elaboration and classification of critical control requirements for an IT infrastructure audit:

1**. CSC Implementation Group 1: Basic Cyber Hygiene Controls**

I. Inventory and Control of Hardware Assets:

Maintain an up-to-date inventory of all authorized hardware devices.

Ensure only authorized devices are allowed to connect to the network.

II. Inventory and Control of Software Assets:

Maintain an up-to-date inventory of all authorized software.

Implement application whitelisting to control execution.

III. Continuous Vulnerability Assessment and Remediation:

Conduct regular vulnerability assessments.

Remediate or mitigate identified vulnerabilities in a timely manner.

IV. Controlled Use of Administrative Privileges:

Restrict and monitor the use of administrative privileges.

Use multi-factor authentication for administrative access.

V. Secure Configuration for Hardware and Software:

Establish and maintain secure configuration baselines.

Regularly assess and remediate deviations from secure configurations.

VI. Maintenance, Monitoring, and Analysis of Audit Logs:

Enable and configure system logging.

Regularly review, analyze, and retain audit logs.

VII. Email and Web Browser Protections:

Implement email filtering to block malicious attachments and links.

Configure web browsers to block access to malicious websites.

VIII. Malware Defenses:

Use anti-virus and anti-malware software.

Regularly update and scan systems for malware.

IX. Data Protection:

Classify and encrypt sensitive information.

Monitor and control the use of removable media.

2. CSC Implementation Group 2: Foundational Security Controls

I. **Secure Network Configuration:**

Configure network devices securely, including firewalls and routers.

Implement boundary defenses to detect and prevent unauthorized access.

II. **Data Protection:**

Implement data loss prevention (DLP) measures.

Use encryption for data in transit and at rest.

III. **Secure Configuration for Network Devices:**

Establish and maintain secure configuration baselines for network devices.

Monitor and manage network device configurations.

IV. **Boundary Defense:**

Implement network-based intrusion detection and prevention systems.

Deploy firewalls and gateways to protect network boundaries.

V. **Data Recovery Capability:**

Implement and test data backup and recovery processes.

Ensure the availability of critical data during and after an incident.

VI. **Secure Wireless Access:**

Implement secure configurations for wireless networks.

Use strong encryption and authentication for wireless access.

VII. **Account Monitoring and Control:**

Monitor user account activities.

Implement automated account management processes.

3. CSC Implementation Group 3: Organizational Advanced Security Controls

I. **Security Skills Assessment and Appropriate Training to Fill Gaps:**

Assess the security skills of the organization's workforce.

Provide ongoing training to address skill gaps.

II. **Application Software Security:**

Ensure secure coding practices in software development.

Regularly assess and remediate software vulnerabilities.

III. **Incident Response and Management:**

Develop and maintain an incident response plan.

Conduct regular incident response exercises and simulations.

IV. **Penetration Tests and Red Team Exercises:**

Conduct regular penetration tests and red team exercises.

Remediate vulnerabilities identified through testing.

V. Implement a Security Awareness and Training Program:

Promote security awareness among employees.

Provide training on cybersecurity best practices.

VI. Advanced Malware Defense:

Implement advanced malware detection and prevention measures.

Use threat intelligence to enhance malware defenses.