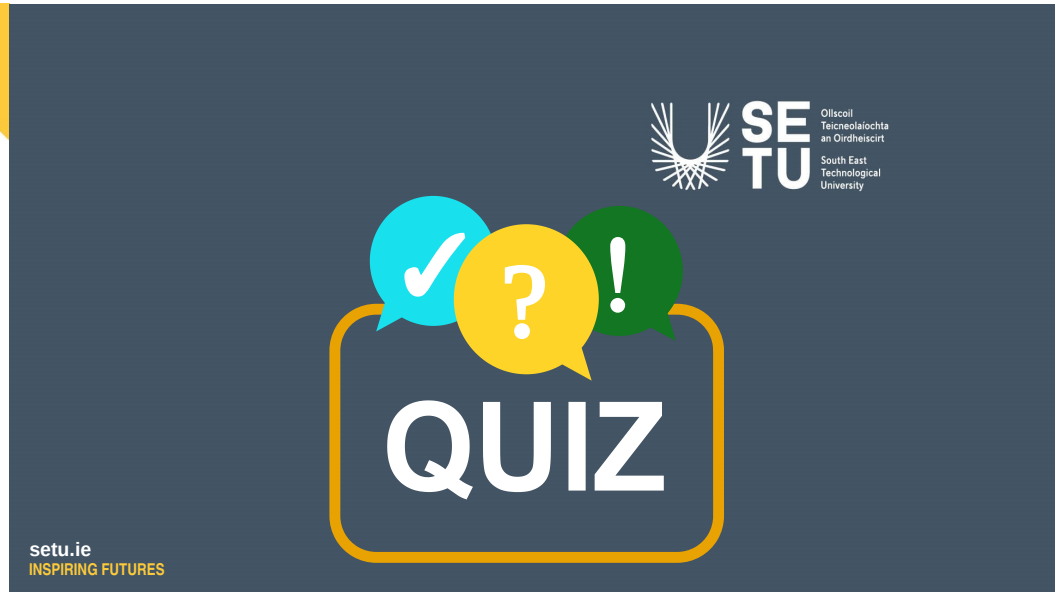
Licence

Learning Objectives

- By the end of this topic you will be able to:
  - Understand the CyFun 2025 Context and Purpose, including its foundation in the RMMs and its alignment with NIS2.
  - Differentiate the Proportional Assurance Levels (**BASIC**, **IMPORTANT**, and **ESSENTIAL**) and the tiered approach to implementing controls.
  - Analyse the Control Requirements per Core Function (GV, ID, PR, DE, RS, & RC) across all assurance levels to determine necessary security practices.
  - Apply the Self-Assessment Methodology, including calculating maturity scores, utilising the tool layout, and determining CAS.
  - Recognise key foundational policies necessary to establish and evidence security controls under the CyFun framework.



Progression of Asset Management

According to the CyFun 2025 Framework, how does Asset Management (ID.AM) evolve as an organisation moves from the BASIC to the IMPORTANT assurance level? (Select all that apply)

- ☐ **BASIC** level already requires maintaining inventories of hardware, software, and designated data types.
- ☐ Moving to **IMPORTANT** introduces the requirement to maintain representations of authorised network communication (network flows).
- ☐ **IMPORTANT** level adds the requirement to maintain inventories of services provided by suppliers.
- ☐ The **ESSENTIAL** level is the first time an organisation is required to prioritise assets based on classification and criticality.
- ☐ Moving to **IMPORTANT** requires identifying and recording vulnerabilities in assets for the first time.

Progression of Asset Management

According to the CyFun 2025 Framework, how does Asset Management (ID.AM) evolve as an organisation moves from the BASIC to the IMPORTANT assurance level? (Select all that apply)

- ☑ **BASIC** level already requires maintaining inventories of hardware, software, and designated data types.
- ☑ Moving to **IMPORTANT** introduces the requirement to maintain representations of authorised network communication (network flows).
- ☑ **IMPORTANT** level adds the requirement to maintain inventories of services provided by suppliers.
- ☒ The **ESSENTIAL** level is the first time an organisation is required to prioritise assets based on classification and criticality.
- ☒ Moving to **IMPORTANT** requires identifying and recording vulnerabilities in assets for the first time.

Data Security and Platform Security

In the PROTECT function, which of the following measures are specifically introduced at the ESSENTIAL level to defend against sophisticated attacks? (Select all that apply)

- ☐ Protecting the Confidentiality, Integrity, and Availability of data-at-rest.
- ☐ Protecting the Confidentiality, Integrity, and Availability of data-in-transit and data-in-use.
- ☐ Formalising the maintenance, replacement, and removal of both hardware and software commensurate with risk.
- ☐ Implementing configuration management practices and secure software development lifecycles.
- ☐ Establishing backups of data that are created, protected, maintained, and tested.

Data Security and Platform Security

In the PROTECT function, which of the following measures are specifically introduced at the ESSENTIAL level to defend against sophisticated attacks? (Select all that apply)

- ☒ Protecting the Confidentiality, Integrity, and Availability of data-at-rest.
- ☑ Protecting the Confidentiality, Integrity, and Availability of data-in-transit and data-in-use.
- ☑ Formalising the maintenance, replacement, and removal of both hardware and software commensurate with risk.
- ☒ Implementing configuration management practices and secure software development lifecycles.
- ☒ Establishing backups of data that are created, protected, maintained, and tested.

Incident Response and Recovery

Which of the following activities represent the transition from IMPORTANT to the ESSENTIAL level regarding how an organisation handles and recovers from an incident? (Select all that apply)

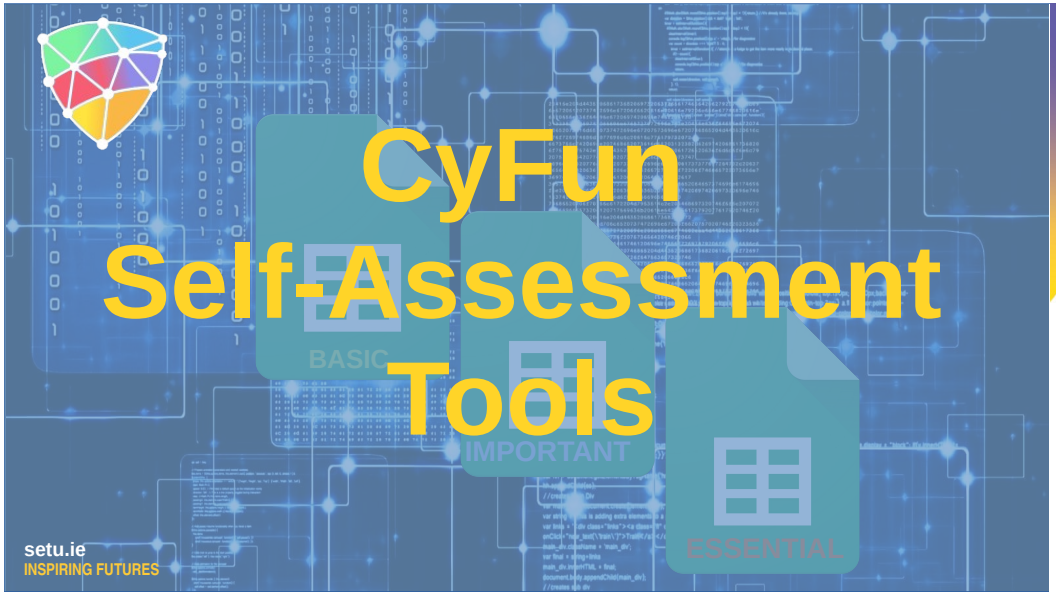
- ☐ Performing root cause analysis and preserving the integrity of investigation records.
- ☐ The first-time requirement to contain an incident.
- ☐ Collecting incident data and metadata while preserving its provenance (forensics).
- ☐ Selecting, scoping, and prioritising specific recovery actions for systematic restoration.
- ☐ Notifying internal and external stakeholders of the incident.

1

Incident Response and Recovery

Which of the following activities represent the transition from IMPORTANT to the ESSENTIAL level regarding how an organisation handles and recovers from an incident? (Select all that apply)

- ☑ Performing root cause analysis and preserving the integrity of investigation records.
- ☒ The first-time requirement to contain an incident.
- ☑ Collecting incident data and metadata while preserving its provenance (forensics).
- ☑ Selecting, scoping, and prioritising specific recovery actions for systematic restoration.
- ☒ Notifying internal and external stakeholders of the incident.



Utilising the CyFun Self-Assessment Tools

- Self-assessment tool spreadsheets to help organisations measure their compliance and maturity against the CyFun Framework and the associated Conformity Assessment Scheme (CAS).
- The tool is aligned with the requirements for Assurance Level **BASIC**, **IMPORTANT**, and **ESSENTIAL**.
- The tool must not be modified as part of any official verification or certification activity, as its alignment to the framework and CAS versions is fixed.
- The aligned versions are always identified within the tool itself.

BASIC IMPORTANT ESSENTIAL

CyFun Tool Layout

Introduction | Maturity Levels | References

- General Information, definitions and supporting documentation

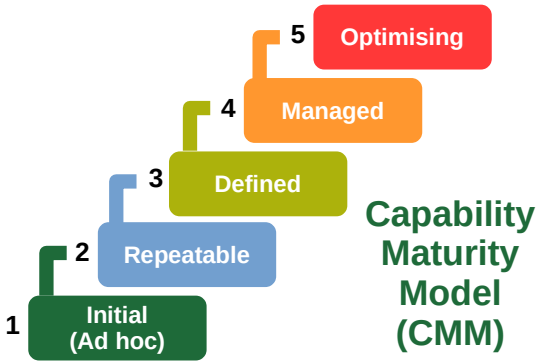
GOVERN | IDENTIFY | PROTECT | DETECT | RESPOND | RECOVER

- Specific controls that must be assessed for each assurance level
- Scores are input on these tabs

BASIC Summary

- Displays calculated Results

Capability Maturity Model (CMM)



Capability Maturity Model (CMM)

- The Tool Maturity Assessments separate the written intent (Policy/Documentation) from the applied practice (Implementation/Operation).

Self-Assessment Completion Date: 2025-10-01								
Subcategory	Requirement	Documentation Score	Implementation Score	Subcategory Documentation Maturity Score	Subcategory Implementation Maturity Score	Category Documentation Maturity Score	Category Implementation Maturity Score
GV.OC-03: Legal, regulatory, and contractual requirements regarding cybersecurity are understood and managed.	**GV.OC-03.1:** Legal and regulatory requirements regarding information and cybersecurity shall be identified and implemented.	1	1	1.00	1.00	1.00	1.00
GV.RM-03: Cybersecurity risk management activities and outcomes are included in enterprise risk management processes.	**GV.RM-03.1:** As part of the organisation-wide risk management strategy, a comprehensive strategy to manage information and cybersecurity risks shall be developed and updated when changes occur.	1	1	1.00	1.00	1.00	1.00

CMM CMM

Capability Maturity Model (CMM)

- The Tool Maturity Assessments separate the written intent (Policy/Documentation) from the applied practice (Implementation/Operation).

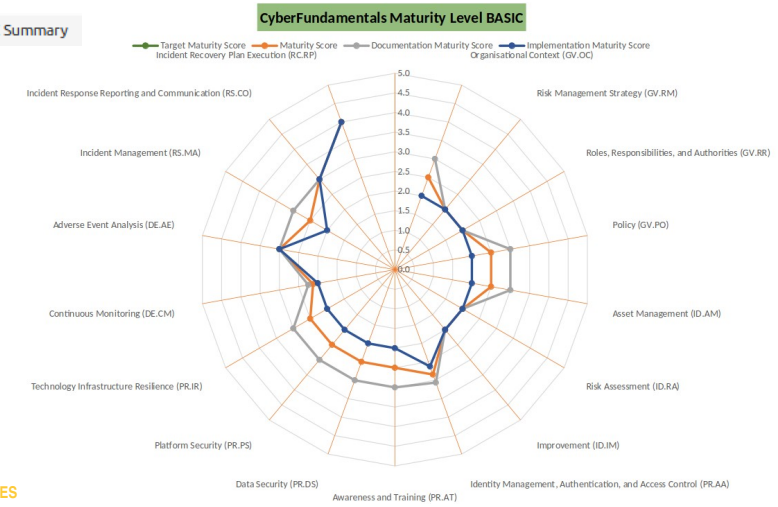
Policy Score

Self-Assessment Completion Date: 2025-10-01								
Subcategory	Requirement	Documentation Score	Implementation Score	Subcategory Documentation Maturity Score	Subcategory Implementation Maturity Score	Category Documentation Maturity Score	Category Implementation Maturity Score
GV.OC-03: Legal, regulatory, and contractual requirements regarding cybersecurity are understood and managed.	**GV.OC-03.1:** Legal and regulatory requirements regarding information and cybersecurity shall be identified and implemented.	1	1	1.00	1.00	1.00	1.00
GV.RM-03: Cybersecurity risk management activities and outcomes are included in enterprise risk management processes.	**GV.RM-03.1:** As part of the organisation-wide risk management strategy, a comprehensive strategy to manage information and cybersecurity risks shall be developed and updated when changes occur.	1	1	1.00	1.00	1.00	1.00

Implementation Score

Summary Report

BASIC Summary

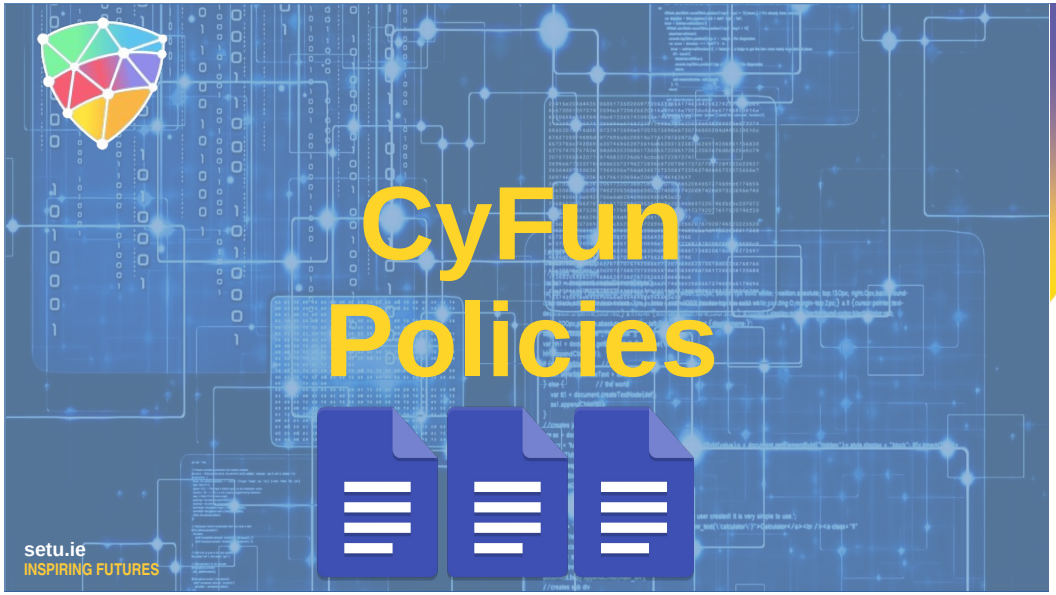


Determining Conformity with CAS

- **Red**: A calculated value that displays in red indicates the organisation is not conforming to the required maturity level.
- **Green**: A calculated value that displays in green indicates conformance to the required maturity level.

BASIC Summary

KEY MEASURES (KM)					
Requirement		Target Maturity Score	KM Maturity Score	Documentation Maturity Score	Implementation Maturity Score
ID.AM-08.2	Patches and security updates for operating systems and critical system components shall be installed.	2.50	4.00	4.00	4.00
PR.AA-01.1	Identities and credentials for authorised users, services, and hardware shall be managed.	2.50	2.50	2.00	3.00
PR.AA-03.2	Multi-Factor Authentication (MFA) shall be required to access the organisation's networks remotely.	2.50	4.00	4.00	4.00



CyFun Policies

Function	Policy Document
GOVERN	Cybersecurity Policy BASIC
	10 golden rules for cybersecurity
IDENTIFY	Asset Management Policies
	Vulnerability and Patch Management Policies
PROTECT	Network Security Policy (NSP)
	ACP BASIC
	Password Policy BASIC
DETECT	Implicitly covered within NSP & Vulnerability policies
RESPOND	Cyber IRP
RECOVER	Back-up and Recovery Policy (BRP)

Cybersecuritry Policy

- **The Governance Foundation document.**
- It defines the "why" and "what" of the security programme to protect assets, people, and commercial advantage.
- It **establishes mandatory baseline requirements** for all personnel, departments, and systems.
- **Guiding Principles**:
  - **Risk-Aware**: Know the environment and adapt to changes.
  - **Secure-by-Design**: Integrate security/privacy into all products and services.
  - **Proactive & Compliant**: Continuous patching and strict GDPR adherence.
- **Mandatory Controls**:
  - **Access**: MFA and "Principle of Minimum Access".
  - **Operations**: Asset inventories, malware protection, and vulnerability patching.
  - **Resilience**: Validated backups and a tested IRP.

10 Golden Rules: The human firewall

- Sets the essential, non-negotiable behaviours for all employees and subcontractors.
- **Authentication & Access**:
  - **MFA**: Mandatory use of MFA whenever available.
  - **Password Hygiene**: Minimum 14 characters; strictly separate professional and personal accounts.
- **Daily Operations**:
  - **Updates & Software**: Install security patches immediately; never download unauthorised software.
  - **Connectivity**: Use the corporate VPN exclusively; avoid all public Wi-Fi.
  - **Physical Security**: Lock screens when away; secure physical papers and avoid eavesdropping in public.
- **Awareness & Response**:
  - **Phishing Defence**: Check for urgency or unknown senders; never click links or open suspicious attachments.
  - **Incident Reporting**: Immediate reporting of phishing or security breaches to IT is mandatory.

Asset Management

- Establishes a structured, lifecycle approach to manage physical, virtual, and informational assets to ensure CIA.
- **Asset Classification**:
  - **Primary Assets**: Vital data and knowledge such as customer records, business processes, and source code.
  - **Secondary Assets**: The supporting infrastructure including hardware, software, networks, and personnel.
- **Inventory Management (ID)**:
  - **Mandatory Tracking**: Continuous tracking from Acquisition and Discovery through Use and Removal.
  - **Detailed Records**: Inventories must document Owners, CIA classifications, and asset dependencies.
- **Operational Security (PR)**:
  - **Layered Defence**: Combines physical storage controls, network segmentation, encryption, and regular backups.
  - **Maintenance**: Requires both proactive patching (Preventive) and documented incident resolution (Corrective).
- **Secure Disposal (RC)**:
  - **Data Erasure**: Obsolete assets must undergo secure data erasure or physical destruction before disposal.
  - **Incident Response**: Lost or stolen assets must be reported immediately and inventories updated to reflect the loss.

Vulnerability & Patch Management (VPMP)

- Actively eliminate security weaknesses, which account for over 90% of cybercrimes.
- **Vulnerability Identification (ID)**:
  - **Risk Assessment**: Mandatory annual review of threats, flaws, and business impact.
  - **Scanning**: Regular internal scans of critical assets and periodic external penetration tests.
  - **Ethical Hacking**: Higher assurance levels (**IMPORTANT**/**ESSENTIAL**) must establish a Coordinated Vulnerability Disclosure Policy (CVDP).
- Patch Management (PR):
  - **Standard Cycle**: All managed IT assets (servers, firewalls, etc.) must be updated at least every 2 months.
  - **Emergency Patches**: Critical security updates must be installed "as soon as possible" following an impact analysis.
  - **Legacy Systems**: Any non-patchable system must be isolated from the Internet and physically secured.
  - **Assurance Scaling**: Compliance requirements (such as scanning frequency) increase in rigor and frequency from **BASIC** to **ESSENTIAL**.

Network Security Policy (NSP)

- Acts as the "first line of defence" (PR) to prevent network mapping, traffic disruption, and unauthorised access to critical systems.
- **Network Segmentation**:
  - Mandates a segregated topology using VLANs and firewall rules.
  - **Strictly separates**: Internet-facing services vs. internal systems, end-users vs. servers, and production vs. dev/test environments.
- **Traffic Control & Firewalling**:
  - **Default Deny**: All traffic is blocked by default unless explicitly required for business.
  - **Prioritisation**: Ensures critical work traffic is protected from non-essential bandwidth use (e.g., streaming).
- **Access & Connectivity**:
  - **VPN + MFA**: Mandatory encryption and MFA for all remote work and M2M communication.
  - **Wi-Fi Standards**: Only WPA2-AES is permitted; guest devices must be restricted to isolated networks.
- **Management & Monitoring**:
  - **Documentation**: Must maintain a secure, up-to-date high-level network diagram.
  - **Logging**: Infrastructure must log traffic flows and administrator events for continuous monitoring.

Access Control Policy (ACP)

- Operates on Authentication (id verification) and Authorisation (granting rights) to define who accesses which assets.
- **Fundamental Rules**:
  - **Least Privilege**: Users are granted the absolute minimum access required for their job function.
  - **MFA**: Strongly preferred and enforced for critical systems and untrusted locations.
  - **Periodic Review**: Access rights are regularly audited and revoked if no longer necessary.
- **Account Hygiene**:
  - **Unique Identities**: User accounts must be personal; shared accounts are strictly discouraged and must be tracked if unavoidable.
  - **Privileged Access**: Admins must use standard accounts for daily tasks (e.g., email) and only use privileged accounts when necessary.
  - **External/Staff Control**: Third-party accounts must be clearly identifiable (prefixes) and set to auto-expire every 3 months unless renewed.
- **Procedural Guardrails**:
  - **Lockout Policy**: Accounts are suspended after a small number of failed attempts (e.g., 3 attempts in 5 minutes) and 90 days of inactivity.
  - **Formal Requests**: All access changes must be requested via standard forms (ACMF/ARF) and approved by HR or a supervisor.

Password Policy

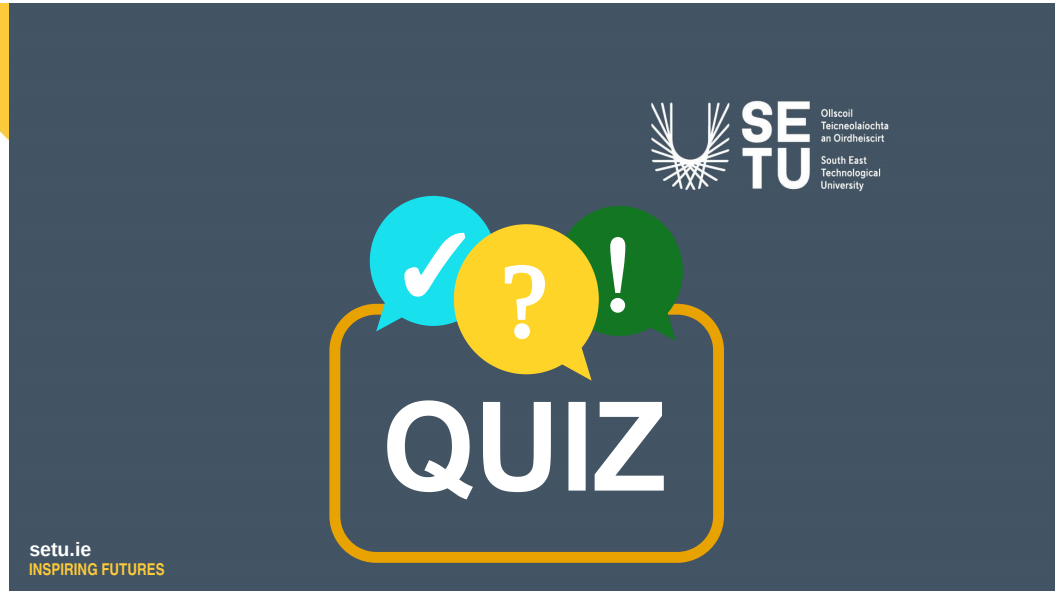
- Prioritises length and MFA over frequent mandatory changes to balance security with user-friendliness.
- **Enforced Strength Rules**:
  - **Length**: Specific minimums required (longer for Admins); systems must support passphrases up to 256 characters.
  - **Complexity**: Must include 3 of 4 categories (upper, lower, digits, symbols) and exclude personal info like usernames.
- **Change & Reuse Logic**:
  - **First-Login Change**: Mandatory for all default or IT-issued passwords.
  - **History**: Systems must block the reuse of at least the last several passwords to prevent "cycling".
- **Attack Prevention**:
  - Mandates mechanisms like Account Lockout, IP Blacklisting, or Login Delays to stop brute-force/automated guessing.
- **User Responsibilities**:
- **Zero Sharing**: Never communicate passwords via email or phone.
  - **Storage**: Use only authorised Password Managers; "Remember Password" browser features are prohibited.
  - **Compensating Controls**: Shorter codes (e.g., 4-digit PINs) are only allowed if combined with physical hardware like smart cards.

Incident Response Plan (IRP)

- Acts as the organisation's firefighting manual, providing structured guidance to manage digital emergencies from detection to recovery.
- **Incident Lifecycle**:
  - **Detection & Analysis**: Classifying severity (Critical to Low) to prioritise resources.
  - **Containment & Evidence**: Stopping the spread (e.g., system isolation) while preserving the forensic chain of custody.
  - **Recovery**: Restoring services based on predefined Recovery Time (RTO) and Point (RPO) targets.
  - **Lessons Learned**: Mandatory post-incident review to prevent recurrence through process changes or training.
- **Roles & Authority**:
  - **CSIRT (Operational)**: Technical experts (engineers/admins) managing the hands-on response.
  - **Management Team (Strategic)**: C-suite oversight, emergency funding, and high-level decisions.
- **Communication & Reporting**:
  - **Strict Control**: Internal/external messaging managed on a need-to-know basis.
  - **NIS2 Compliance**: Significant incidents must be reported to the NCSC within 24 hours, with a final report due after one month.

Back-up & Recovery Policy (BRP)

- Ensures data availability and integrity through mandatory procedures for protection against disasters, ransomware, or human error.
- **Performance Metrics**:
  - **RPO**: Sets the maximum tolerable "data loss window".
  - **RTO**: Sets the maximum time allowed to restore services.
  - **Validation**: Mandatory recovery tests for all critical systems must be conducted at least annually.
- **Security Controls**:
  - **Encryption**: Data must be encrypted during transfer and at rest; keys must not be stored exclusively on-site.
  - **Access**: Backups must be protected by the same security levels (MFA/least privilege) as the original production data.
- **Resilience Strategies**:
  - **The 3-2-1 Rule**: Maintain 3 copies of data, on 2 different media types, with 1 copy stored off-site.
  - **GFS Rotation**: Implements a "Grandfather-Father-Son" schedule (Monthly/Weekly/Daily) to provide multiple historical restore points.
  - **Location Strategy**: Requires physical separation between original data and backups to prevent total loss in localised disasters (e.g., fire/flood).



The "Human Firewall" & User Access

Which of the following actions are MANDATORY for users under the 10 Golden Rules and Access Control Policy (ACP)? (Select all that apply)

- ☐ Using MFA for professional accounts whenever possible.
- ☐ Setting a password of at least 14 characters for professional accounts.
- ☐ Using the "Remember Password" feature in web browsers to prevent forgetting complex credentials.
- ☐ Separating professional and personal account passwords.
- ☐ Locking the computer screen every time the user steps away from their desk.

1

The "Human Firewall" & User Access

Which of the following actions are MANDATORY for users under the 10 Golden Rules and Access Control Policy (ACP)? (Select all that apply)

- ☑ Using MFA for professional accounts whenever possible.
- ☑ Setting a password of at least 14 characters for professional accounts.
- ☒ Using the "Remember Password" feature in web browsers to prevent forgetting complex credentials.
- ☑ Separating professional and personal account passwords.
- ☑ Locking the computer screen every time the user steps away from their desk.

Network Defence & Segmentation

According to the Network Security Policy, which strategies must be implemented to protect the organisation's digital borders? (Select all that apply)

- ☐ Allowing unmanaged guest devices to connect to the main corporate network for convenience.
- ☐ Implementing a "Default Deny" rule for all traffic between segregated VLANs.
- ☐ Separating end-user devices from servers using network segmentation.
- ☐ Using WPA2-AES encryption for all wireless network communications.
- ☐ Disabling network logging on internal switches to maximise network performance and reduce storage costs.

Network Defence & Segmentation

According to the Network Security Policy, which strategies must be implemented to protect the organisation's digital borders? (Select all that apply)

- ☒ Allowing unmanaged guest devices to connect to the main corporate network for convenience.
- ☑ Implementing a "Default Deny" rule for all traffic between segregated VLANs.
- ☑ Separating end-user devices from servers using network segmentation.
- ☑ Using WPA2-AES encryption for all wireless network communications.
- ☒ Disabling network logging on internal switches to maximise network performance and reduce storage costs.

Data Resilience & Disaster Recovery

Per the Back-up and Recovery Policy, which requirements ensure that data can be successfully restored after a disaster? (Select all that apply)

- ☐ Performing recovery tests for all critical systems at least once every three years.
- ☐ Storing at least one copy of backup data in a different physical location.
- ☐ Keeping backup encryption keys stored on the same server as the backup for easy access.
- ☐ Ensuring that three copies of data are maintained on at least two different types of storage media.
- ☐ Using unencrypted SMS to send full login credentials for backup systems to the IT team.

Data Resilience & Disaster Recovery

Per the Back-up and Recovery Policy, which requirements ensure that data can be successfully restored after a disaster? (Select all that apply)

- ☒ Performing recovery tests for all critical systems at least once every three years.
- ☑ Storing at least one copy of backup data in a different physical location.
- ☒ Keeping backup encryption keys stored on the same server as the backup for easy access.
- ☑ Ensuring that three copies of data are maintained on at least two different types of storage media.
- ☒ Using unencrypted SMS to send full login credentials for backup systems to the IT team.

Verification & Certification

Feature	Verification (BASIC & IMPORTANT)	Certification (ESSENTIAL)
Assurance Level	BASIC or IMPORTANT	ESSENTIAL
Process Type	Validation/Verification of a self-declaration.	Certification of an ISMS.
Objective	To receive an official label for the organisation's cybersecurity maturity level.	To obtain a higher level of assurance and a presumption of conformity with mandatory regulations such as NIS2 for high-risk entities.
Basis	Focuses on checking the effective implementation of the specific CyFun controls.	Often aligns with the more rigorous requirements of an ISMS standard such as ISO/IEC 27001, in addition to the CyFun requirements.

Paths to Compliance

- **Preliminary Phase** (Common to All):
  - **Selection**: Use the CyFun tool to determine the target level (**BASIC**, **IMPORTANT**, and **ESSENTIAL**).
  - Internal audit of security maturity against specific framework controls.
  - Implementing corrective measures to close identified security gaps.
- **Path A: Verification** (**BASIC**, **IMPORTANT**):
  - An authorised Conformity Assessment Body (CAB) reviews evidence and conducts on-site checks to verify the self-assessment.
  - Awarded an official Verification Report and the CyFun label.
- **Path B: Certification** (**ESSENTIAL**):
  - The most rigorous path; involves a two-stage audit including technical testing (Pen-testing, code reviews) and in-depth process analysis.
  - Awarded a formal Certificate of Conformity, the highest level of independent assurance.
  - Provides independent evidence of compliance with NIS2 Directive "duty of care" obligations.

Learning Objectives

- Understand the CyFun 2025 Context and Purpose, including its foundation in the Risk Management Measures and its alignment with NIS 2 ✓
- Differentiate the Proportional Assurance Levels (**BASIC**, **IMPORTANT**, and **ESSENTIAL**) and the tiered approach to implementing controls ✓
- Analyse the Control Requirements per Core Function (GV, ID, PR, DE, RS, & RC) across all assurance levels to determine necessary security practices ✓
- Apply the Self-Assessment Methodology, including calculating maturity scores, utilising the tool layout, and determining CAS ✓
- Recognise key foundational policies necessary to establish and evidence security controls under the CyFun framework ✓

SETU Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

EUR ING Dr Diarmuid Ó Briain
Innealtóir Cairte agus Léachtóir Sinsearach
D +353 59 917 5000 | E diarmuid.obriain@setu.ie | **setu.ie**
Campas Bhóthar Chill Chainnigh, Ceatharlach, R93 V960, Éire

SETU Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

Thank you

engcore
advancing technology