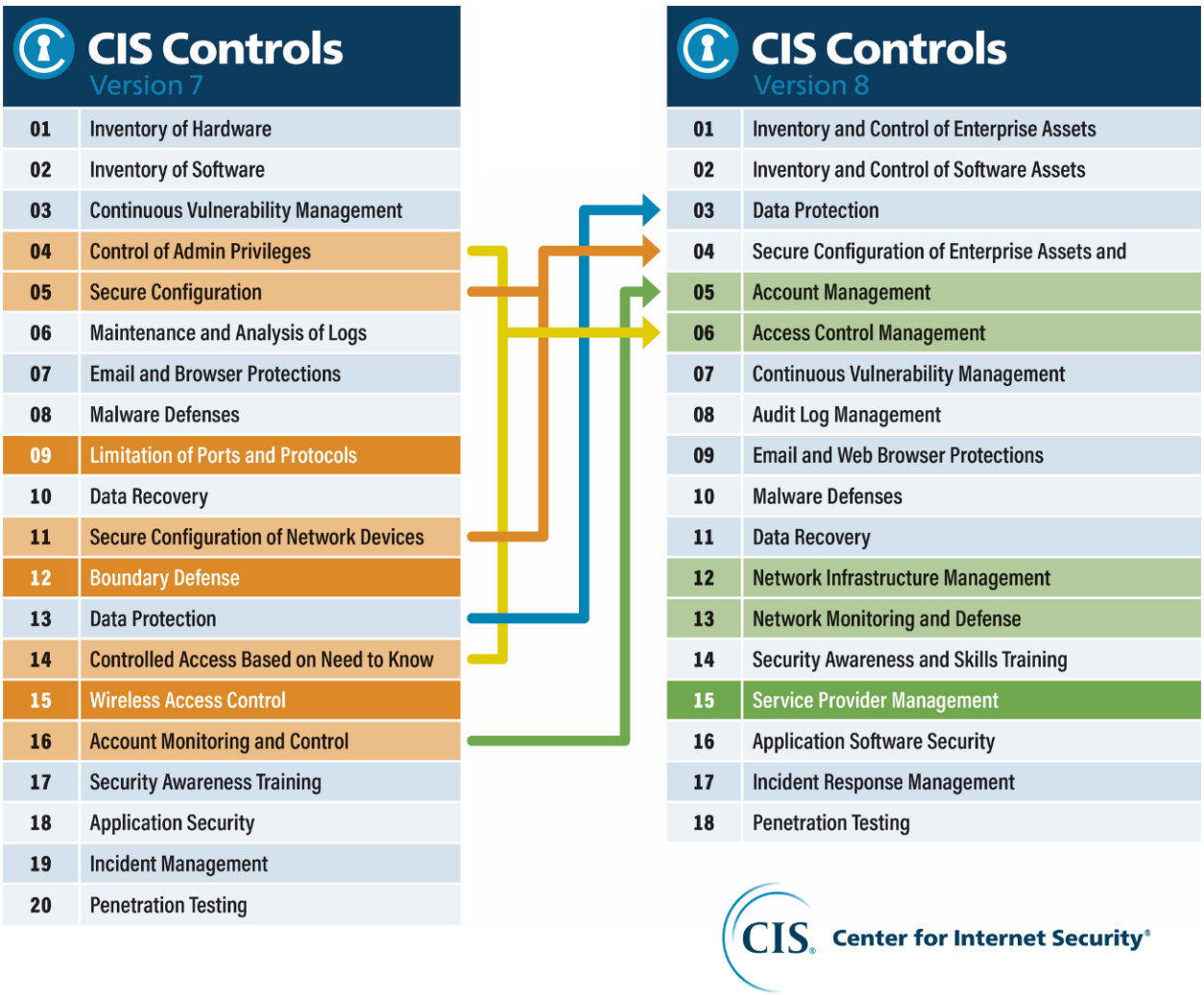
Task – 6

Name : C DEVAKI NANDAN REDDY

Understanding CIS Policy version 7and write about them



CIS Controls Version 7	
01	Inventory of Hardware
02	Inventory of Software
03	Continuous Vulnerability Management
04	Control of Admin Privileges
05	Secure Configuration
06	Maintenance and Analysis of Logs
07	Email and Browser Protections
08	Malware Defenses
09	Limitation of Ports and Protocols
10	Data Recovery
11	Secure Configuration of Network Devices
12	Boundary Defense
13	Data Protection
14	Controlled Access Based on Need to Know
15	Wireless Access Control
16	Account Monitoring and Control
17	Security Awareness Training
18	Application Security
19	Incident Management
20	Penetration Testing

CIS Controls Version 8	
01	Inventory and Control of Enterprise Assets
02	Inventory and Control of Software Assets
03	Data Protection
04	Secure Configuration of Enterprise Assets and
05	Account Management
06	Access Control Management
07	Continuous Vulnerability Management
08	Audit Log Management
09	Email and Web Browser Protections
10	Malware Defenses
11	Data Recovery
12	Network Infrastructure Management
13	Network Monitoring and Defense
14	Security Awareness and Skills Training
15	Service Provider Management
16	Application Software Security
17	Incident Response Management
18	Penetration Testing

CIS Center for Internet Security®

The Center for Internet Security (CIS) develops and maintains a set of best practice guidelines and security controls known as the CIS Controls and CIS Benchmarks. These guidelines are designed to help organizations improve their cybersecurity posture. The most recent version as of my last knowledge update in January 2022 is CIS Policy Version 7. These policies help organizations to establish and maintain effective security policies and practices. Here is a brief overview of some of the key elements of CIS Policy Version 7:

1. **CIS Controls:** CIS Policy Version 7 is closely aligned with the CIS Controls, which are a prioritized set of actions designed to mitigate the most common and dangerous cyber threats. These controls provide a roadmap for organizations to improve their security posture.
2. **Policy Development:** CIS Policy Version 7 emphasizes the importance of well-defined policies as the foundation of an organization's cybersecurity program. It provides guidance on how to develop, maintain, and enforce security policies effectively.
3. **Data Protection:** Data protection is a significant focus in CIS Policy Version 7. It provides guidance on how to classify and protect sensitive data, including recommendations for encryption, data retention, and access control.
4. **Identity and Access Management:** This section outlines best practices for managing user identities and controlling access to systems and data. It includes guidance on strong authentication, access control, and account management.
5. **Incident Response and Recovery:** CIS Policy Version 7 places a strong emphasis on incident response and recovery planning. It provides guidance on how to develop an effective incident response plan, including procedures for detection, reporting, and recovery from security incidents.
6. **Security Awareness and Training:** Educating employees about cybersecurity is crucial. The policy provides recommendations for security awareness and training programs, including topics, training frequency, and monitoring.
7. **Network Security:** It covers various network security aspects, such as network segmentation, firewall management, and intrusion detection/prevention systems. The policy advises on securing network infrastructure to prevent unauthorized access and data breaches.
8. **Endpoint Security:** This section focuses on securing individual devices (endpoints) within the organization. It provides guidance on implementing antivirus software, host-based firewalls, and secure configuration of endpoints.
9. **Mobile Device Management:** With the proliferation of mobile devices in the workplace, CIS Policy Version 7 includes recommendations for managing and securing mobile devices effectively. This includes mobile device security policies and procedures.
10. **Physical Security:** Physical security is often overlooked but is a critical aspect of overall cybersecurity. The policy provides recommendations for securing physical assets, such as data centers and server rooms.
11. **Cloud Security:** With the increasing use of cloud services, this version of the policy includes guidance on how to secure cloud-based environments, including data storage and applications.

CIS Policy Version 7 aims to provide comprehensive guidance for organizations to establish and maintain effective cybersecurity policies and practices. It reflects the evolving threat landscape and emerging technologies, making it a valuable resource for organizations looking to enhance their cybersecurity posture. Organizations are encouraged to review the specific details of the policy and align them with their unique security needs and compliance requirements.