicable)** |
| 🞎 LLN | 🞎 Speaking  🞎 Reading  🞎 Writing  🞎 Confidence | 🞎 Verbal assessment  🞎 Presentations  🞎 Demonstration of a skill  🞎 Use of diagrams  🞎 Use of supporting documents such as wordlists |
| 🞎Non-English Speaking Background | 🞎 Speaking  🞎 Reading  🞎 Writing  🞎 Cultural background  🞎 Confidence | 🞎 Discuss with the student and supervisor (if applicable) whether language, literacy and numeracy are likely to impact on the assessment process  🞎 Use methods that do not require a higher level of language or literacy than is required to perform the job role  🞎 Use short sentences that do not contain large amounts of information  🞎 Clarify information by rephrasing, confirm understanding  🞎 Read any printed information to the student  🞎 Use graphics, pictures and colour coding instead of, or to support, text  🞎 Offer to write down, or have someone else write, oral responses given by the student  🞎 Ensure that the time available to complete the assessment, while meeting enterprise requirements, takes account of the student’s needs |
| 🞎Indigenous | 🞎 Knowledge and understanding  🞎 Flexibility  🞎 Services  🞎 Inappropriate training and assessment | 🞎 Culturally appropriate training  🞎 Explore understanding of concepts and practical application through oral assessment  🞎 Flexible delivery  🞎 Using group rather than individual assessments  🞎 Assessment through completion of practical tasks in the field after demonstration of skills and knowledge. |
| 🞎Age | 🞎 Educational background  🞎 Limited study skills | 🞎 Make sure font size is not too small  🞎 Trainer/Assessor should refer to the student’s experience  🞎 Ensure that the time available to complete the assessment takes account of the student’s needs  🞎 Provision of information or course materials in accessible format.  🞎 Changes in teaching practices, e.g. wearing an FM microphone to enable a student to hear lectures  🞎 Supply of specialised equipment or services, e.g. a note-taker for a student who cannot write  🞎 Changes in lecture schedules and arrangements, e.g. relocating classes to an accessible venue  🞎 Changes to course design, e.g. substituting an assessment task  🞎 Modifications to physical environment, e.g. installing lever taps, building ramps, installing a lift |
| 🞎Educational background | 🞎 Reading  🞎 Writing  🞎 Numeracy  🞎 Limited study skills and/or learning strategies | 🞎 Discuss with the Student previous learning experience  🞎 Ensure learning and assessment methods meet the student’s individual need |
| 🞎Disability | 🞎 Speaking  🞎 Reading  🞎 Writing  🞎 Numeracy  🞎 Limited study skills and/or learning strategies | 🞎 Identify the issues  🞎 Create a climate of support  🞎 Ensure access to support that the student has agreed to  🞎 Appropriately structure the assessment  🞎 provision of information or course materials in accessible format, e.g. a text book in braille  🞎 Changes in teaching practices, e.g. wearing an FM microphone to enable a student to hear lectures  🞎 Supply of specialised equipment or services, e.g. a note taker for a student who cannot write  🞎 Changes in lecture schedules and arrangements, e.g. relocating classes to an accessible venue  🞎 Changes to course design, e.g. substituting an assessment task  🞎 Modifications to physical environment, e.g. installing lever taps, building ramps, installing a lift |

| **Explanation of reasonable adjustments strategy used (If required)** |
| --- |
|  |

# **Unit Assessment Task (UAT)**

## **Assessment Task 2 – Unit Project (UP)**

**Assessment type:**

Unit Project (UP)

**Assessment task description:**

* This is the second (2) assessment task you have to successfully complete to be deemed competent in this unit of competency.
* This assessment task requires you to complete a project.
* You will receive your feedback within two weeks - you will be notified by your trainer/assessor when results are available.
* You must attempt all activities of the project for your trainer/assessor to assess your competency in this assessment task.

**Applicable conditions:**

* Activity 1 is untimed and activity 2 is timed.
* You must read and respond to all criteria of the project.
* You may handwrite/use computers to answer the criteria of the project.
* You must complete the task independently.
* No marks or grades are allocated for this assessment task. The outcome of the task will be Satisfactory or Not Satisfactory.
* As you complete this assessment task you are predominately demonstrating your practical skills, techniques and knowledge to your trainer/assessor.
* The trainer/assessor may ask you relevant questions on this assessment task to ensure that this is your own work.

**Resubmissions and reattempts:**

* Where a student’s answers are deemed not satisfactory after the first attempt, a resubmission attempt will be allowed.
* You must speak to your Trainer/Assessor if you have any difficulty in completing this task and require reasonable adjustments (e.g. can be given as an oral assessment).
* For more information, please refer to your RTO Student Handbook.

**Location:**

* This assessment task may be completed in an independent learning environment or learning management system.
* Your trainer/assessor will provide you further information regarding the location of completing this assessment task.

**General Instructions for attempting the project:**

* You will be analyse enterprise data security requirements create new plan, review encryption technologies and their respective costs in this assessment task.
* You will be required to correctly attempt all activities of this assessment task.

## You must concise to the point and write answers according to the given word-limit to each question and do not provide irrelevant information.

## You must use non-discriminatory language. The language used should not devalue, demean, or exclude individuals or groups on the basis of attributes such as gender, disability, culture, race, religion, sexual preference or age. Gender inclusive language should be used.

**How your trainer/assessor will assess your work?**

* This assessment task requires the student to successfully complete and submit a project.
* Answers must demonstrate the student’s understanding and skills of the unit.
* You will be assessed according to the provided performance checklist/ performance criteria.
* Assessment objectives/ measurable learning outcome(s) are attached as performance checklist/ performance criteria with this assessment task to ensure that you have successfully completed and submitted the assessment task.
* If all assessment tasks are deemed Satisfactory (S), then the unit outcome is Competent (C).
* If at least one of the assessment task is deemed Not Satisfactory (NS), then the unit outcome is Not Yet Competent (NYC).
* Once all assessment tasks allocated to this Unit of Competency have been undertaken, trainer/assessor will complete an Assessment plan to record the unit outcome. The outcome will be either Competent (C) or Not Yet Competent (NYC).
* The “Assessment Plan” is available with the Unit Assessment Pack (UAP) – Cover Sheet.

## **Assessment Task 2 - Unit Project (UP)**

**Instructions to complete this assessment task**:

* Please write your responses in the template provided.
* You may attach a separate sheet if required.
* You must include the following particulars in the footer section of each page of the attached sheets:
  + Student ID or Student Name
  + Unit ID or Unit Code
  + Course ID or Course Code
  + Trainer and assessor name
  + Page numbers
* You must staple the loose sheets together along with the cover page.
* You must attach the loose sheets chronologically as per the page numbers.
* Correction fluid and tape are not permitted. Please do any corrections by striking through the incorrect words with one or two lines and rewriting the correct words.
* The premise of the project must be closely related to the previous assessment task.
* This submission must be well presented and follow the guidelines and instructions provided.
* Please follow the format as indicated in the template section below.
* One of the most important steps that you can take: proofread your project.
* Project must be of 500-800 words in length, using 11-point font, double-spaced, and must include a cover page, table of contents, introduction, body, summary or conclusion, and works cited.
* Appropriate citations are required.
* All RTO policies are in effect, including the plagiarism policy.

**Scenario: -**

“Elegant Technical Education”, is one of the leading colleges in Australia providing opportunities for students to acquire a technical education and offer courses and diplomas in the disciplines of Accounting, Project Management, Automotive, Hospitality and Business. The campus of the college is in the CBD of Melbourne and it has almost 1200 students are enrolled. A staff team consisting of 40 members use the resources of the college. The college has already been transformed into paperless environment and all the proceedings along with the student’s academic progress and evaluations are done on network-based modules.

The online services offered at the college includes:

* Induction and Enrolment System
* Educational Moodle system
* Student progress monitoring system
* Application for Finance
* Email Server
* Data Server

The IT infrastructure includes a computer Lab connected in LAN, Data Server, Proxy Server, attendance machine. It also includes the desktops being provided to th staff members in their offices, staff room and respective classes, which are all connected in a network. A number of users including students, teachers and staff members use mobile and laptops while connecting to the Wi-Fi of the college as guests.

But, it has been observed that often online data is compromised and a better authentication system needs to be implemented on the network. Better authorisation and authentication which will lead to a secure college information system. It has been observed by the IT department that the students using their personal devices including laptops and hand-held devices are the major threats to the information system.

Traditional device-centric IP-based security techniques are inadequate to meet this new reality. The Services of Information Security Manager – Adam has been employed by the college to improve security and access to the college information system. Adam has an extensive experience of more than 10 years of System and Network security including Cloud applications.

David the existing IT Manager of the College will help and assist Adam in order to maintain the college’s security plan.

Roles and responsibilities of Adam:

* Provide security guidance and input to reviews of proposed projects, services and vendors.
* Lead reviews and selection processes for the new information security solutions.
* Administer security controls such as firewalls, security information and event management, remote access, access controls, intrusion detection/prevention, malware protection, data leakage prevention, etc.
* Design, perform and conduct penetration testing to identify system vulnerabilities. ‬‬
* Maintain awareness of emerging information security threats. Provide subject matter expertise to management on a broad range of information security topics and standards.
* Create and present information security awareness training programs for employees.
* Develop security policies, processes, procedures, standards and guides.
* Participate in (and sometimes leads) security incident responses and investigations. Coordinating security plans with outside vendors

Roles and responsibilities of David:

* Identifying and acting on opportunities to improve and update software and systems
* Developing and implementing IT policy and best practice guides for the organisation
* Designing training programs and workshops for staff
* Conducting regular system audits
* Running and sharing regular operation system reports with senior staff
* Overseeing and determining timeframes for major IT projects including system updates, upgrades, migrations and outages
* Managing and reporting on allocation of IT budget
* Providing direction for IT team members
* Identifying opportunities for team training and skills advancement

It has been suggested by the Information Security Manager to apply role-based access control – RBAC as the new unified network security approach. It helps in the following ways:

* Supports multiple user types with multiple access profiles
* Addresses compliance requirements
* Leverages identity to integrate with the network infrastructure directly

Also, following are the terms been defined by Adam in advice with It Manager David:

* Client - Device / user attempting to access the network
* Policy Enforcement Point (PEP) - network device that brokers access request and enforces policy result (i.e. WLAN AP, Firewall, VPN gateway, Ethernet switch)
* Policy Decision Point (PDP) – network device that decides policy for client based on PEP and PIP interaction
* Policy Information Point (PIP) - a source of information in setting policy (i.e. user directory, asset management system)
* Accounting - Audit destination for client access and network usage

**Security policies**

Also, before implementation of the authentication system for the information security of the college network, the following are the security policies related to authentication which have been agreed upon:

**a. General**

i. A suitable method of authentication must be used by all users and systems accessing “Elegant technical Education Systems or Networks”. In most cases this will be a “Elegant Technical Education” issued username and password.

ii. Unauthenticated access will be permitted only in exceptional circumstances and such systems must be explicitly configured for such use.

iii. For general computing devices (e.g. PCs) appropriate accounting information must be kept.

iv. Unused accounts must be disabled and default or blank passwords must be changed.

**b. Passwords**

i. Passwords must be kept secure; they should never be divulged to anyone not authorised to know them.

ii. Passwords should be changed at regular intervals.

iii. Passwords must be protected in use; in particular they should not be passed over unsecure networks in clear text.

iv. The user’s identity must be clearly established before a password is issued to a user.

v. Passwords should not be overused.

* “Elegant Technical Education” usernames and passwords should not be used with non “Elegant Technical Education” systems.
* Separate usernames and passwords should be used for trusted and untrusted systems.

vi. Password should be complex and obscure, such that they are not easily guessed by people or computer systems.

**c. Authentication Data Storage**

i. There is a need to process Authentication Data to manage user accounts and to allow Information Systems to be able to authenticate users.

Typically, Authentication Data is held electronically in directories (e.g. MS Active Directory) or in databases.

ii. The systems holding Authentication Data should be hardened to enhance their security and should not be used for any additional purpose that might compromise their security.

iii. All electronic copies of Authentication data must be encrypted.

iv. Authentication Data must be protected from Brute Force Attacks. (e.g. password guessing).

v. Access to Authentication Data should be restricted such that only the data necessary is available to each member of staff. Particular care is required to restrict access to password files.

vi. Where Authentication Data is available in plain text (e.g. print outs) staff should be aware of its sensitivity, ensuring its protection and secure disposal.

Initially, before commencement of the project, following points are agreed by the Information Security Manager, IT Manager and the Management of the college:

* All WLAN Access is authenticated enabling user audit and differentiated access
* There is an explicit deny rule that will automatically block anything not

permitted by a rule.

* In this way manually create a rule for permitted traffic and everything

else is automatically blocked.

* Design access lists as we need and each group can have their own unique access list.
* Dynamic VLAN assignment segments the traffic with enforcement via ACLs
* Guests can be forced to the Internet only, contractors can be given restricted

Internal access, privileged employees can see sensitive areas

* Guest access is fully audited rather than open

**Activity 1: (Analysing authentication requirement)**

After having the detail look at the scenario given above, you need to analyse the requirements in relation to the enterprise security plan of the college including the following:

* Background of the enterprise security plan
* Issues identified in the network
* Hardware and software required
* Analyses and list different authentication options according to the given scenario
* Different Authentication options
* Authentication Goals using relevant Authentication and authorisation options

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

***College Enterprise Security Plan Template***

|  |
| --- |
| Background- |
| Issues identified in the network |
| Hardware and software required |
| Identify user and security requirements |
| Different Authentication options |
| Authentication Goals using relevant authentication and authorisation options |

## **Performance criteria checklist for unit assessment task:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Trainer/ Assessor to complete** | | | |
| **Assessment activities to be completed** | * Analysing authentication requirement * For a full project outline, please refer to the student assessment instructions | | |
| **Resources required for the unit assessment task** | * Unit assessment guide template * Access to live or simulated working environment * Interaction with others | | |
| **Does the candidate meet the following criteria** | **Yes** | **No** | **Trainer/Assessor Comments** |
| Understood College’s requirements of security |  |  |  |
| Defined Requirements for security relevant to network security |  |  |  |
| Identified Hardware and software required |  |  |  |
| Identified user and security requirements |  |  |  |
| Defined authentication options and goals relevant to authentication and authorisation processes |  |  |  |

**Activity 2: (Deployment of Authentication solution and configuration of Authentication software)**

**Note: This activity is in continuation of activity 1.**

After the analysis of the college enterprise security plan and requirements for the security/authentication, along with the review of different available authentication options, do the following:

* Design and implement an authentication realm to protect the different servers and applications on the network.
* Add and manage users and apply authorisation rules to the realm. Also, define user’s attributes and their setup.
* Configure authentication filters and authorisation parameters as per the requirement.

This activity is a continuation of activity 1. You are required to participate in a practical demonstration task. You need to complete this activity in 2 to 3 hours.

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

* A site where deployment of authentication solution may be conducted
* A live network
* Servers
* Authentication software
* Security policies (as per scenario)

You have received a final approval from David to start the configuration of the authentication project, so you must perform the installation and configuration of authentication software and tools along with the creation of authentication realm on the live network.

Assume the you are “Adam” and you configurethe authentication software and manage the authentication realm.

You need to install the authentication software on the Data Server and set permissions on the network relevant to the different users.

Student must follow vendor instruction to install the software. You also need to follow organisation security policies (given in the scenario) during this task.

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

**Performance criteria checklist for unit assessment task:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Trainer/ Assessor to complete** | | | |
| **Assessment activities to be completed** | * Deployment of Authentication solution and configuration of Authentication software * For a full project outline, please refer to the student assessment instructions | | |
| **Resources required for the unit assessment task** | * Unit assessment guide template | | |
| **Does the candidate meet the following criteria** | **Yes** | **No** | **Trainer/Assessor Comments** |
| Designed and Implemented Authentication Realm   * Student followed the organisational security policies * Followed the vendor instructions * Completed the activity in a given timeframe |  |  |  |
| Installed and configured the authentication software   * Student followed the organisational security policies * Followed the vendor instructions |  |  |  |
| Managed the authentication software as per the authentication realm |  |  |  |

# **Unit Assessment Result Sheet (UARS)**

## **Assessment Task 2 – Unit Project**

## **Student and Trainer/Assessor Details**

|  |  |
| --- | --- |
| **Unit code** | ICTNWK503 |
| **Unit name** | Install and maintain valid authentication processes |
| **Outcome of Unit Assessment Task (UAT)** | |  | | --- | | **First attempt:** |   Outcome (please make sure to tick the correct checkbox):  Satisfactory (S) ☐ or Not Satisfactory (NS) ☐  Date: \_\_\_\_\_\_\_(day)/ \_\_\_\_\_\_\_(month)/ \_\_\_\_\_\_\_\_\_\_\_\_(year)   |  | | --- | | **Second attempt:** |   Outcome (please make sure to tick the correct checkbox):  Satisfactory (S) ☐ or Not Satisfactory (NS) ☐  Date: \_\_\_\_\_\_\_(day)/ \_\_\_\_\_\_\_(month)/ \_\_\_\_\_\_\_\_\_\_\_\_(year) |
| **Feedback to Student** | |  | | --- | | * **First attempt:** |  |  | | --- | | * **Second attempt:** | |
| **Student Declaration** | * I declare that the answers I have provided are my own work. Where I have accessed information from other sources, I have provided references and or links to my sources. * I have kept a copy of all relevant notes and reference material that I used as part of my submission. * I have provided references for all sources where the information is not my own. I understand the consequences of falsifying documentation and plagiarism. I understand how the assessment is structured. I accept that all work I submit must be verifiable as my own. * I understand that if I disagree with the assessment outcome, I can appeal the assessment process, and either re-submit additional evidence undertake gap training and or have my submission re-assessed. * All appeal options have been explained to me. |
| **Student Signature** |  |
| **Date** |  |
| **Trainer/Assessor Name** |  |
| **Trainer/Assessor Declaration** | I hold:  🗹 Vocational competencies at least to the level being delivered  🗹 Current relevant industry skills  🗹 Current knowledge and skills in VET, *and undertake*  🗹 Ongoing professional development in VET  *I declare that I have conducted an assessment of this candidate’s submission. The assessment tasks were deemed current, sufficient, valid and reliable. I declare that I have conducted a fair, valid, reliable, and flexible assessment. I have provided feedback to the above-named candidate.* |
| **Trainer/Assessor Signature** |  |
| **Date** |  |
| **Office Use Only** | Outcome of Assessment has been entered onto the Student Management System on \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (insert date)  by (insert Name) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

**Unit Pre-Assessment Checklist (UPAC)**

# **UAT 3 –Unit Project (UP)**

## **Purpose of the checklist**

The pre-assessment checklist helps students determine if they are ready for assessment. The trainer/assessor must review the checklist with the student before the student attempts the assessment task. If any items of the checklist are incomplete or not clear to the student, the trainer/assessor must provide relevant information to the student to ensure they understand the requirements of the assessment task. The student must ensure they are ready for the assessment task before undertaking it.**Section 1: Information for Students**

* Please make sure you have completed the necessary prior learning before attempting this assessment.
* Please make sure your trainer/assessor clearly explained the assessment process and tasks to be completed.
* Please make sure you understand what evidence is required to be collected and how.
* Please make sure you know your rights and the Complaints and Appeal process.
* Please make sure you discuss any special needs or reasonable adjustments to be considered during the assessment (refer to the Reasonable Adjustments Strategy Matrix and negotiate these with your trainer/assessor).
* Please make sure that you have access to a computer and the internet (if you prefer to type the answers).
* Please ensure that you have all the required resources needed to complete this Unit Assessment Task (UAT).
* Due date of this assessment task is according to your timetable.
* In exceptional (compelling and compassionate) circumstances, an extensionto submit an assessment can be granted by the trainer/assessor.
* Evidence of the compelling and compassionate circumstances must be provided together with your request for an extension to submit your assessment work.
* Request for an extension to submit your assessment work must be made before the due date of this assessment task.

## **Section 2: Reasonable adjustments**

* Students with carer responsibilities, cultural or religious obligations, English as an additional language, disabilityetc. can request for reasonable adjustments.
* Please note, academic standards of the unit/course will not be lowered to accommodate the needs of any student, but there is a requirement to be flexible about the way in which it is delivered or assessed.
* The Disability Standards for Education requires institutions to take reasonable steps to enable the student with a disability to participate in education on the same basis as a student without a disability.
* Trainer/Assessor must complete the section below “Reasonable Adjustment Strategies Matrix” to ensure the explanation and correct strategy have been recorded and implemented.
* Trainer/Assessor must notify the administration/compliance and quality assurance department for any reasonable adjustments made.
* All evidence and supplementary documentation must be submitted with the assessment pack to the administration/compliance and quality assurance department.

|  |  |  |
| --- | --- | --- |
| **Reasonable Adjustment Strategies Matrix (Trainer/Assessor to complete)** | | |
| **Category** | **Possible Issue** | **Reasonable Adjustment Strategy**  **(select as applicable)** |
| 🞎 LLN | 🞎 Speaking  🞎 Reading  🞎 Writing  🞎 Confidence | 🞎 Verbal assessment  🞎 Presentations  🞎 Demonstration of a skill  🞎 Use of diagrams  🞎 Use of supporting documents such as wordlists |
| 🞎Non-English Speaking Background | 🞎 Speaking  🞎 Reading  🞎 Writing  🞎 Cultural background  🞎 Confidence | 🞎 Discuss with the student and supervisor (if applicable) whether language, literacy and numeracy are likely to impact on the assessment process  🞎 Use methods that do not require a higher level of language or literacy than is required to perform the job role  🞎 Use short sentences that do not contain large amounts of information  🞎 Clarify information by rephrasing, confirm understanding  🞎 Read any printed information to the student  🞎 Use graphics, pictures and colour coding instead of, or to support, text  🞎 Offer to write down, or have someone else write, oral responses given by the student  🞎 Ensure that the time available to complete the assessment, while meeting enterprise requirements, takes account of the student’s needs |
| 🞎Indigenous | 🞎 Knowledge and understanding  🞎 Flexibility  🞎 Services  🞎 Inappropriate training and assessment | 🞎 Culturally appropriate training  🞎 Explore understanding of concepts and practical application through oral assessment  🞎 Flexible delivery  🞎 Using group rather than individual assessments  🞎 Assessment through completion of practical tasks in the field after demonstration of skills and knowledge. |
| 🞎Age | 🞎 Educational background  🞎 Limited study skills | 🞎 Make sure font size is not too small  🞎 Trainer/Assessor should refer to the student’s experience  🞎 Ensure that the time available to complete the assessment takes account of the student’s needs  🞎 Provision of information or course materials in accessible format.  🞎 Changes in teaching practices, e.g. wearing an FM microphone to enable a student to hear lectures  🞎 Supply of specialised equipment or services, e.g. a note-taker for a student who cannot write  🞎 Changes in lecture schedules and arrangements, e.g. relocating classes to an accessible venue  🞎Changes to course design, e.g. substituting an assessment task  🞎 Modifications to physical environment, e.g. installing lever taps, building ramps, installing a lift |
| 🞎Educational background | 🞎 Reading  🞎 Writing  🞎 Numeracy  🞎 Limited study skills and/or learning strategies | 🞎 Discuss with the Student previous learning experience  🞎 Ensure learning and assessment methods meet the student’s individual need |
| 🞎Disability | 🞎 Speaking  🞎 Reading  🞎 Writing  🞎 Numeracy  🞎 Limited study skills and/or learning strategies | 🞎 Identify the issues  🞎 Create a climate of support  🞎 Ensure access to support that the student has agreed to  🞎 Appropriately structure the assessment  🞎 provision of information or course materials in accessible format, e.g. a text book in braille  🞎 Changes in teaching practices, e.g. wearing an FM microphone to enable a student to hear lectures  🞎 Supply of specialised equipment or services, e.g. a note taker for a student who cannot write  🞎 Changes in lecture schedules and arrangements, e.g. relocating classes to an accessible venue  🞎 Changes to course design, e.g. substituting an assessment task  🞎 Modifications to physical environment, e.g. installing lever taps, building ramps, installing a lift |

| **Explanation of reasonable adjustments strategy used (If required)** |
| --- |
|  |

# **Unit Assessment Task (UAT)**

## **Assessment Task 3 – Unit Project (UP)**

**Assessment type:**

Unit Project (UP)

**Assessment task description:**

* This is the third (3) assessment task you have to successfully complete to be deemed competent in this unit of competency.
* This assessment task requires you to complete a project.
* You will receive your feedback within two weeks - you will be notified by your trainer/assessor when results are available.
* You must attempt all activities of the project for your trainer/assessor to assess your competency in this assessment task.

**Applicable conditions:**

* This project is timed.
* You must read and respond to all criteria of the project.
* You may handwrite/use computers to answer the criteria of the project.
* You must complete the task independently.
* No marks or grades are allocated for this assessment task. The outcome of the task will be Satisfactory or Not Satisfactory.
* As you complete this assessment task you are predominately demonstrating your practical skills, techniques and knowledge to your trainer/assessor.
* The trainer/assessor may ask you relevant questions on this assessment task to ensure that this is your own work.

**Resubmissions and reattempts:**

* Where a student’s answers are deemed not satisfactory after the first attempt, a resubmission attempt will be allowed.
* You must speak to your Trainer/Assessor if you have any difficulty in completing this task and require reasonable adjustments (e.g. can be given as an oral assessment).
* For more information, please refer to your RTO Student Handbook.

**Location:**

* This assessment task may be completed in a simulated learning environment.
* Your trainer/assessor will provide you further information regarding the location of completing this assessment task.

**General Instructions for attempting the project:**

* This assessment task is in continuation to the previous task.
* You will be expanding the knowledge and skills acquired during the previous assessment task.

## You must concise to the point and write answers according to the given word-limit to each question and do not provide irrelevant information.

## You must use non-discriminatory language. The language used should not devalue, demean, or exclude individuals or groups on the basis of attributes such as gender, disability, culture, race, religion, sexual preference or age. Gender inclusive language should be used.

## You will be required to correctly attempt all activities of this assessment task.

**How yourtrainer/assessor will assess your work?**

* This assessment task requires the student to successfully complete and submit a project.
* Answers must demonstrate the student’s understanding, knowledge and skill of the unit.
* You will be assessed according to the provided performance checklist/ performance criteria.
* Assessment objectives/ measurable learning outcome(s) are attached as performance checklist/ performance criteria with this assessment task to ensure that you have successfully completed and submitted the assessment task.
* If all assessment tasks are deemed Satisfactory (S), then the unit outcome is Competent (C).
* If at least one of the assessment task is deemed Not Satisfactory (NS), then the unit outcome is Not Yet Competent (NYC).
* Once all assessment tasks allocated to this Unit of Competency have been undertaken, trainer/assessor will complete an Assessment plan to record the unit outcome. The outcome will be either Competent (C) or Not Yet Competent (NYC).
* The “Assessment Plan” is available with the Unit Assessment Pack (UAP) – Cover Sheet.

## **Assessment Task 3 - Unit Project (UP)**

**Instructions to complete this assessment task**:

* Please write your responses in the template provided.
* You may attach a separate sheet if required.
* You must include the following particulars in the footer section of each page of the attached sheets:
  + Student ID or Student Name
  + Unit ID or Unit Code
  + Course ID or Course Code
  + Trainer and assessor name
  + Page numbers
* You must staple the loose sheets together along with the cover page.
* You must attach the loose sheets chronologically as per the page numbers.
* Correction fluid and tape are not permitted. Please do any corrections by striking through the incorrect words with one or two lines and rewriting the correct words.
* The premise of the project must be closely related to the previous assessment task.
* This submission must be well presented and follow the guidelines and instructions provided.
* Please follow the format as indicated in the template section below.
* One of the most important steps that you can take: proofread your project.
* Appropriate citations are required.
* All RTO policies are in effect, including the plagiarism policy.

**Activity 1 (Application of authentication methods)**

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 2 to 3 hours.

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

* A site where encryption installation may be conducted
* A live network
* Servers
* Authentication software
* Security policies
* Vender instructions for hardware and software
* Biometric authentication adaptors

After configuring authentication software in assessment task 2, you (Adam) are required to apply relevant authentication methods on the network according to vendor instructions and organisation policies. You need to do the following:

* Develop authentication protocols
* Implement these to the network and user access as per the college enterprise security plan
* Implement the authentication system and users as per the requirements and ensure that it follows current authentication standards
* Includesbiometric authentication adaptors as a part of implementation
* Management of the permissions and configuration information to the central secure location
* Define the Policy Server, Directory Connectivity, Supplicant Management,

Legacy Support, Information Security Administrator, Group or Policy Administrator and User

* Complete the given template 1 relevant to the application of the authentication methods.

**Template 1**

|  |
| --- |
| ***PURPOSE***  ***SCOPE***  ***Application to Systems***  ***EXCEPTIONS***  ***ROLES AND RESPONSIBILITIES***  ***POLICY***  ***Authenticator Feedback*** |

## **Performance criteria checklist for unit assessment task:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Trainer/ Assessor to complete** | | | |
| **Assessment activities to be completed** | * Application of authentication methods * For a full project outline, please refer to the student assessment instructions | | |
| **Resources required for the unit assessment task** | * Unit assessment guide template * Access to live or simulated working environment * Interaction with others | | |
| **Does the candidate meet the following criteria** | **Yes** | **No** | **Trainer/Assessor Comments** |
| Managed Authentication Protocols |  |  |  |
| Implemented protocols on network |  |  |  |
| Implemented authentication system |  |  |  |
| Ensured authentication system is updated |  |  |  |
| Managed Permissions and configurations to central secure location |  |  |  |
| Defined the Policy Server, Directory Connectivity, Supplicant Management, Legacy Support, Information Security Administrator, Group or Policy Administrator and User |  |  |  |

***Activity 2: (Role Play - Informing users about authentication system and their responsibilities)***

***Note: This activity is in continuation of activity 1.***

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

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

The purpose of the role play is to inform users about the authentication system and their roles and responsibilities as per the college security plan.

* Information Security Manager
* Group or Policy Administrator - IT Manager
* User

You will act as theInformation Security Manager, while the trainer/assessor will act as the IT Manager. Also, a class mate of you will act as the user and you need to brief the user about the authentication system and his responsibilities relevant to the enterprise security plan. You will also discuss suitable authentication protocols.

Your trainer/assessor also participate in the role play discussing the policies and privileges set on the IT resources and network.

Your trainer/assessor will act as IT Manager and will ask you the following questions:

1. Authorisation of the users
2. Responsibilities due to the new authentication system including permissions and privileges while accessing the different sources of information of college

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:** | | | |

**Performance checklist**

|  |  |  |  |
| --- | --- | --- | --- |
| **Trainer/ Assessor to complete** | | | |
| **Assessment activities to be completed** | * Role Play - Informing users about authentication system and their responsibilities * For a full project outline, please refer to the student assessment instructions | | |
| **Resources required for the unit assessment task** | * Unit assessment guide template * Access to live or simulated working environment * Interaction with others | | |
| **Does the candidate meet the following criteria** | **Yes** | **No** | **Trainer/Assessor Comments** |
| Started role-play with greetings |  |  |  |
| Explained the authentication and User responsibilities |  |  |  |
| Used simple language to explain technical terminology |  |  |  |
| Explained the roles to individuals |  |  |  |
| Discussed suitable authentication protocols |  |  |  |
| Body Language during Presentation including:   * Eye contact * Tone * Gesture |  |  |  |

**Activity 3**: **(Monitoring of the Authentication Software)**

As you have implemented the authentication over the network in a live server/network environment in the previous assessment activities, you are required to monitor the authentication system in this activity. You need to complete this task in 1 to 2 hours.

In this activity you need to monitor the functioning of the “Authentication system” by performing the following tasks in a live server/network environment.

* Analysis of the authentication system as per the roles of different users and college security and Quality of Service requirements
  + Use different software’s and techniques to test the authentication system
* To monitor ongoing security, complete below incident ticket and reporting processes template.
* You need to test the authentication system at least two different times for ongoing security monitoring and must complete following template for both occasions.
* You need to report authentication system issues to you trainer and discuss the solutions.
* Make changes to the authentication system if required.

Fill in the template given below for incident records and reporting processes:

|  |
| --- |
| **Executive overview** |
| **Incident record overview**  This document is intended to provide an understanding of the attributes/fields that need to be captured in an incident ticket |

|  |  |  |
| --- | --- | --- |
| Field Description(where necessary) | | |
| IncidentID |  |  |
| Issue/s or System faults |  |  |
| Contactname |  |  |
| Firstname |  |  |
| Last name |  |  |
| Date and time |  |  |
| Incident reported to: |  |  |
| Location: |  |  |

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

## **PPerformance criteria checklist for unit assessment task:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Trainer/ Assessor to complete** | | | |
| **Assessment activities to be completed** | * Monitoring of the Authentication Software * For a full project outline, please refer to the student assessment instructions | | |
| **Resources required for the unit assessment task** | * Unit assessment guide template * Access to live or simulated working environment * Interaction with others | | |
| **Does the candidate meet the following criteria** | **Yes** | **No** | **Trainer/Assessor Comments** |
| Analysed the authentication system as per the roles of different users and college security and Quality of Service requirements including:   * Check that validity of the digital certificates * Check different permissions and privileges being assigned to different users as per their roles and responsibilities * Check overall network performance |  |  |  |
| Monitored security using security monitoring tools |  |  |  |
| Complete the provided monitoring template |  |  |  |
| Discussed the authentication system issues with the trainer and adjust authentication system as required |  |  |  |
| Checked local computer security logs for and submitted to the trainer/assessor |  |  |  |
| Checked logs of permissions and privileges |  |  |  |

# **Unit Assessment Result Sheet (UARS)**

## **Assessment Task 3 – Unit Project**

## **Student and Trainer/Assessor Details**

|  |  |
| --- | --- |
| **Unit code** | ICTNWK503 |
| **Unit name** | Install and maintain valid authentication processes |
| **Outcome of Unit Assessment Task (UAT)** | |  | | --- | | **First attempt:** |   Outcome (please make sure to tick the correct checkbox):  Satisfactory (S) ☐ or Not Satisfactory (NS) ☐  Date: \_\_\_\_\_\_\_(day)/ \_\_\_\_\_\_\_(month)/ \_\_\_\_\_\_\_\_\_\_\_\_(year)   |  | | --- | | **Second attempt:** |   Outcome (please make sure to tick the correct checkbox):  Satisfactory (S) ☐ or Not Satisfactory (NS) ☐  Date: \_\_\_\_\_\_\_(day)/ \_\_\_\_\_\_\_(month)/ \_\_\_\_\_\_\_\_\_\_\_\_(year) |
| **Feedback to Student** | |  | | --- | | * **First attempt:** |  |  | | --- | | * **Second attempt:** | |
| **Student Declaration** | * I declare that the answers I have provided are my own work. Where I have accessed information from other sources, I have provided references and or links to my sources. * I have kept a copy of all relevant notes and reference material that I used as part of my submission. * I have provided references for all sources where the information is not my own. I understand the consequences of falsifying documentation and plagiarism. I understand how the assessment is structured. I accept that all work I submit must be verifiable as my own. * I understand that if I disagree with the assessment outcome, I can appeal the assessment process, and either re-submit additional evidence undertake gap training and or have my submission re-assessed. * All appeal options have been explained to me. |
| **Student Signature** |  |
| **Date** |  |
| **Trainer/Assessor Name** |  |
| **Trainer/Assessor Declaration** | I hold:  🗹 Vocational competencies at least to the level being delivered  🗹 Current relevant industry skills  🗹 Current knowledge and skills in VET, *and undertake*  🗹 Ongoing professional development in VET  *I declare that I have conducted an assessment of this candidate’s submission. The assessment tasks were deemed current, sufficient, valid and reliable. I declare that I have conducted a fair, valid, reliable, and flexible assessment. I have provided feedback to the above-named candidate.* |
| **Trainer/Assessor Signature** |  |
| **Date** |  |
| **Office Use Only** | Outcome of Assessment has been entered onto the Student Management System on \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (insert date)  by (insert Name) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |