

Title: Cyber Fundamentals Framework
Long Title: Cyber Fundamentals Framework
Credits: 10
NFQ Level: Expert

Module Description:

In this module, learners will critically evaluate the effective application of the Cyber Fundamentals Framework. Cyber Fundamentals (CyFun) provides a structured, risk-based approach enabling organisations to organise and evidence their cybersecurity measures and is recommended by the National Cyber Security Centre. Learners will examine key technical, organisational and human security controls, integrating governance, risk and compliance considerations to optimise enterprise cybersecurity posture. Through applied analysis of real-world scenarios, learners will integrate insights from a range of enterprise cyber risk environments to critically appraise and guide proportionate cybersecurity strategies aligned with the CyFun Framework.

Learning Outcomes

On successful completion of this module the learner will be able to:

- LO1** Critically examine the Cyber Fundamentals (CyFun) Framework and its practical application to enterprise cybersecurity risk management.
- LO2** Evaluate organisational cyber risk environments and determine appropriate mitigation levels across technical, organisational, and human domains.
- LO3** Appraise enterprise cybersecurity governance alignment with the CyFun Framework, evidencing clear accountability and leadership ownership.
- LO4** Design and integrate CyFun cybersecurity controls with relevant industry standards, considering the operational and financial impacts of non-compliance.
- LO5** Critically analyse how the CyFun Framework enables the coordinated management of cybersecurity governance, risk, and compliance in complex organisational environments.
- LO6** Interpret CyFun Framework analyses into effective recommendations for strategic cyber risk management at an executive level.

Indicative Content

CyFun Framework

Purpose, scope and structure of the Cyber Fundamentals Framework (co-owned Belgian NCSC & Irish NCSC cyber risk management framework). Core governance, risk and control domains within CyFun. Application of CyFun to enterprise cybersecurity risk management processes, including Baseline Assessments, Key Measures, CyFun Toolbox & Self Assessment Tool and Maturity Scores. CyFun Proportionality (Small, Basic, Important, Essential) and related key measures.

Cybersecurity Risk Management

Enterprise cyber risk environment and threat analysis. Critical assets and business dependencies. Vulnerability assessments across technical, organisational and human domains. Proportionate mitigation aligned to risk tolerance and CyFun controls. Third-party risk exposure. Continuous monitoring. Cybersecurity posture.

Cybersecurity Governance

Enterprise cybersecurity governance evaluations. Cybersecurity governance legislative and regulatory requirements and best practices. CyFun Framework's 'Govern' function implementation guidance.

Industry Standards, Compliance & Violations

Leading cybersecurity industry standards and frameworks, including NIST Cybersecurity Framework v2.0, CIS Controls and ISO27001. Regulatory compliance requirements, including NIS2 and other relevant EU cybersecurity legislation. The operational & non-financial implications of non-compliance.

Cybersecurity Governance, Risk & Compliance

Integrated Governance, Risk and Compliance (GRC) practices and tools. GRC Reporting and dashboards. Assurance & Testing Strategies. Continuous improvement strategies.

Cybersecurity Communication Skills

Executive outlook. Structured executive communications options. Actionable recommendations based on industry- best practice, including alignment with the CyFun Framework and relevant cybersecurity legislation and regulations.

Course Work

Assessment Type	Assessment Description	Outcome Addressed	% of Total	Assessment Date
Project	The Learner will produce a written report to a professional standard appraising the effectiveness of the CyFun risk management framework and judging its effectiveness in the mitigation of differing cybersecurity risks scenarios. Findings should be fully documented and/or presented.	1,2	40	Week 6
Project	Findings should be fully documented and/or presented. Learners will conduct a cybersecurity risk assessment of a Use-Case/Real Organisation using the CyFun Framework's Self-Assessment Tool. Learners will develop a Cyber Risk Mitigation Plan to close identified gaps. Learners must effectively defend their research, formulating an executive presentation capable of clearly supporting a summary of their findings to their peers and experts in the field. Findings should be fully documented and/or presented.	3,4,5,6	60	Sem End

No End of Module
Formal Exam

Assessment Breakdown	%
Coursework	100

Re-Assessment Requirement

Coursework Only

This module is reassessed solely on the basis of re-submitted coursework. There is no repeat written examination.

Workload – Full Time

Workload Type	Workload Description	Hours	Frequency	Average Weekly Learner Workload
Lecture	Lectures covering the concepts underpinning the learning outcomes.	2	Every Week	2.00
Lab	Lab to support learning outcomes.	2	Every Week	2.00
Independent & Directed Learning (Non-contact)	Independent learning.	3	Every Week	3.00
Total Hours				7.00
Total Weekly Learner Workload				7.00
Total Weekly Contact Hours				4.00

Workload – Part Time

Workload Type	Workload Description	Hours	Frequency	Average Weekly Learner Workload
Lecture	Lectures covering the concepts underpinning the learning outcomes.	2	Every Week	2.00
Lab	Lab to support learning outcomes.	2	Every Week	2.00
Independent & Directed Learning (Non-contact)	Independent Study.	3	Every Week	3.00
Total Hours				7.00
Total Weekly Learner Workload				7.00
Total Weekly Contact Hours				4.00

Recommended Resources

Cynthia Brumfield. (2021), Cybersecurity Risk Management, John Wiley & Sons, p.180, [ISBN: 9781119816287].

Jason Edwards, Griffin Weaver. (2024), The Cybersecurity Guide to Governance, Risk, and Compliance, John Wiley & Sons, p.677, [ISBN: 9781394250196].

Juan Luis Salas-Riega, Yasmina Riega-Virú, Mario Ninaquispe-Soto, José Miguel Salas-Riega. (2025), Cybersecurity and the NIST Framework: A Systematic Review of its Implementation and Effectiveness Against Cyber Threats, International Journal of Advanced Computer Science & Applications, Volume 16, Issue 6, <https://doi.org/10.14569/IJACSA.2025.016 0672>

National Cyber Security Centre Ireland. (2025), Cyber Fundamentals (CyFun) Frequently Asked Questions, 23 June 2025, <https://www.ncsc.gov.ie/CyFun/CyFunFAQ/>

Website, CyFun. (2026), CyberFundamentals Framework, <https://cyfun.eu/en>

Website, National Institute of Standards & Technology. (2024), NIST Cybersecurity Framework v2.0, <https://www.nist.gov/cyberframework>

Website, International Organization for Standardization (ISO). (2022), ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements, ISO, <https://www.iso.org/standard/27001>

Website, International Organization for Standardization (ISO). (2022), ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls, <https://www.iso.org/standard/75652.html>

Website, International Organization for Standardization (ISO). (2018), ISO 31000:2018 Risk management — Guidelines, <https://www.iso.org/standard/65694.html>