1. **Using the 7 IT domains, select ALL the domains your company utilizes. Next, describe why you selected each of the domains (how does your company utilize them).**

- User Domain:
  - Includes all individuals who access the company's systems, such as employees, contractors, and third-party service providers. This domain is utilized for managing access rights and training users on security policies.
- Workstation Domain:
  - Consists of all end-user devices, such as desktops in the front desk area, laptops used by doctors, and computers in examination rooms. These devices are crucial for daily operations like patient check-ins and medical examinations.
- LAN Domain:
  - Encompasses the internal network within iSeeU Eyecare's premises, connecting various workstations, servers, and medical equipment. This domain supports the seamless flow of data and communication within the facility.
- LAN-to-WAN Domain:
  - This domain manages the interface between the local area network and wider networks, such as the internet or connections to other locations. It is crucial for secure data transmission, including patient information sharing between sites.
- WAN Domain:
  - The wide area network domain includes the connectivity between different iSeeU Eyecare locations, allowing for resource sharing and centralized data management across the organization.
- Remote Access Domain:
  - Covers the methods and technologies used by staff to access the company's network remotely, essential for doctors working remotely or accessing information from outside the clinic.
- System/Application Domain:
  - This domain includes all servers and applications used for patient management, billing, and medical records. It is fundamental to the storage, processing, and management of patient data and financial transactions.

2. **Using the selected domains from item 1 above, select the two most important domains your company needs to address. Describe why each of the two domains you selected is the two most important.**

- System/Application Domain:
  - The most critical, as it directly handles sensitive patient data and financial information. Ensuring its security is vital for compliance with HIPAA and PCI DSS, and for maintaining patient trust.
- LAN-to-WAN Domain:
  - Crucial for safeguarding data in transit. This domain's security ensures that patient information and financial data transmitted between sites and over the internet are protected against interception and breaches.

3. **Using the 7 IT domains, what domains will NOT be as important for your company if Zero Trust was implemented? Describe why they will NOT be as important for your company.**

- LAN Domain:
    - Under a Zero Trust architecture, the internal network's traditional perimeter defenses become less important. Access decisions are made based on identity and context, not network location.
- Remote Access Domain:
    - Zero Trust treats all access requests with equal skepticism, whether they originate inside or outside the network. This diminishes the traditional role of the Remote Access Domain, as secure access controls and authentication are uniformly applied.

4. **Using the Compliance and Audit video, the slide entitled "Other Types of Supporting Documents," AND the Information Gathering and Reporting video slide entitled "Digital Forensics Reporting," what three documents listed or mentioned are the most important documents you would deliver for:**
    a. **a Ransomware case to a digital forensics investigator? Describe why each of the selected items is the most important document.**
        - Incident Logs:
            - Provide a timeline and context for the ransomware attack, helping investigators understand the entry point and spread.
        - Backup Files:
            - Crucial for assessing the impact of the attack on data integrity and for recovery purposes without paying the ransom.
        - System Images:
            - Offer a snapshot of the compromised systems for forensic analysis, aiding in identifying the ransomware strain and potential data leaks.

    b. **a data breach case to a digital forensics investigator? Describe why each of the selected items is the most important document.**
        - Access Logs:
            - Vital for tracking unauthorized access attempts, helping to identify the compromised data's scope and the attacker's methodology.
        - Network Traffic Logs:
            - Important for detecting unusual data flows that may indicate data exfiltration, offering insights into the breach's nature and scale.
        - Data Inventory Documentation:
            - Crucial for understanding which data was potentially compromised, guiding the response and mitigation strategies to protect affected individuals and prevent future breaches.