ncfe.

Level 3 Certificate in Cyber Security Practices
Unit 3: Cyber security testing, vulnerabilities and controls
Section 3: Controls in cyber security

Cyber security frameworks – CIS

The CIS framework is divided into three Implementation Groups (IGs). Each IG identifies a set of Safeguards that organisations need to implement. There are a total of 153 Safeguards, divided up into 18 groups of Controls.

The 18 Controls in the CIS framework are:

CIS Control 1: Inventory and Control of Enterprise Assets

Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorised and unmanaged assets to remove or remediate.

CIS Control 2: Inventory and Control of Software Assets

Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorised software is installed and can execute, and that unauthorised and unmanaged software is found and prevented from installation or execution.

CIS Control 3: Data Protection

Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.

Level 3 Certificate in Cyber Security Practices
Unit 3: Cyber security testing, vulnerabilities and controls
Section 3: Controls in cyber security

CIS Control 4: Secure Configuration of Enterprise Assets and Software

Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).

CIS Control 5: Account Management

Use processes and tools to assign and manage authorisation to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software.

CIS Control 6: Access Control Management

Use processes and tools to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for enterprise assets and software.

CIS Control 7: Continuous Vulnerability Management

Develop a plan to continuously assess and track vulnerabilities on all enterprise assets within the enterprise’s infrastructure, in order to remediate and minimise the window of opportunity for attackers. Monitor public and private industry sources for new threat and vulnerability information.

CIS Control 8: Audit Log Management

Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack.

CIS Control 9: Email Web Browser and Protections

Improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behaviour through direct engagement.

CIS Control 10: Malware Defences

Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets.

CIS Control 11: Data Recovery

Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state.

CIS Control 12: Network Infrastructure Management

Establish, implement, and actively manage (track, report, correct) network devices, in order to prevent attackers from exploiting vulnerable network services and access points.

Level 3 Certificate in Cyber Security Practices
Unit 3: Cyber security testing, vulnerabilities and controls
Section 3: Controls in cyber security

CIS Control 13: Network Monitoring and Defence

Operate processes and tooling to establish and maintain comprehensive network monitoring and defence against security threats across the enterprise's network infrastructure and user base.

CIS Control 14: Security Awareness and Skills Training

Establish and maintain a security awareness program to influence behavior among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise.

CIS Control 15: Service Provider Management

Develop a process to evaluate service providers who hold sensitive data, or are responsible for an enterprise's critical IT platforms or processes, to ensure these providers are protecting those platforms and data appropriately.

CIS Control 16: Application Software Security

Manage the security life cycle of in-house developed, hosted, or acquired software to prevent, detect, and remediate security weaknesses before they can impact the enterprise.

CIS Control 17: Incident Response Management

Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack.

CIS Control 18: Penetration Testing

Test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (people, processes, and technology), and simulating the objectives and actions of an attacker.