Ques:

A. What is the legal impact to an organization if three pillars of Cyber Security fail? [1 + 1 * 4 = 5]

B. For each of the following assets, assign a low, moderate, or high impact level for the loss of confidentiality, availability, and integrity, respectively. Justify your answers.
a. Amazon store online with flash sales every week.
b. Housing development bidding application website for government projects.
c. Apollo App containing reports and data of patients belonging to multiple diagnostic labs.
d. Horse Riding betting application, having user's activity and bidding details.

Ans:

Legal Implication of data breach: the laws requiring data protection and data privacy vary from country to country, for example, If your business is U.S.-based, you have to comply with state-specific laws, as no federal privacy law is in place; also if you're operating from the EU, you must comply with the GDPR.

Scope of Penalties:
The likelihood and severity of fines can vary depending on the level of breach, number of individuals affected and regional jurisdiction. Country- and state-specific laws vary, so your legal team will be of great help in defining your firm's liability in case of a data or privacy breach.

Litigation
One may be aware of the risks involved in cyber-attacks, but legal action may be still brought if you fail to first notify the concerned individuals and authorities about the data breach.

	Confidentiality	Integrity	Availability
Amazon	Moderate	High	High
HD	High	Low	High
Apollo	High	Low	High
Horse Riding	Moderate	Moderate	High

Ques:

Consider you are an individual in finance domain [1 + 2 + 2 = 5]
a. Explain what types of cyber-attacks can happen, and how to handle those?
b. As a user, what you will do in order to prevent your system from being hacked by a hacker?
c. What are the sources of cyber-attacks? And how it can be prevented, explain with example?

a.
1. SQL Injection. 2. Phishing Attack. 3. Physical Intrusion - use of Defense in depth solutions to ensure fail-safe are in place are at all levels, ensuring all the solutions are patched and up-date and performing periodic security assessments. 4. Insider Attacks - Separation of roles, least privilege access, reviewed security policies for all operation procedures 5. Customer accounts compromise - User awareness and enabling multiple factors of authentication 6. Social Engineering attacks - Periodic attack simulation, user awareness and training thorough all means 7. MITM attack (Man in the middle attack)

b.
1. Perform safe web search and validate that website uses SSL certificate by seeing the padlock sign in the browser address bar 2. Ensure Endpoint protection 3. Install genuine operating system and anti-virus with license 4. Keep both above mentioned updated with patches and virus definition updates. 5. Control access to system 6. Multifactor authentication enabled for the login roles. 7. Refrain from using free Wi-Fi. 8. Secure connection to the servers and disabling un-used ports.

c.
1. Vulnerability Exploits due to unpatched software or systems in the network - regular patching and periodic security review of the systems
2. DDoS Attacks - IDS/IPS, Firewall, DDoS prevention solutions
3. Malware - Anti-malware, network security solutions and user awareness
4. Social engineering attacks - Periodic simulations and user awareness
5. Sponsored attacks (state / competitor) - Defense in depth and periodic simulations to check readiness and effectiveness
6. Insider threat / Disgruntled employees - Separation of roles, stringent security policies for all operational procedures.

Hackers, Phishing emails**,** Malicious insiders**,** social engineering**,** Man in the middle attack, Malwares, Denial of service attack, MITM attack,

Ques:

a. Explain how Lipner's integrity matrix model meets the requirements or constraints for commercial models.
b. Let's suppose we have a network that requires 29 subnets while maximizing the number of hosts addresses available on each subnet. How can we accomplish this? Explain? [3 x 2 = 6]

a.

Lipner described some integrity concerns you might find in a commercial data processing environment:

1 Users will not write their own programs but use existing production software.

2 Programmers develop and test applications on a nonproduction system, possibly using contrived data.

3 Moving applications from development to production requires a special process.

4 This process must be controlled and audited.

5 Managers and auditors must have access to system state and system logs.

Lipner devised his Integrity Matrix Model to handle the constraints via a combination of BLP and Biba Integrity.

There are two confidentiality levels:

- Audit Manager (AM): system audit and management.
- System Low (SL): all other processes.

In addition, there are three confidentiality categories:

- Production (SP): production code and data.
- Development (SD): programs under development.
- System Development (SSD): system programs in development.

Security levels (both confidentiality and integrity) are assigned to subjects based on their roles in the organization and their need to know.

User Role Confidentiality Integrity

Ordinary users (SL,{SP}) (ISL,{IP})

Application developers (SL,{SD}) {ISL,{ID})

System programmers (SL,{SSD}) {ISL,{ID})

System managers/auditors (AM,{SP,SD,SSD}) {ISL,{IP,ID})

System controllers (SL,{SP,SD}) {ISP,{IP,ID})

and downgrade

Here, downgrade means the ability to move software (objects) from development to production.

Conclusion:

Lipner developed a hybrid policy using both BLP and Biba's Strict Integrity to address commercial integrity concerns.

Some modifications relating to tranquility were required to allow moving applications from the development to production domains.

The result is acceptable but not entirely intuitive. Perhaps an entirely new modeling paradigm would be preferable.

b.

We need /29 subnets; therefor CIDR value will be 29.

Hence, we need to borrow 5 bits from the host, Now, in the last octet there will 3 Host bits left for the Host IPs. So, Total number of IPs will be = 2^3 = 8
And, out of 8 two will be used for Network ID & Broadcast IDs.
So, the total number of IPS available will be = (8-2) = 6 Host IPs for allocation is each network.

Ques:

Consider you are a Security Architect in your organization. A complex system has more changes of having security problems. In addition, too complex the system is, too many opportunities for something to go wrong. You would like to create small reusable components for repeated functionality. Which design principle is applicable in this scenario? Describe the design principle. Clearly explain the design principle with an example. [1 + 2 + 2 = 5]

Ans:

Modularity design principle, as It states that the security mechanism must be developed:
- as separate and protected modules, and
- using the modular architecture -

The module structure helps us in, focusing on the structure design and implementation of the single cryptographic module, focusing on the mechanism to protect the module from tampering, and migrating to new technology or upgrading the features of security mechanism with modifying the entire system

For Example:

AWS - as it is built on Microservices which has a separate module for authentication, authorization, provisioning, monitoring. Changing one module doesn't impact the entire system

Ques:

Suppose you are a network admin, specify which protocols will be applied in below scenarios [1 X 5 = 5]

a. We want to allow users to login to a host from a remote location and take control as if they were sitting at the machine

b. We want to allow the download/upload of files between a client/server

c. To send email messages from clients to servers over the internet

d. To transfer web page from server to client

e. When no handshaking between sender and receiver is required

Ans:

a. Telnet

b. FTP

c. SMTP

d. HTTP

e. UDP

Ques:

Some Host H1 has IP address 192.168.1.97 and is connected through two routers ROU1 and ROU2 to another host H2 with IP address 192.168.1.80. Router ROU1 has IP addresses 192.168.1.135 and 192.168.1.110. ROU2 has IP addresses 192.168.1.67 and 192.168.1.155. The netmask used in the network is 255.255.255.224.

Given the information above, how many distinct subnets are guaranteed to already exist in the network? Explain it with proper steps [2 + 2 = 4]

Ans:

3

IP addresses given in the problem are of type Class C, and default mask is 24 for Class C

Here given mask is 27 bits (11111111 11111111 11111111 11100000)

subnet ID: 3 bits

existing subnets: 011, 010 and 100