COMPUTER SCIENCE

ATAR course sample examination one

Marking key

Marking keys are an explicit statement about what the examining panel expect of candidates when they respond to particular examination items. They help ensure a consistent interpretation of the criteria that guide the awarding of marks.

Section One: Short answer   **40% (78 Marks)**

Question 1 (4 marks)

Describe **two** external network threats.

Description	Marks
For each (2 x 2 marks)	
Describes an external network threat	2
States a fact about an external network threat	1
Total	**4**
Answers could include: • denial of service (DOS). A DOS attack overwhelms or locks up resources preventing access to them • man-in-the-middle (MitM). A MitM attack is when a bad actor intercepts network traffic and then reads and/or modifies it before sending it on.	
Accept other relevant answers.	

Question 2 (3 marks)

Complete the table below by identifying a characteristic of each data type listed.

Description	Marks
For each (3 x 1 mark)	
Identifies a characteristic	1
Total	**3**
Answers could include: • Float: contains fractions or decimals • String: a sequence of characters • Boolean: having two outcomes or possibilities.	
Accept other relevant answers.	

Question 3 **(4 marks)**

Describe each of the following types of data integrity.

- Domain integrity
- Referential integrity

Description	Marks
For each (2 x 2 marks)	
Describes the type of data integrity	2
States a fact about the type of data integrity	1
Total	**4**
Answers could include: Domain integrity – requires a given field that only stores a single piece of atomic data and that the data is of the correct data type and it meets the constraints. Referential integrity – requires that foreign keys refer back to a primary key that exists in the parent table. Referential integrity is lost if a foreign key entry has no matching primary key value in the parent table.	
Accept other relevant answers.	

Question 4 **(4 marks)**

(a) Define the term 'delete anomaly' and, from the table above, outline an example of a delete anomaly. (2 marks)

Description	Marks
Defines delete anomaly	1
Identifies an example	1
Total	2
Answers could include: A delete anomaly occurs when deletion of a record results in data that is unavoidably lost because the data does not appear anywhere else. For example, if Harry Greats is removed from the Sports System project, the data about the Physical Education department is also lost as this is the only record in which it appears.	
Accept other relevant answers.	

(b) Define the term 'update anomaly' and, from the table above, outline an example of an update anomaly. (2 marks)

Description	Marks
Defines update anomaly	1
Identifies an example	1
Total	2
Answers could include: An update anomaly occurs when multiple instances of the same data appear in a table which results in any changes to the data requiring multiple instances to be changed. For example, if the name of the IT department was to change, it would require four instances of that data to be changed.	
Accept other relevant answers.	

Question 5 **(13 marks)**

(a) Write Boolean logical expressions to test each of the following:

- the variable "age" stores the age in years of a passenger
- the variable "student" stores a Boolean value indicating whether the passenger is a student.

Your Boolean expression should resolve as true for passengers who are either:

- younger than 18
- older than 65
- a student. (3 marks)

Description	Marks
age>65 age<18	1
correct use of OR	1
student = true	1
Total	3
Answers could include: age > 65 OR age < 18 OR student = True.	
Accept other relevant answers.	

(b) Outline **two** differences between a 'class' and an 'object'. (2 marks)

Description	Marks
For each (2 x 1 mark)	
Outlines a difference between a class and an object	1
Total	2
Answers could include: • a class is a template created in source code whereas an object is an instance of a class, created at runtime and stored in memory • a class is created only once whereas multiple objects can be created from a single class.	
Accept other relevant answers.	

Question 5 (continued)

(c)   Write the pseudocode for a 'Passenger' class. The Passenger class has an identification number, name, date of birth and credit as private attributes.

Your constructor should:
- accept name and date of birth as parameters
- generate a new ID using a function called 'get_new_id'
- set credit to have a value of zero.

Include a stub for a method called 'get_age' which has no parameters and always returns 18.   (8 marks)

Description	Marks
Defines the class	1
Declares private variables	1
Declares constructor	1
Calls get_new_id to set the id_number variable	1
Sets name and date_of_birth using the parameters	1
Sets credit to be 0	1
Declares get_age module (method)	1
Returns 18 from the get_age module	1
Total	**8**

Answers could include:

```
CLASS Passenger
    PRIVATE id_number
    PRIVATE name
    PRIVATE date_of_birth
    PRIVATE credit    PUBLIC MODULE Passenger(new_name, new_date_of_birth)
        id_number = get_new_id()
        Function
            name = new_name
            date_of_birth = new_date_of_birth
            credit = 0
    END MODULE
    PUBLIC MODULE get_age()
        RETURN 18
    END MODULE
END CLASS
```

Accept other relevant answers.

Question 6   **(3 marks)**

Explain how social engineering (phishing) can be used to gain unauthorised access to a network, despite technical security measures being present.

Description	Marks
Explains social engineering and how it can bypass technical security measures	3
Describes social engineering with limited reference to the bypassing of technical security measures	2
Outlines social engineering	1
Total	3
Answers could include:	

Social engineering is when an attacker uses trickery to convince another person to give them information or access to which others should not be privileged. This can be in the form of emails, phone calls or in person. Once the attacker phishes enough information from the victim, if limited security is in place the attacker can gain access to the system through the use of the victim's credentials.

Accept other relevant answers.

Question 7   **(4 marks)**

(a)   Describe how a breakpoint debugging technique helps programmers identify errors in
       code.   (2 marks)

Description	Marks
Describes how a breakpoint is used to identify errors	2
States a fact about how a breakpoint is used to identify errors	1
Total	2
Answers could include:	

A breakpoint tells the debugger to pause execution on that line and allows the programmer to see the values of variables that exist in the program. The programmer can step through the program and identify variable values that are unexpected/incorrect or cause errors.

Accept other relevant answers.

(b)   Referring to the content of line 8 in the code fragment above, outline why a breakpoint is
       a more comprehensive debugging option than using print statements.   (2 marks)

Description	Marks
Outlines why a breakpoint is more comprehensive than print statements with reference to line 8	2
Outlines why a breakpoint is more comprehensive than print statements	1
Total	2
Answers could include:	

The breakpoint allows a developer to see the values and results of all of these every time the program steps through, and can pause or step forward whenever they wish. Print statements require the programmer to specify each variable they would like to print, and it is not always possible to capture function returns. Additional code is required to pause program execution.

Accept other relevant answers.

Question 8 (3 marks)

Explain how a network switch uses MAC addresses to determine to which physical port a particular incoming data packet should be directed in order to reach its intended connected device.

Description	Marks
Explains how a network switch uses MAC addresses to determine to which physical port a particular incoming data packet should be directed in order to reach its intended connected device	3
Describes how a network switch uses MAC addresses to determine to which physical port a particular incoming data packet should be directed in order to reach its intended connected device	2
States a fact about a network switch	1
Total	3
Answers could include: When a new device connects to a switch it advertises its MAC address with the switch and the switch adds this MAC address to its own internal address table. This associates the MAC address of the physical device (host) with a specific port. When the frame arrives at the switch, its MAC address is used to direct the frame to the correct port.	
Accept other relevant answers.	

Question 9 (6 marks)

Complete the missing information in the table below of Open Systems Interconnection (OSI) layers:

OSI layer	Role of the layer	Example network component hardware or protocol	Marks
7. Application	End user application protocols	HTTP	1
6. Presentation	Formatting of data, encryption and decryption	SSL	1
5. Session	Manages connections between endpoints	NetBIOS	-
4. Transport	Ensures data arrives as expected	TCP	1
3. Network	Routing packets, determining best path	Routers	1
2. Data link	Breaks packets into frames	Switches	1
1. Physical	Sends data using signals, such as electricity or visible light	Cables	1
		Total	6
Accept other relevant answers.			

Question 10 **(4 marks)**

Define the role of each of the terms in the acronym 'ACID' as it applies to databases.

Description	Marks
For each (4 x 1 mark)	
Defines the role of the term	1
Total	**4**
Answers may include: • atomicity – all parts of a database transaction succeed, or no parts do • consistency – data is guaranteed to be consistent according to defined rules and constraints • isolation – no transactions can affect the outcomes of any other transactions • durability – once a transaction has been committed it will be permanent.	
Accept other relevant answers.	

Question 11 **(2 marks)**

Define the role of 'red team' and 'blue team' as they relate to penetration testing.

Description	Marks
For each (2 x 1 mark)	
Defines the role of the team	1
Total	**2**
Answers could include: • the red team has the role of attacking an organisation to highlight vulnerabilities as part of penetration testing • the blue team has the role of assessing the defences from within an organisation and making improvements.	
Accept other relevant answers.	

Question 12 **(2 marks)**

State **one** different activity to be carried out by a member of the red team and the blue team.

Description	Marks
For each (2 x 1 mark)	
States a correct activity for the team	1
Total	**2**
Answers could include: • red team: sending phishing emails • blue team: audits and conducts digital analysis to create a baseline of network activity and more easily spot unusual or suspicious activity.	
Accept other relevant answers.	

Question 13 (4 marks)

Justify the use of symmetric encryption in creating an asymmetric connection to a website.

Description	Marks
Justifies the use of symmetric encryption in creating an asymmetric connection to a website	4
Explains the use of symmetric encryption in creating an asymmetric connection to a website	3
Describes how the use of symmetric encryption in creating an asymmetric connection to a website	2
States a fact about symmetric and/or asymmetric encryption	1
Total	4
Answers could include: Data is transferred using symmetric encryption keys when using protocols such as HTTPS. However, it is not possible for both the client and server to share a symmetric encryption key securely over the Internet without making use of asymmetric encryption. The server sends through a certificate containing its public key – which can be used for asymmetric encryption (establishing a connection). The client uses the public key to generate a symmetric key and shares this with the server. Client and server can then exchange data securely using the symmetric key.	
Accept other relevant answers.	

Question 14 (1 mark)

Identify a program control structure used in the pseudocode in line 4 above.

Description	Marks
Identifies a program control structure	1
Total	1
Answers could include: • decision (two-way selection) • IF/ELSE statement.	
Accept other relevant answers.	

Question 15   **(5 marks)**

(a)   Describe how data is sent through a network using packets.   (2 marks)

Description	Marks
Describes how data is sent through a network using packets	2
Outlines how data is sent through a network using packets	1
Total	**2**
Answers could include: The source computer splits the data into multiple packets – each with their own headers indicating metadata such as the destination and source address and sequence number. These packets are then sent across the network and reassembled at the destination.	
Accept other relevant answers.	

(b)   State a purpose of the 'protocol' section of the packet.   (1 mark)

Description	Marks
States a purpose of the protocol section	1
Total	**1**
Answers could include: The protocol section indicates which protocol should interpret/handle the packet when it arrives at its destination.	
Accept other relevant answers.	

(c)   Describe the concept of subnetting.   (2 marks)

Description	Marks
Describes the concept of subnetting	2
States a fact about subnetting	1
Total	**2**
Answers could include: Subnetting involves the logical dividing of a larger network into smaller, more manageable subnetworks or subnets. It plays a crucial role in IP address management and efficient network design.	
Accept other relevant answers.	

Question 16 (2 marks)

Describe the purpose of issuing a network 'ping' command with respect to network troubleshooting and performance management.

Description	Marks
Describes the purpose of a ping with respect to network troubleshooting and performance	2
States a fact about the use of a ping with respect to network troubleshooting and performance	1
Total	2
Answers could include:	
A ping sends ICMP packets to a destination address to measure the time taken to send and receive messages to a particular host. The ping command is used to troubleshoot a network in order to identify bottlenecks and data transfer issues at each hop.	
Accept other correct answers.	

Question 17 (4 marks)

Discuss why a binary search would be a more suitable algorithm to use than a linear search algorithm.

Description	Marks
Discusses why a binary search is a more suitable algorithm than a linear search	4
Explains why a binary search is a more suitable algorithm than a linear search	3
Describes why a binary search is a more suitable algorithm than a linear search	2
States a fact about a linear and/or binary search algorithm	1
Total	4
Answers could include:	
A linear search can look through every single entry before finding the data it is searching for. Binary search is more effective as it 'divides and conquers' the elements on sorted arrays. Each time a binary search checks an element, it eliminates half of the remaining possible elements, significantly reducing search time of the array, making it more suitable than a linear search algorithm.	
Accept other relevant answers.	

Question 18 **(2 marks)**

Outline why it is important to use live test data including a sufficiently large volume of test data (load testing) before completing a software development project.

Description	Marks
Outlines why it is important to use a sufficiently large volume of test data before completing a software development project	2
States a fact about using large volumes of test data before completing a software development project	1
Total	2
Answers could include:	
A large volume of test data provides potentially untested input in a way that simulates real world use. This helps to show that your software project can handle real world input loads without becoming overwhelmed.	
Accept other relevant answers.	

Question 19 **(2 marks)**

State **two** actions that organisations need to take in order to adhere to data security in relation to the Australian Privacy Principle 11 (APP11) of the *Privacy Act of 1988*.

Description	Marks
For each (2 x 1 mark)	
States an action that organisations need to take in order to adhere to data security as indicated in the APP11	1
Total	2
Answers could include:	
• the APP11 requires organisations to take reasonable steps to safeguard personal data from unauthorised access, disclosure, alteration, or loss • it requires organisations to conduct security risk assessments.	
Accept other relevant answers.	

Question 20 **(3 marks)**

Explain **one** ethical implication when using data mining techniques.

Description	Marks
Explains an ethical implication of using data mining	3
Describes an ethical implication of using data mining	2
States a fact about an ethical implication of using data mining	1
Total	3
Answers could include: Privacy The use of medical and pharmaceutical records for data mining to gather data about an individual's lifestyle and health can be perceived by many to be an invasion of an individual's privacy. Stereotyping Patterns discovered in data mining of shopping behaviour are used to build profiles of characteristics or behaviour. Analysis of the data may show certain buying patterns of groups which may lead to stereotyping.	
Accept other relevant answers.	

Question 21 **(3 marks)**

Explain the difference in characteristics between 'one-dimensional' and 'two-dimensional' arrays.

Description	Marks
Explains the difference in characteristics between one-dimensional and two-dimensional arrays	3
Describes the difference in characteristics between one-dimensional and two-dimensional arrays	2
States a fact about the difference in characteristics between one-dimensional and two-dimensional arrays	1
Total	3
Answers could include: A one-dimensional (1D) array is a linear ordered collection of elements of the same data type, such as a list or a row of values. A two-dimensional (2D) array is a data structure that is represented using a grid of rows and columns. The elements in a 2D array are accessed using the row and column indices, whereas in a 1D array, only a single index is used.	
Accept other relevant answers.	

Section Two: Extended answer **60% (105 Marks)**

Question 22 **(23 marks)**

(a)   Using variables in the table of the source booklet, create a program control structure that tests if the centre of the puck is within the goal zone and prints either "true" or "false" (5 marks)

Description	Marks
Compares centre X with top left X	1
Compares centre Y with top left Y	1
Compares centre X with bottom right X	1
Compares centre Y with bottom right Y	1
Outputs correct result.	1
Total	**5**

Answers could include:
 	
IF (Puck.X > TLX AND Puck.Y < TLY) AND (Puck.X < BRX and Puck.Y > BRY) THEN
        PRINT("true")
ELSE
        PRINT("false")
END IF	

Accept other relevant answers.	

Question 22 (continued)

(b)   Write a Python function called 'insert_new_high_score' which accepts the following:

•   a two-dimensional array of 10 existing, sorted high scores and player's initials stored as three character strings
•   an integer containing the player score entry to the 'high_scores' table.

Your function must determine whether the new score is high enough to include in the list, and if so, must insert the score and initials into the appropriate locations in the array.

Your function must return a two-dimensional array of the top 10 sets of high scores and initials. You may not make use of any external libraries.   (12 marks)

Description	Marks
Function beginning and end	1
Declares function	1
Structure in iteration through array (for or while loop)	1
Condition in iteration	1
Locates each index to insert new score	1–3
Moves each of the lower scores down in the array	1–2
Addresses each element in arrays correctly	1–2
Returns correctly sorted array	1
Total	**12**

Answers could include:

```python
def insertNewHighScore(highScores, initials, newScore):
    found = False
    updatedScores = [[0, 0] for _ in range(10)]  # Initialize a list with 10 elements, each containing [0, 0]

    for i in range(10):
        if highScores[i][1] >= newScore and not found:
            updatedScores[i][0] = highScores[i][0]
            updatedScores[i][1] = highScores[i][1]
            found = True
        else:
            if found:
                updatedScores[i][0] = highScores[i - 1][0]
                updatedScores[i][1] = highScores[i - 1][1]
            else:
                updatedScores[i][0] = initials
                updatedScores[i][1] = newScore
                found = True

    return updatedScores
```

Accept other relevant answers.

(c)   Assume your code works well, but you have decided to write a series of unit tests. Describe a purpose of unit tests when writing code.   (2 marks)

Description	Marks
Describes a purpose of unit tests when writing code	2
States the purpose of unit tests when writing code	1
Total	**2**
Answers could include: Unit tests are designed to take sample input and test small pieces of code against expected results. Unit tests can very quickly detect the results from the input and match with the expected output.	
Accept other relevant answers.	

(d)   Given the example data structure in the source booklet for representing the sample high score array, list **four** new score values you would use as test data and state a reason why you have selected each of their values.   (4 marks)

Description	Marks
For each (4 x 1 mark)	
Lists a score and states a valid reason	1
Total	**4**
Answers could include: • 3000: this will be too low to be included and should return the array it received with all values unchanged • 8000: this will be the new highest score and the lowest score will be eliminated • 4000: this belongs in the middle of the list • 3555: this is an identical score – it should end up just below the existing same score and the lowest score will be eliminated.	
Accept other relevant answers.	

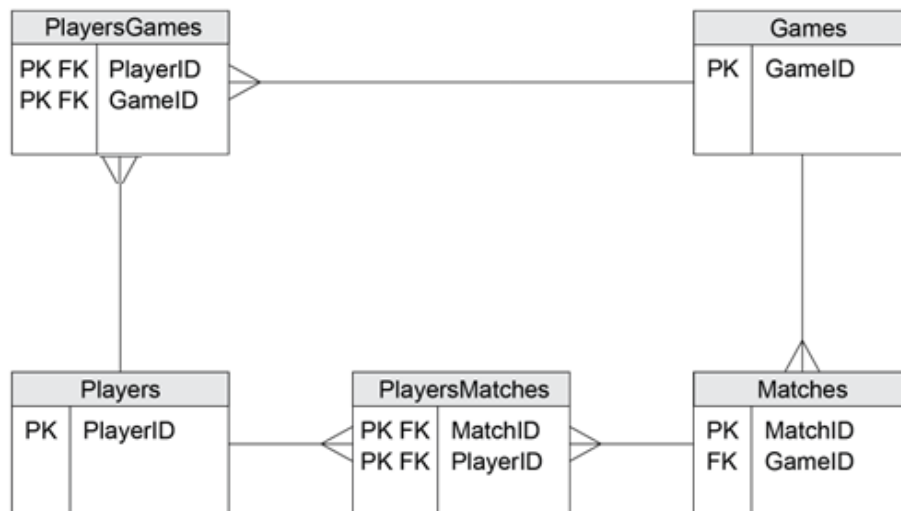**Question 23**   **(35 marks)**

(a)   Given the information above, outline a reason why it would be better to use a unique
       integer 'PlayerID' attribute that cannot be changed as the primary key instead of the
       username.   (2 marks)

Description	Marks
Outlines why PlayerID is a more suitable unique integer that cannot be changed as the primary key	2
States a fact about PlayerID	1
Total	2
Answers could include: A primary key is a unique identifier for records in the table but is used in multiple locations as a foreign key in other tables. If the username can be changed this could cause anomalies in a variety of locations.	
Accept other relevant answers.	

(b)   Create an entity relationship (ER) diagram using crow's foot notation showing the tables
       necessary to store data about matches on Pointed Nostalgia's game-matching service.
       Resolve any many to many relationships and show only key attributes.   (18 marks)

Description	Marks
For each entity (5 x 1 mark)	
Includes an entity	1
Subtotal	5
For each primary key attribute (5 x 1 mark)	
Includes a primary key attribute	1
Subtotal	5
For each foreign key attribute (3 x 1 mark)	
Includes foreign key attributes in the relevant entity	1
Subtotal	3
For each cardinality (5 x 1 mark)	
Includes a cardinality	1
Subtotal	5
Total	18
Answers could include: 	
Accept other relevant answers.	

(c)   Each game has a GameID, Title, Price and MaxPlayers. Complete the data dictionary
        below for the attributes in the Games table.   (6 marks)

Description					Marks
Element name	**Data type**	**Size/format**	**Description**	**Constraint**	
GameID	Integer	4, Autoincrement	Primary key for this table	Unique	1
Title	Text	64	Title of game	Not null	1
Price	Float	3,2	Price of game	Not null	1–2
MaxPlayers	Integer	2	Maximum number of players in a match	Minimum of 1	1–2
				Total	**6**

(d)   Write a query using SQL to create the Games table.
        Note: you do not need to enforce custom constraints such as 'minimum of 1'.   (4 marks)

Description	Marks
Create table games	1
Fields listed (as per dictionary)	1
Data types and sizes (as per dictionary)	1
Primary key and not null constraints set	1
Total	**4**
Answers could include: CREATE TABLE Games (GameID INTEGER PRIMARY KEY, Title TEXT(64) NOT NULL, Price FLOAT(3,2) NOT NULL, MaxPlayers INTEGER(2) NOT NULL)	
Accept other relevant answers.	

(e)   Write a query using SQL to return all player usernames with matches recorded for the
        game with a GameID of 7.   (5 marks)

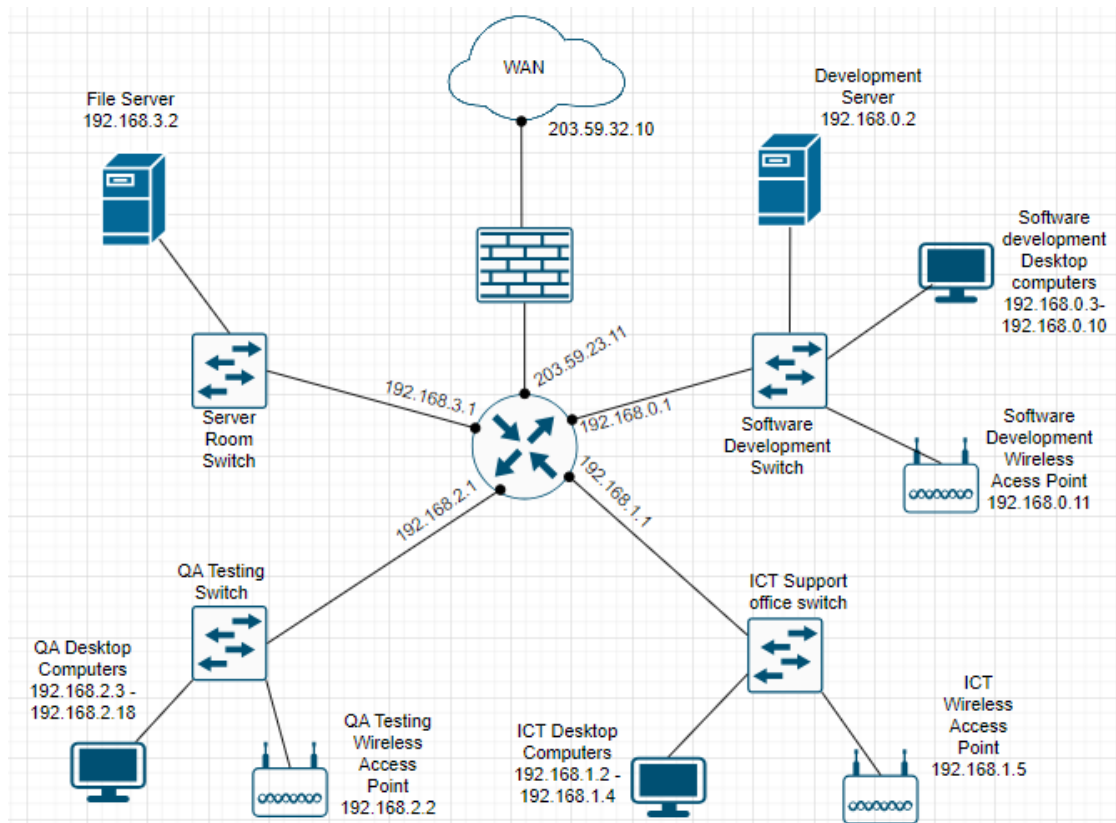| Description	Marks
SELECT Username	1
FROM Players, PlayersMatches, Matches	1
WHERE GameID = 7	1
AND Players.PlayerID = PlayersMatches.PlayerID	1
AND PlayersMatches.MatchID = Matches.MatchID	1
Total	**5**
Accept other relevant answers.	

Question 24 **(27 marks)**

(a) Complete the network diagram showing the proposed Pointed Nostalgia network using CISCO conventions. Desktops may be represented using a single symbol with an address range given to their network, as indicated for the developers' network. Label each component to show what it is and which network it belongs to. Allocate appropriate IP addresses to each end point device. Wireless clients do not need to be included.

(16 marks)

Description	Marks
Main router connecting to ICT support network	1
Switch connected to appropriate router (4 x 1 mark)	1–4
Fileservers attached to the appropriate switch (2 x 1 mark)	1–2
Valid fileserver IPs (2 x 1 mark)	1–2
ICT desktops appropriate IP range, connected to correct network	1
Wireless access points connected to appropriate switches	1
Identification of public WAN IP addresses	1
Development desktops labelled with appropriate IP range – different from ICT network, connected to correct network	1
Firewall correctly placed	1
QA desktops labelled with appropriate IP range – different from ICT and development network, connected to correct network	1
Cisco conventions used and components labelled	1
Total	**16**

Answers could include:

Accept other relevant answers.

(b) Describe the use of a traceroute for evaluating performance and/or troubleshooting across multiple networks. (2 marks)

Description	Marks
Describes the use of a traceroute for evaluating performance and/or troubleshooting across multiple networks	2
States a fact about a traceroute	1
Total	2
Answers could include:	
Traceroutes run a series of pings to each node or hop on a path to the destination address on another network. This can allow an administrator to identify performance issues and assist in diagnosing problems by providing response times at different stages of a packet's route.	
Accept other relevant answers.	

(c) You have been asked to determine whether transmission control protocol (TCP) or user datagram protocol (UDP) would be a better choice of protocol for Pointed Nostalgia's new online turn-based strategy game. Compare UDP and TCP protocols and justify a selection of one over the other for this specific game. (4 marks)

Description	Marks
Comparison	
Compares UDP and TCP protocols	2
States a fact about UDP or TCP protocols	1
Subtotal	2
Justification	
Selects TCP	1
Justifies selections of TCP	1
Subtotal	2
Total	4
Answers could include:	
TCP prioritises reliable and ordered delivery of data, ensuring that an entire message will be delivered at the cost of time. UDP prioritises speed of delivery, usually at the cost of reliability. Given the game is not dependant on fast reactions and is turn based, TCP would be the most suitable option, as it would ensure reliable delivery of data.	
Accept other relevant answers.	

Question 24 (continued)

(d)   Describe private IPv4 addressing and explain why it exists.   (5 marks)

Description	Marks
Description	
Describes private IPv4 addressing	2
Limited description of private IPv4 addressing	1
Subtotal	**2**
Explanation	
Explains why private IPv4 addressing exists	3
Describes why private IPv4 addressing exists	2
Outlines why private IPv4 addressing exists	1
Subtotal	**3**
Total	**5**
Answers could include: Addresses in IPv4 are in either the private or public range. Private addresses are only usable in local networks – no traffic to private addresses will be routed on the Internet. The reason why private IP addressing exist is because there is a shortage of IPv4 addresses and some have been set aside for private use only to reduce the demand for public addresses. This allows private addresses to be reused in local networks around the world, with each local network having only one public address if need be.	
Accept other relevant answers.	

Question 25 **(20 marks)**

(a) Describe how SQL Injection can put a database at risk. (2 marks)

Description	Marks
Describes how SQL Injection can put a database at risk	2
States a fact about how SQL Injection can put a database at risk	1
Total	2

Answers could include:

SQL injection occurs whenever code accepts user input and then uses it directly within a query – this means a user can run their own arbitrary SQL commands remotely.

Accept other relevant answers.

(b) Identify how you would mitigate an SQL Injection as a network security threat. (1 mark)

Description	Marks
Identifies how an SQL Injection would be mitigated as a network security threat	1
Total	1

Answers could include:

The solution is to use parameterised queries – this will mean that user input will never be passed as an SQL command, only as data.

Accept other relevant answers.

(c) Describe what a notifiable data breach is and outline **four** actions that the company must take in response. (6 marks)

Description	Marks
Describes a notifiable data breach	2
States a fact about a notifiable data breach	1
Subtotal	2
For each action (4 x 1 mark)	
Outlines an action to be taken	1
Subtotal	4
Total	6

Answers could include:

A notifiable data breach is an incident where an attacker gains unauthorised access to individuals' private data being held by an organisation. Under Australian law, the breach must be likely to result in serious harm to one or more of the individuals and the organisation must have been unable to prevent the risk of that harm.

If this is the case, the company must:
•   contain the data breach
•   assess the damage done
•   notify the individuals involved and the Office of the Australian Information Commissioner
•   review the incident and consider actions to prevent future breaches.

Accept other relevant answers.

Question 25 (continued)

(d)   As a result of the data breach, the company is tightening its security processes and setting up several solutions. Describe how each of the following security solutions help to prevent or mitigate future attacks.

- using a virtual private network for all remote workers.
- access control lists.
- user training.   (6 marks)

Description	Marks
For each security solution (3 x 2 marks)	
Describes the purpose of a security solution	2
States a fact about the security solution	1
Total	6
Answers could include:	

- a virtual private network helps secure network access against hacking remote access services and ports by creating an encrypted tunnel for employees' data
- access control lists help to ensure that only intended users have access to resources, reducing the chances of attacks or unauthorised access to data
- user training helps reinforce security policies and procedures, protecting against social engineering attacks such as phishing.

Accept other relevant answers.

(e)   Identify **one** early method of encryption and describe its weaknesses.   (3 marks)

Description	Marks
Identifies an early method of encryption	1
Subtotal	1
Description	
Describes a weakness of the encryption method	2
States a fact about the encryption method	1
Subtotal	2
Total	3
Answers could include:	

Vigenère cipher
Uses a repeated key combing plain text with the key. Easily broken if we know the length of the key and use the character frequency method similar to the substitution cipher.

Accept other relevant answers.

When implementing some methods of encryption, you have the option of using either 128 bits or 256 bits for the key.

(f)   State **one** advantage and **one** disadvantage of using a smaller number of bits for an encryption key. (2 marks)

Description	Marks
States an advantage	1
States a disadvantage	1
Total	**2**
Answers could include: Advantage: The encryption and decryption process will be faster and use less resources. Disadvantage: Encryption is easier to break by brute-force.	
Accept other relevant answers.	