TIME CONSTRAINED ASSESSMENT

Unit:
Network Security and Cryptography

SAMPLE TIME CONSTRAINED ASSESSMENT
MARKING SCHEME

Markers are advised that, unless a task specifies that an answer be provided in a particular form, then an answer that is correct (factually or in practical terms) **must** be given the available marks. If there is doubt as to the correctness of an answer, the relevant NCC Education materials should be the first authority.

This marking scheme has been prepared as a **guide only** to markers and there will frequently be many alternative responses which will provide a valid answer.

Each candidate's script must be fully annotated with the marker's comments (where applicable) and the marks allocated for each part of the tasks.

Throughout the marking, please credit any valid alternative point.

Where markers award half marks in any part of a task, they should ensure that the total mark recorded for the task is rounded up to a whole mark.

Marker's comments:		
Moderator's comments:		
Mark:	**Moderated mark:**	**Final mark:**
Penalties applied for academic malpractice:		

Answer ALL questions

Question 1

Part a)

(LO 5,7,8) – 10 Marks

Describe in detail good practices (including appropriate protocols) and recommendations you will implement to:

i) Enhance the security of remote access to the corporate network.

ii) Restrict remote connections of Paramount Finance UK Ltd.'s employees only.

Marking Scheme

0-2 marks	3 marks	4-5 marks	6 marks	7-10 marks
No or Rudimentary *understanding of the scenario question and answers appear to be out of scope and does not provide enough information on good practices for additional security of remote desktop connections.*	***Brief*** *discussion or lists good practices for additional security of remote desktop connections. and configuration.*	***Generic*** *understanding of good practices for additional security of remote desktop connections. which include but not limited to the following: Use of RDP Gateways -Tunnelling RDP connects through IPSec, SSH, VPNs -Use of strong password policy -Implementing Two-Factor authentication - Software updates.*	***Consistent and detailed*** *understanding of good practices for additional security of remote desktop connections. which include but not limited to the following: Use of RDP Gateways -Tunnelling RDP connects through IPSec, SSH, VPNs -Use of strong password policy -Implementing Two-Factor authentication - Software updates.*	***Excellent and comprehensive*** *understanding of good practices for additional security of remote desktop connections. which include but not limited to the following: -Use of RDP Gateways -Tunnelling RDP connects through IPSec, SSH, VPNs -Use of strong password policy -Implementing Two-Factor authentication - Software updates.*
Rudimentary *discussion on restricting remote access to employees or not specifically addressing the type of*	***Briefly highlights or lists*** *security implementations on restricting remote access to employees.*	***Generic*** *discussion on restricting remote access to employees and does or not specific in addressing the*	***Some detailed discussion*** *and explanation on restricting remote access to employees.*	***Specific and excellent discussion*** *of restricting remote connections to employees only should include IP addressing,*

operating system, vulnerabilities and requirements identified in the scenario question	*Solution lacks detailed discussion addressing vulnerabilities and requirements stated in the scenario.*	*type of operating system and vulnerabilities and requirements stated in the scenario question.*	*Some discussion on enabling Network Level Authentication.* *Generic recommendation in preventing remote desktop brute force attacks.*	*firewalls, enabling network-level authentication etc.* *Set an account lockout policy to prevent brute force attacks.* *Changing the listening default ports.*
***No or Rudimentary** details on improving security on the remote client.*	***Brief** discussion on improving security on the remote client.*	***Some** details on improving security on the remote client.*	***Consistent** discussion on improving security on the remote client.*	***Excellent** details on improving security on the remote client which includes an up-to-date operating system, browsers, anti-virus installed etc.*

Question 1

Part b)

(LO 7,8) – 5 Marks

Using Paramount Finance UK Ltd.'s Network Architecture (Figure 1), design a new well-labelled network diagram:

i) To include Demilitarized Zone(s) (DMZs) to protect critical servers.

ii) Include VPNs for secure remote access for employees working off-site. Critical systems should also be identified.

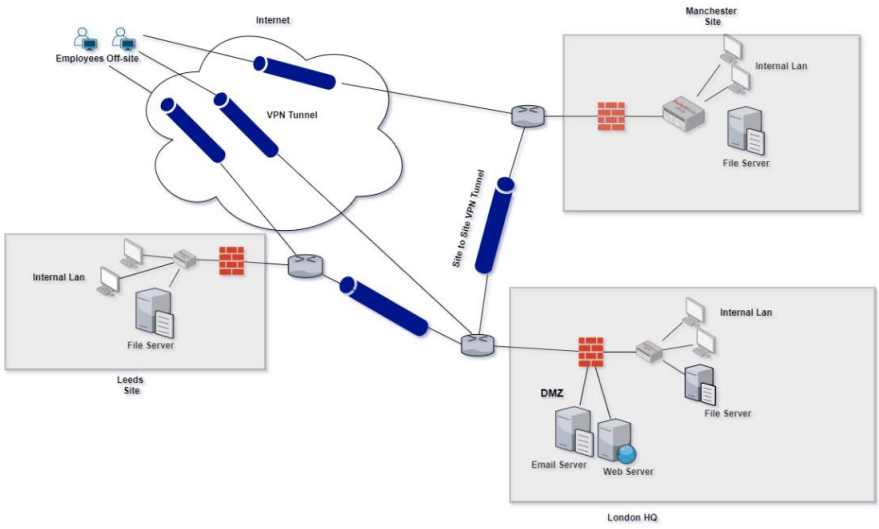

Figure 1. Suggested Solution (Award marks for similar diagram)

Marking Scheme

0-1 marks	2-3 marks	4-5 marks
Generic diagram not matching network diagram. Labelling/ positioning of key components is missing. *No clear identification of internal or critical components.*	*Similar diagram but key components are largely missing. The positioning of key components such as DMZ, file/mail/webserver is inconsistent.* *Some internal systems are identified but with poor labelling.*	*Diagram similar to the solution above. Firewall/DMZ correctly labelled for 3 sites. Positions of File, Mail and Web servers are accurate.* *Excellent and clear identification of critical and internal systems.*
No or vague representation of VPN tunnels for remote users and sites.	*The diagram includes VPNs but not clearly illustrated or some are missing*	*The diagram includes User to site VPNs for all 3 sites and Site to Site VPNs*

Question 1

Part c)

(LO 7,8) – 10 Marks

Explain in detail, reasons for your chosen network design **and** the purpose/functions of the Demilitarized Zones (DMZs) **and** VPNs.

Marking Scheme

0-2 marks	3 marks	4-5 marks	6 marks	7-10 marks
No or Generic/Basic *discussion on DMZs not based or specific to the scenario*	*Limited justification for design based on the scenario is mentioned but details on the functions of DMZs are missing.*	*Some justification for design based on the scenario is mentioned but details on the functions of DMZs are missing.*	*Consistent answers* ***based on the scenario*** *which include* ***most key features of DMZ (a subnetwork of the internal network*** *which* ***separates internal network from other untrusted*** *or public networks*	*Excellent* ***detailed*** *justification which includes* ***DMZ as a subnetwork of the internal network*** *which separates internal network from other untrusted or public networks based on the scenario.*
No or rudimentary discussion on secure RDP/ VPN as a secure, private, and encrypted communication	*Some key points on secure RDP/VPN as a secure, private, and encrypted communication tunnel for remote workers across the*	*A brief discussion on secure RDP/VPN as a secure, private, and encrypted communication tunnel for remote workers*	*Consistent discussion on secure RDP/VPN as a secure, private, and encrypted communication tunnel for remote workers across the*	*Excellent detailed justification for secure RDP or VPN as a secure, private, and encrypted communication tunnel for remote workers across the*

tunnel for remote workers across the public internet to all sites.	*public internet to all sites.*	*across the public internet to all sites.*	*public internet to all sites.*	*public internet to all sites.*
Vague or ambiguous explanations for including web and mail server at HQ in a DMZ.	*Highlights some few reasons for including web and mail server at HQ in a DMZ as it requires access by the public and remote employees.*	*Good attempt on reasons for including web and mail server at HQ in a DMZ as it requires access by the public and remote employees.*	*Adequate discussion on reasons for including web and mail server at HQ in a DMZ as it requires access by the public and remote employees.*	*Excellent justification for including web and mail server at HQ in a DMZ as it requires access by the public and remote employees.*
No clear justification for including file server internally behind a firewall.	*Justification for including File servers as part of an internal critical system is missing or lacks detail.*	*Justification for including File servers as part of an internal critical system are presented.*	*Justification for including File servers as part of an internal critical system are presented.*	*Justification for including File servers as part of an internal critical system are presented.*

Question 2

Part a)

(LO5 &6) – 5 Marks

Explain the difference between vulnerability management and vulnerability scanning.

Marking Scheme

0-1 marks	2-3marks	4-5 marks
No or Rudimentary *explanation on the difference between vulnerability management and vulnerability scanning*	***Some*** *discussion on the difference between vulnerability management and vulnerability scanning.*	***Excellent and detailed*** *explanation of the difference between vulnerability management and vulnerability scanning.*
No examples of vulnerability management processes and vulnerability scanning types.	*Some examples of vulnerability management processes and vulnerability scanning types.*	*Includes detailed examples of vulnerability management processes and vulnerability scanning types.*

Question 2
Part b)
(LO 5 &6) – 10 Marks

Explain the difference between known **and** unknown vulnerabilities **including** methods you will use to detect them on the webserver.

Marking Scheme

0-2 marks	3 marks	4-5 marks	6 marks	7-10 marks
No or vague *explanation of the difference between known and unknown vulnerabilities*	***Limited*** *discussion on the difference between known and unknown vulnerabilities*	***Some*** *discussion on the difference between known and unknown vulnerabilities*	***Consistent*** *discussion on the difference between known and unknown vulnerabilities*	***Detailed*** *explanation of the difference between known and unknown vulnerabilities*
No or rudimentary *discussion on methods which includes the use of vulnerability scanners, penetration testing and sound security practices.*	***Limited*** *discussion on methods which includes the use of vulnerability scanners, penetration testing and sound security practices.*	***Some*** *discussion on methods which includes the use of vulnerability scanners, penetration testing and sound security practices.*	***Consistent*** *details and discussion on methods which includes the use of vulnerability scanners, penetration testing and sound security practices.*	***Excellent and detailed*** *discussion on methods which includes the use of vulnerability scanners, penetration testing and sound security practices*
No examples *of vulnerability scanning tools and penetration testing techniques such as password cracking, dictionary attacks, SQL injection etc.*	***Limited*** *examples of vulnerability scanning tools and penetration testing techniques such as password cracking, dictionary attacks, SQL injection etc.*	***Some*** *examples of vulnerability scanning tools and penetration testing techniques such as password cracking, dictionary attacks, SQL injection etc.*	***Consistent*** *examples of vulnerability scanning tools and penetration testing techniques such as password cracking, dictionary attacks, SQL injection etc.*	***Detailed*** *discussion on examples of vulnerability scanning tools citing examples of port, network, database, and web application scanners. Includes penetration testing techniques such as password cracking, dictionary attacks, brute- force methods, SQL injection etc.*

Question 2
Part c)
(LO 5 &6) – 10 Marks

Explain authentication **including** methods that can be used to improve password security **and** authentication on the company's web server

Marking Scheme

0-2 marks	3 marks	4-5 marks	6 marks	7-10 marks
No or vague *discussion on authentication.*	***Basic*** *discussion on authentication* ***key details*** *such as preventing unauthorised access, access control, accountability, identification, and verification are* ***missing.***	***Some*** *discussion on authentication* ***but key details*** *such as preventing unauthorised access, access control, accountability, identification, and verification are* ***missing.***	***Consistent*** *discussion on authentication* ***but includes few details*** *such as preventing unauthorised access, access control, accountability, identification, and verification are* ***missing.***	***Excellent and detailed*** *discussion on authentication. Includes details such as preventing unauthorised access, access control, accountability, identification, and verification.*
No or vague *discussion on improving password security.*	***Lists*** *ways to improve password security includes enforcing complex/stronger passwords.* ***Discussion on implementing*** *security policy that includes but isn't limited to password expiration and complexity* ***are missing.***	***Limited*** *discussion on improving password security includes enforcing complex/stronger passwords* ***but*** *discussion on implementing security policy that includes but isn't limited to password expiration and complexity* ***are missing.***	***Some*** *discussion on improving password security includes enforcing complex/stronger passwords* ***but*** *discussion on implementing security policy that includes but isn't limited to password expiration and complexity* ***are missing***	***Excellent and detailed*** *discussion on improving password security includes enforcing complex/stronger passwords. Includes implementing security policy that includes but isn't limited to password expiration and complexity.*
No or vague details *on improving authentication.*	***Lists*** *some methods for improving authentication.*	***Briefly*** *mentions some methods for improving authentication using multi-factor authentication such as OTP, PINs, Biometrics etc.*	***Some*** *consistent discussion on improving authentication using multi-factor authentication such as OTP, PINs, Biometrics etc.*	***Excellent details*** *on improving authentication using multi-factor authentication such as OTP, PINs, Biometrics etc*

Question 3
Part a)
(LO 3 &4) – 10 Marks

Explain what a phishing attack is **and** discuss recommendations that should be implemented by Paramount Finance to prevent phishing attacks.

Marking Scheme

0-2 marks	3 marks	4-5 marks	6 marks	7-10 marks
No or Rudimentary *understanding of phishing attack*	***Generic*** *understanding of phishing attacks* ***but missing key points.***	***Brief*** *explanation of phishing attacks*	***Details are mostly consistent*** *with the explanation of phishing attacks*	***Detailed explanation*** *of phishing attacks with examples.*
No or vague *suggestions/recommendations.*	***Lists some*** *suggestions but missing key points on educating employees and conducting training sessions and mock phishing scenarios.*	***Brief details*** *on suggestions which involves educating employees and conducting training sessions with mock phishing scenarios.*	***Discussion includes some*** *appropriate suggestions such as educating employees and conducting training sessions with mock phishing scenarios as part of a penetration test or vulnerability assessment.*	***Discussion includes all*** *appropriate suggestions such as educating employees and conduct training sessions with mock phishing scenarios as part of a penetration test or vulnerability assessment.*
No or Rudimentary *recommendations which include details of creating or implementing security policy that includes but isn't limited to password expiration and complexity.*	***Lists a few some details but missing key details*** *on creating or implementing security policy that includes but isn't limited to password expiration and complexity.*	***Brief discussion but missing key points*** *which includes creating or implementing security policy that includes but isn't limited to password expiration and complexity.*	***Includes some details on*** *creating or implementing a security policy that includes but isn't limited to password expiration and complexity.*	***Detailed recommendations*** *on creating and implementing a security policy that includes but isn't limited to password expiration and complexity.*

Question 3
Part b)
(LO 3) – 10 Marks

Provide detailed recommendations that will protect devices such as laptops and removable media used by the company's employees for work against unauthorised access, data theft and deletion.

Marking Scheme

0-2 marks	3 marks	4-5 marks	6 marks	7-10 marks
Little to no *recommendation of encrypting customer data, files, disks or implementing email security.*	***Highlights some*** *recommendation of encrypting customer data, files, disks or implementing email security.*	***Brief overview*** *of protecting sensitive customer data by encrypting documents, files and disks or servers, employee computers etc or implementing email security.*	***Details are consistent*** *with strategies for protecting sensitive customer data by encrypting documents, files and disks or servers, employee computers etc or implementing email security.*	***Recommendation includes details*** *of protecting sensitive customer data by encrypting documents, files and disks or servers, employee computers etc and implementing email security.*
Rudimentary or no *examples of Full Disk, File System encryption, password-protecting documents, access controls solutions.*	***Lists examples*** *of Full Disk, File System encryption, password-protecting documents, access controls solutions.*	***Details highlight a few solutions*** *but for Full Disk, File System encryption solutions but not specific to the wide range of devices listed in the scenario.*	***Details include generic solutions*** *for Full Disk, File System encryption solutions but not specific to the wide range of devices listed in the scenario.*	***Details include specific examples*** *of Full Disk Encryption, File systems encryption solutions such as PGP, Symantec, password protecting, access control solutions etc. that can be used on the wide range of devices and operating systems listed in the scenario.*
No recommendations *on backups or examples that include data backup facilities off-site*	***Lists recommendations*** *on backups or examples that include data backup facilities off-site*	***Briefly highlights some*** *recommendations on backups or examples that include data backup facilities off-site*	***Consistent details on*** *recommendations that include backups and examples of data backup facilities off-site or automated backups*	***Excellent recommendations*** *that include backups and examples of data backup facilities off-site or automated backups.*

Question 3
Part c)
(LO 2,4) – 5 Marks

Describe what a digital signature is and explain its role in the security of email communications.

Marking Scheme

0-1 marks	2-3 marks	4-5 marks
No or Rudimentary *explanation of digital signature*	***Limited*** *explanation of digital signature*	***Detailed*** *explanation of digital signature.*
No or Rudimentary *discussion on the use of digital signature to ensure the integrity of email messages.*	***Some*** *consistent discussion on the use of digital signature to ensure the integrity of email messages.*	***Detailed explanation*** *which include guaranteeing the integrity or that the contents of an email message have not been altered. Sender verification and non-repudiation.*

Question 4
Part a)
(LO 1) – 10 Marks

Explain the functions of hashing algorithms for file integrity and select an appropriate one best suited for employees to verify the integrity of downloaded files. You should justify your selected algorithm.

Marking Scheme

0-2 marks	3 marks	4-5 marks	6 marks	7-10 marks
Rudimentary or no *detail on functions of hashing algorithms such as SHA-1, SHA-256 etc an algorithm that calculates the fixed-size bit string value from a file.*	***Limited discussion*** *on functions of hashing algorithms but with no examples of specific hash functions to be used.*	***Explanation includes an overview*** *of functions of hashing algorithm such as SHA-1, SHA-2, SHA-256 etc as an algorithm that calculates the fixed-size bit string value from a file.*	***Consistent details*** *on functions of hashing algorithms such as SHA-1, SHA-2, SHA-256 etc as an algorithm that calculates the fixed-size bit string value from a file.*	***Excellent discussion*** *functions of hashing algorithms such as SHA-1, SHA-2, SHA-256 etc as an algorithm that calculates the fixed-size bit string value from a file.*
No justification for choosing a specific hashing algorithm such as SHA-1,	***Lists few*** *justification for choosing a specific hashing algorithm* ***but***	***Brief*** *justification for choosing a specific hashing algorithm such*	***Detailed and consistent*** *justification for choosing a specific hashing*	***Excellent justification*** *for choosing a specific hashing algorithm such as SHA-1,*

SHA-2 over MD2, MD4, MD5.	***not** comparison with weaker algorithms*	*as SHA-1, SHA-2 over MD2, MD4, MD5.*	*algorithm such as SHA-1, SHA-2 over MD2, MD4, MD5.*	*SHA-2 over MD2, MD4, MD5.*
***No detail** presented on hashing algorithms as one-way functions to verify the integrity of a downloaded file has not been modified or altered checks during or after a file transfer session.*	***Lists hashing algorithms** as one-way functions to verify the integrity of a downloaded file have not been modified or altered checks during or after a file transfer session.*	***Brief overview** of hashing algorithms as one-way functions to verify the integrity of a downloaded file has not been modified or altered checks during or after a file transfer session.*	***Details consistent** with hashing algorithms as one-way functions to verify the integrity of a downloaded file has not been modified or altered checks during or after a file transfer session.*	***Justification includes excellent details** of hashing algorithms as one-way functions to verify the integrity of a downloaded file has not been modified or altered checks during or after a file transfer session.*

Question 4

Part b)

(LO 2, 3) – 10 Marks

Explain Public Key Infrastructure (PKI) **and** its benefits to support secure information exchange over insecure networks.

Marking Scheme

0-2 marks	3 marks	4-5 marks	6 marks	7-10 marks
***Ambiguous/rudimentary** understanding of asymmetric encryption / PKI*	***Key points** highlighting some understanding of asymmetric encryption / PKI*	***Adequate understanding** of asymmetric encryption / PKI*	***Detailed understanding** of asymmetric encryption / PKI*	***Excellent understanding** of asymmetric encryption / PKI*
***No or vague discussion** on the benefits of PKI*	***Missing Key points** of the benefits of PKI but*	***Some key points but lacks details** on the benefits of PKI*	***Includes some detail** on the benefits of PKI*	***Excellent and detailed** discussion on the benefits of PKI*
***No or rudimentary** discussion on PKI use in secure delivery of cryptographic keys, internet security and internal, verify sending identity and ensure privacy.*	***Missing Key points** on PKI use in secure delivery of cryptographic keys, internet security and internal networks, verify sending*	***Some key points but lack details** on PKI use in secure delivery of cryptographic keys, internet security and internal*	***Includes some details** on PKI use in secure delivery of cryptographic keys, internet security and internal networks,*	***Excellent and detailed** discussion on PKI use in secure delivery of cryptographic keys, internet security and internal networks, verify*

	identity and ensure privacy.	*networks, verify sending identity and ensure privacy.*	*verify sending identity and ensure privacy*	*sending identity and ensure privacy.*

Question 4

Part c)

(LO 9) – 5 Marks

Suppose an employee off-site intends to access a file server remotely using a public Wi-Fi connection from a local café. Explain the vulnerabilities inherent in open-public wireless networks.

Marking Scheme

0-1 marks	**2-3marks**	**4-5 marks**
The discussion does not show *an understanding of open-public wireless networks*	***Demonstrates some understanding*** *of open-public wireless networks*	***Detailed understanding*** *of open-public wireless networks*
No or Rudimentary *discussion on vulnerabilities inherent in open-public wireless networks.*	***Highlights some*** *but not all vulnerabilities which include man-in-the middles attacks, sniffing attacks, malware distribution, rogue APs.*	***Detailed discussion*** *includes man-in-the middles attacks, sniffing attacks, malware distribution, rogue APs.*

Learning Outcomes matrix

Task	Learning Outcomes assessed	Marker can differentiate between varying levels of achievement
1	LO5 LO7 LO8	Yes
2	LO5 LO6	Yes
3	LO2 LO3 LO4	Yes
4	LO1 LO2 LO3 LO9	Yes

Grade descriptors

Learning Outcome	Pass	Merit	Distinction
Understand the most common types of cryptographic algorithm	Demonstrate adequate understanding of common types of cryptographic algorithm	Demonstrate robust understanding of common types of cryptographic algorithm	Demonstrate highly comprehensive understanding of common types of cryptographic algorithm
Understand the Public-key Infrastructure	Demonstrate adequate level of understanding	Demonstrate robust level of understanding	Demonstrate highly comprehensive level of understanding
Understand security protocols for protecting data on networks	Demonstrate adequate understanding of security protocols	Demonstrate robust understanding of security protocols	Demonstrate highly comprehensive understanding of security protocols
Be able to digitally sign emails and files	Demonstrate ability to perform the task	Demonstrate ability to perform the task consistently well	Demonstrate ability to perform the task to the highest standard
Understand Vulnerability Assessments and the weakness of using passwords for authentication	Demonstrate adequate level of understanding	Demonstrate robust level of understanding	Demonstrate highly comprehensive level of understanding
Be able to perform simple vulnerability assessments and password audits	Demonstrate ability to perform the task	Demonstrate ability to perform the task consistently well	Demonstrate ability to perform the task to the highest standard
Be able to configure simple firewall architectures	Demonstrate adequate level of understanding and ability	Demonstrate robust level of understanding and ability	Demonstrate highly comprehensive level of understanding and ability
Understand Virtual Private Networks	Demonstrate adequate level of understanding	Demonstrate robust level of understanding	Demonstrate highly comprehensive level of understanding
Be able to deploy wireless security	Demonstrate ability to perform the task	Demonstrate ability to perform the task consistently well	Demonstrate ability to perform the task to the highest standard