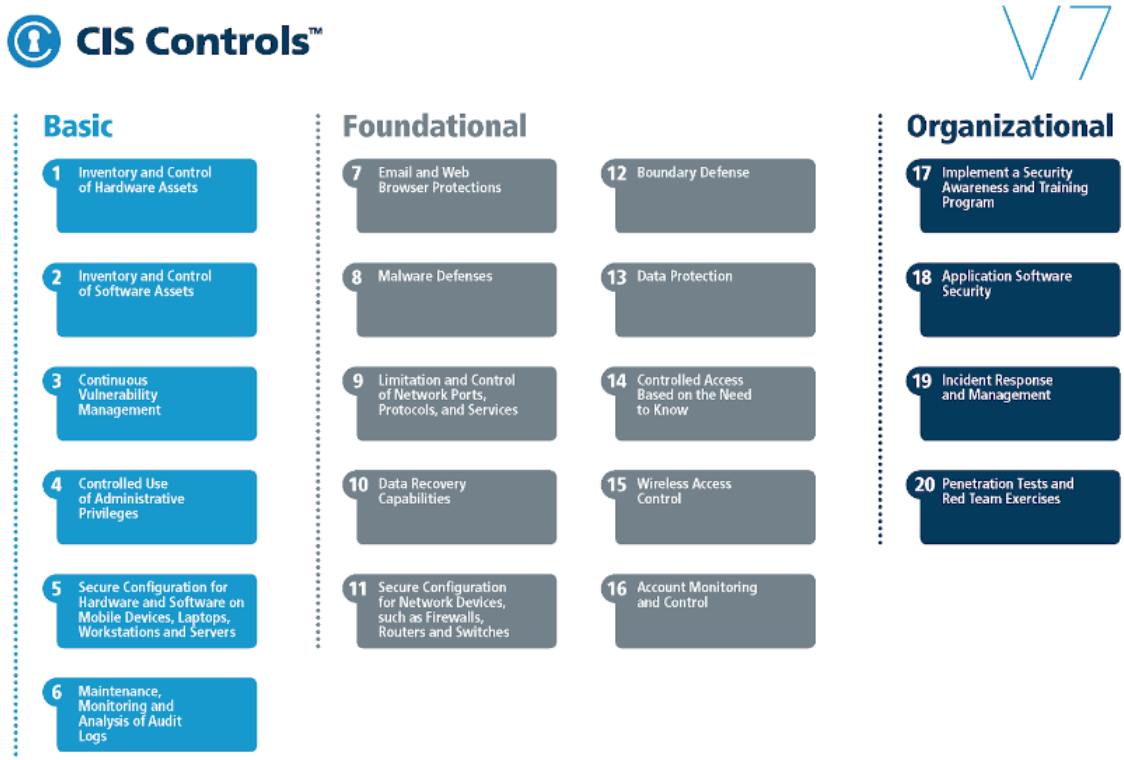
Saumyaa Prajapat
21BCI0265

Task 6

Understanding CIS

The CIS Critical Security Controls (CIS Controls) are a prioritized set of Safeguards to mitigate the most prevalent cyber-attacks against systems and networks. They are mapped to and referenced by multiple legal, regulatory, and policy frameworks.



Basic:

1. **Inventory and Control of Hardware Assets:** This involves maintaining an accurate record of all physical IT equipment, ensuring proper tracking, management, and security measures are in place for each asset to prevent loss and unauthorized access.

2. **Inventory and Control of Software Assets:** Similar to hardware assets, this focuses on tracking and managing software licenses, versions, and installations across the organization to ensure compliance, security, and efficient resource allocation.

3. **Continuous Vulnerability Management:** Regularly identifying, assessing, and mitigating vulnerabilities in hardware and software to minimize the risk of exploitation by malicious actors or malware.

4. **Controlled Use of Administrative Privileges:** Implementing strict controls over administrative access to systems and data, limiting privileges to authorized personnel only, thereby reducing the potential for unauthorized changes or breaches.

5. **Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers:** Configuring devices with security best practices in mind to minimize potential vulnerabilities and ensure a strong defense against potential attacks.

6. **Maintenance, Monitoring, and Analysis of Audit Logs:** Consistently reviewing and analyzing audit logs to detect and respond to potential security incidents, ensuring the integrity and confidentiality of logged data.

Foundational:

7. **Email and Web Browser Protections**: Implementing security measures to safeguard against email and web-based threats, such as phishing and malware, to reduce the risk of unauthorized access or data breaches.

8. **Malware Defenses:** Deploying effective anti-malware solutions and strategies to detect, prevent, and remediate malware infections that could compromise the organization's systems and data.

9. **Limitation and Control of Network Ports, Protocols, and Services:** Managing and controlling network communication channels to minimize potential avenues for cyberattacks and unauthorized data transfers.

10. **Data Recovery Capabilities**: Establishing procedures and tools for data backup and recovery to ensure business continuity and data integrity in the event of data loss or system disruptions.

11. **Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches:** Applying robust security configurations to network infrastructure devices to prevent unauthorized access and maintain the confidentiality of network traffic.

12. **Boundary Defense**: Implementing security measures at network boundaries to monitor and control incoming and outgoing traffic, preventing unauthorized access and data leakage.

13. **Data Protection:** Applying encryption, access controls, and other security measures to safeguard sensitive data throughout its lifecycle, both in transit and at rest.

14. **Controlled Access Based on the Need to Know:** Granting access to resources based on the principle of least privilege, ensuring that users can only access the information necessary for their roles and responsibilities.

15. **Wireless Access Control:** Implementing secure authentication and encryption mechanisms for wireless networks to prevent unauthorized access and eavesdropping.

16. **Account Monitoring and Control:** Regularly monitoring user accounts and their activities to detect and respond to suspicious or unauthorized actions that could compromise security.

Organizational:

17. Implement a Security Awareness and Training Program: Educating employees about security best practices and potential threats to foster a security-conscious organizational culture.

18. **Application Software Security:** Integrating security measures into the software development lifecycle to identify and mitigate vulnerabilities in applications and prevent potential exploitation.

19. **Incident Response and Management:** Establishing a well-defined plan and procedures to effectively respond to and manage security incidents, minimizing the impact of breaches or attacks.

20. **Penetration Tests and Red Team Exercises:** Conducting controlled simulated attacks to identify vulnerabilities and weaknesses in the organization's security posture, enabling proactive improvements to defenses.