TASK - 6

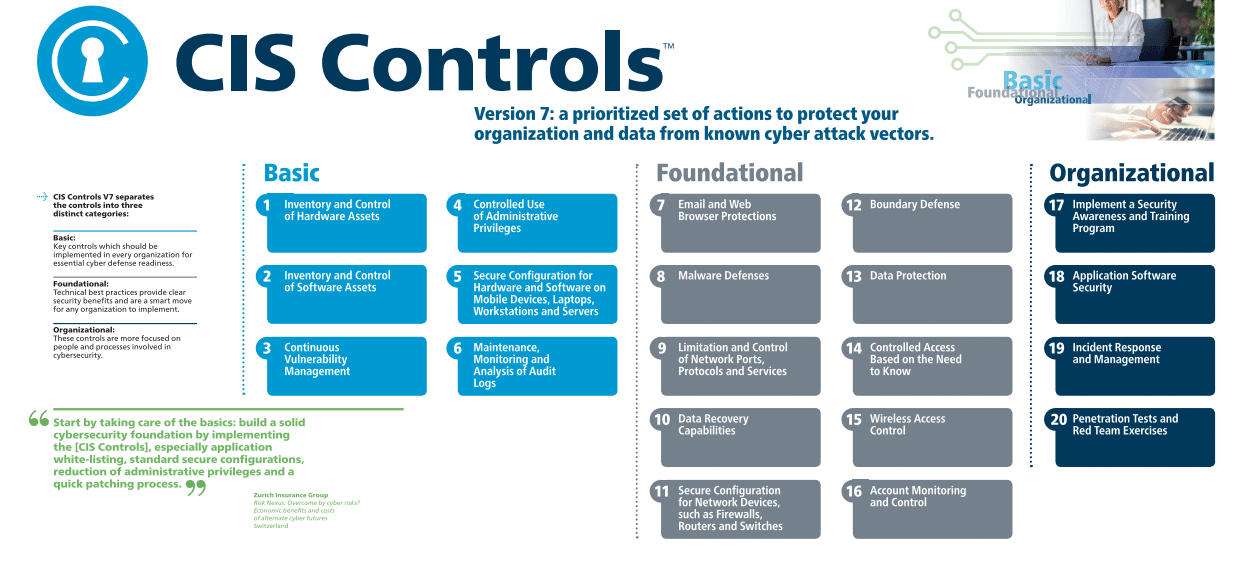
[Bhumireddy Thanmaye 21BCI0013](mailto:bhumireddy.thanmaye2021@vitstudent.ac.in)

UNDERSTANDING OF CIS CONTROLS

CIS Controls broadly classified into 3 categories

1. Basic
2. Foundational
3. Organizational

**Basic:** key controls which should be implemented in every organization to achieve essential cyber defense readiness.



**1. Inventory of Authorized and Unauthorized Devices.**

Organizations must actively manage all the hardware devices on the network, so only authorized devices are given access. Unauthorized and unmanaged devices need to be prevented from gaining access. If they happen to achieve access, they need to be discovered, before any damage is inflicted.

**2. Inventory of Authorized and Unauthorized Software.**

Organizations must actively manage all software on the network, so only authorized software is installed and can execute. Security measures like application whitelisting can enable organizations to find unauthorized software and prevent installation or execution quickly.

**3. Continuous Vulnerability Management.**

Organizations need to continuously acquire, assess and take action on new information (e.g., software updates, patches, security advisories, and threat bulletins) to identify and remediate vulnerabilities and minimize the window of opportunity for attackers

**4. Controlled Use of Administrative Privileges.**

This control requires companies to use automated tools to monitor user behavior and keep track of assignments, and configuration of administrative privileges on computers, networks, and applications.

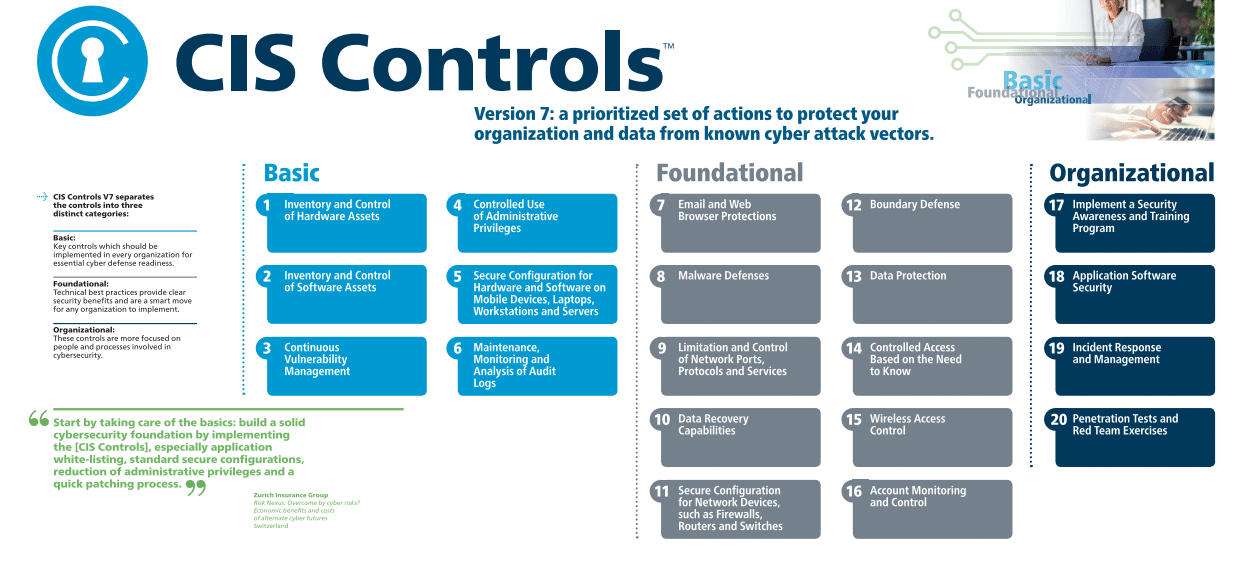
**5.Secure Configuration for Hardware and Software on Mobile Device,Laptops,Workstations and Servers**

Companies need to establish, implement and manage the security configuration of laptops, servers, and workstations. Companies have to follow rigorous configuration and change control processes to prevent attackers from exploiting vulnerable services and settings.

**6. Maintenance, Monitoring, and Analysis of Audit Logs.**

Organizations need to collect, manage and analyze audit logs to use in the investigation and recovery process of an attack.Lack of security logging and analysis enables attackers to hide their location and activities in the network. Even after it has been revealed which systems have been compromised, without complete logging records, it will be difficult to measure the damage extent and remediate the vulnerability.

**Foundational:** Technical best practices provide clear security benefits and are a smart move for any organization to implement.



**7. Email and Web Browser Protections:**

Given the prevalence of email and web-based attacks, this control provides guidance on securing email systems and web browsers to prevent phishing and malware attacks.

**8.Malware Defenses:**

Protecting against malware is essential. This control offers strategies for defending against malware threats, including antivirus software and regular updates.

**9. Limitation and Control of Network Ports, Protocols, and Services:** Reducing the attack surface by controlling network ports, protocols, and services is the focus of this control. It advises organizations on which ports and services to disable or limit.

**10.Data Protection:**

This control focuses on data security, including encryption, data loss prevention, and protecting sensitive information from unauthorized access or disclosure.

**11.Secure Configuration for Network Devices, such as Firewalls and Routers:**

Properly configuring network devices is vital for maintaining a secure network infrastructure. This control provides guidelines for secure configuration practices.

**12. Boundary Defense:**

Protecting the network perimeter is crucial. This control covers strategies for implementing strong boundary defenses against external threats.

**13.Data Protection and Privacy:**

Building on Control 10, this control specifically addresses data privacy requirements, including compliance with data protection regulations such as GDPR or HIPAA.

**14.Secure Configuration for Cloud and Virtualization:**

As organizations increasingly use cloud and virtualization technologies, this control provides recommendations for securing these environments.

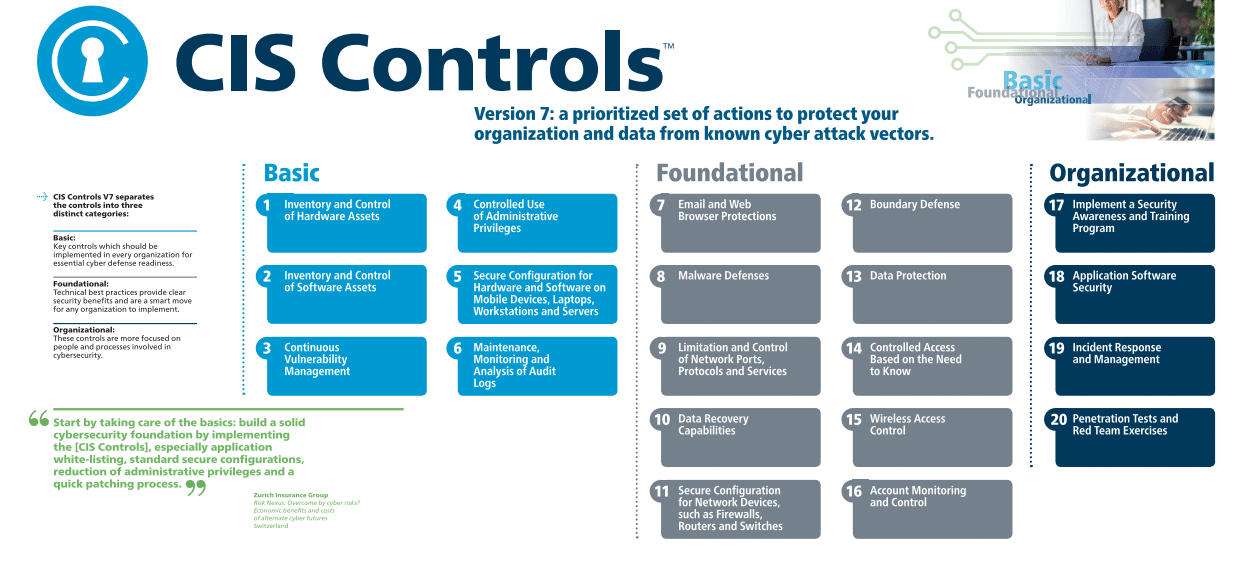
**15.Incident Response and Management:**

Preparing for and responding to security incidents is a critical aspect of cybersecurity. This control outlines the steps to take when a security incident occurs.

**16. Penetration Testing, Red Teaming, and Threat Hunting:**

Regular testing of your organization's security defenses is essential. This control covers penetration testing, red teaming, and proactive threat hunting activities.

**Organizational:** These remaining controls have a stronger focus on the people and processes involved in cybersecurity.



**17. Security Skills Assessment and Appropriate Training to Fill Gaps:** Ensuring that your workforce has the necessary cybersecurity skills is vital. This control addresses the importance of assessing skills and providing training as needed.

**18.Secure Software Development:**

Building secure software from the ground up is crucial. This control provides guidance on integrating security into the software development lifecycle.

**19.Supply Chain Security:**

The supply chain can be a weak link in cybersecurity. This control focuses on ensuring the security of products and services from third-party vendors.

**20.Identity and Access Management:**

Controlling and managing user access to systems and data is a fundamental aspect of security. This control provides recommendations for effective identity and access management practices.