

- **Ibrahim Mahamad**
ID 2337318

Group number 9

Moodle name LCLM4002- Digital Skills (June 2024)

10 Steps To Cyber Security

Defining and communicating your Board's Information Risk Management Regime is central to your organisation's overall cyber strategy. CESG recommend you review this regime - together with the nine associated security areas described below - in order to protect your business against the majority of cyber threats.



• Ibrahim Mahamad
ID 2337318
Group number 9
Moodle name LCLM4002-
Digital Skills (June 2024)

Incident Management

- Establish an incident response and disaster recovery capability. Produce and test incident management plans. Provide specialist training to the incident management team. Report criminal incidents to law enforcement.

Network Security

- Protect your networks against external and internal attack. Manage the network perimeter. Filter out unauthorised access and malicious content. Monitor and test security controls

Malware Prevention

- Produce relevant policy and establish anti-malware defences that are applicable and relevant to all business areas. Scan for malware across the organisation.

Monitoring

- Establish a monitoring strategy and develop supporting policies. Continuously monitor all ICT systems and networks. Analyse logs for unusual activity that could indicate an attack:

Information Risk Management Regime



Maintain the Board's engagement with the cyber risk.



Produce supporting information risk management policies.



Establish an effective governance structure and determine your risk appetite.



User Education and Awareness

- Produce user security policies covering acceptable and secure use of the organisation's systems. Establish a staff training programme. Maintain user awareness of the cyber risks

Home and Mobile Working

- Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline build to all devices. Protect data both in transit and at rest.

Secure Configuration

- Apply security patches and ensure that the secure configuration of all ICT systems is maintained. Create a system inventory and define a baseline build for all ICT devices.

Removable Media Controls

- Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing into the corporate system

Managing User Privileges

- Establish account management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs