

GOVERNMENT
OF MALTA

Government response to the Consultation on **the transposition of Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the European Union (NIS 2 Directive)**

Ministry for Home Affairs, Security and Employment (MHSE) / Ministeru għall-Intern, is-Sigurtà u x-Xogħol

This publication (excluding Logos) may be re-used free of charge in any format or medium provided that it is re-used accurately and not used in a misleading context. This material must be acknowledged as Government of Malta and the title of the publication specified.

Any queries regarding this publication should be sent at: onlineconsultations@gov.mt.

Published by Ministry for Home Affairs, Security and Employment (MHSE) / Ministeru għall-Intern, is-Sigurtà u x-Xogħol

Contents

CONTENTS

Contents 4
Executive Summary 5
Introduction and overview 5
Responses to the consultation and process used to seek stakeholder views 5
Summary of responses and decisions 6
Implementation 21
Contact Details 22

Executive Summary

Introduction and overview

1. A brief introduction about the subject.

The Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148, also known as the **NIS2 Directive**, entered into force on 16 January 2023. The obligations and measures outlined in the Directive began to apply from 18 October 2024.

The NIS2 Directive establishes a common regulatory framework for cybersecurity across the European Union. It requires Member States to strengthen cybersecurity capabilities and introduce risk-management measures and reporting in critical sectors. The NIS2 Directive also sets rules on cooperation, information sharing, supervision, and enforcement.

2. The public consultation date.

On September 6, 2024, the Government published a public consultation paper seeking public input on the proposed draft order to effectively implement the NIS2 Directive into Maltese law.

3. This consultation sought views on:

On the transposition of the NIS2 Directive into Maltese law.

Responses to the consultation and process used to seek stakeholder views

This document is the Government Response to this consultation and sets out the Government's decisions on these matters.

4. The closing date of the public consultation. Which methods were used to receive the feedback. The total amount of responses. From whom you received the feedback.

The consultation concluded on 7 October 2024. Both the consultation document and the reply form were available online, and responses were accepted electronically. A total of 22 responses were received, originating from various sectors including financial services, telecommunications, information technology, aviation, pharmaceuticals, and food. Additionally, responses came from local authorities, voluntary organizations, and private individuals.

5. Include (if any) meetings with stakeholders and list who the stakeholders were.

No meetings were held with stakeholders during the consultation period. Following the consultation period, meetings were held with the Malta Communications Authority, the Malta Financial Services Authority and the Ministry for the National Heritage, the Arts and Local Government.

Summary of responses and decisions

The following is a summary of the consultation responses received. We would like to thank all those who took the time to respond to the consultation and participate in stakeholder meetings around the consultation exercise.

6. Statistics.

- Total feedback received: 22
- Total feedback received by individuals: 2
- Total feedback received by organisations: 20
- Total feedback received through email: 9
- Total feedback received through online form: 13
- Total feedback received by post: 0

7. Summary of feedback received.

PART I – PRELIMINARY

Article 3 – Definitions

1. **Auditor and Audit Firm**: Questions on the definitions and the roles, recommended replacement with 'security expert', 'technical expert', or 'service provider'. Recommended removing the definition of 'audit firm'.

2. **Other Definitions**: Recommended inserting the following definitions or adding more information to existing: 'entity providing domain name registration services', 'reseller', 'cloud computing services', 'computing resources', 'broad remote access', 'scalable' and 'traffic light protocol'.

3. **Guidance Needed**: Sought guidance on terms like 'security scanning', 'pro-active scanning' and 'non-intrusive scanning'.

4. **Public Administration Entities**: Recommended full transposition with clarity on 'local level' and 'regional level' and inclusion of all public entities.

5. **Legitimate Access Seeker**: Recommended adding this term to include the investigation of illegalities, aligning with the European Commission's anti-counterfeiting recommendations, and ensuring free, immediate access to WHOIS data.

6. **Domain Name Registration Services**: Recommended clarification to include providers and resellers of privacy and proxy services.

7. **Internal CSIRT**: Further clarification was sought as it was being inconsistently used in other sections of the transposition.

Article 4 – Applicability

8. **Entity Activities**: Clarification needed on whether only key business activities or all activities, including supporting ones, should be considered.

9. **Guidelines for Impact and Risk**: Required for determining significant impact and systemic risk.

10. **Entity List**: Clarification on whether a list of entities will be published.

11. **Exemptions and Precedence**: Clarification on exemptions from other sector-specific legislation and whether such legislation takes precedence over NIS2.

12. **Impact on Smaller Businesses**: Current criteria may disadvantage smaller businesses; impact assessments should consider business size, economic impact, and industry role.

PART II – CRITICAL INFRASTRUCTURE ADVISORY BOARD, CRITICAL INFRASTRUCUTRE PROTECTION DEPARTMENT AND CSIRTMalta

Article 6 - Critical Infrastructure Protection Advisory Board

13. **Secretary's Voting Rights**: To clearly indicate that the secretary does not have voting rights.

Article 7 – National Cybersecurity Strategy

14. **Notification Structure**: Clarification on which Maltese structure will notify the Commission on the national cybersecurity strategy.

Article 8 – Critical Infrastructure Protection Department

15. **Self-Registration Mechanism**: Clarification needed on the procedure.

16. **Competent Authority Designation**: Recommended designating the Malta Communications Authority (MCA) as the competent authority for specific sectors.

17. **Cooperation Group Participation**: Request to amend participation by other competent authorities.

18. **Entity Specification and Overlaps**: The Department should specify which entities are subject to the order and address overlaps with other regulations.

19. **Regulatory Responsibilities**: Clarification on cooperation between CIPD and MCA. Recommended designating MCA as the sole competent authority for all digital services.

20. **NIS2 and DORA overlap**: Highlighted duplication and conflicts in compliance requirements. Proposed joint certification or waiving certain audit obligations under Directive (EU) 2022/2554 (DORA) if NIS2 requirements are met.

21. **ECNS Providers**: Clarification on whether such providers will receive direct input from MCA under this order.

22. **Designation criteria**: Clarification needed on criteria to designate essential and important entities.

23. **Communication**: Clarification on whether CIPD will proactively contact entities on their obligations.

24. **Risk assessments and plans**: Clarification on how CIPD will ensure these are in place and on requirements.

25. **Investigations and simulations**: More information needed on how CIPD will conduct investigations and simulations.

26. **Monitoring obligations**: Clarification on entities' obligations regarding CIPD monitoring.

27. **Compliance timelines**: Further information on specific deadlines for compliance.

Article 9 - CSIRTMalta and Computer Security Incident Response Teams (CSIRTs)

28. **National CSIRT responsibility**: Obligations should be transposed faithfully in the order.

29. **Distinction of national CSIRT**: Clarification on whether it will be distinct from the existing CSIRT.

30. **Incident management process**: Clarification on when and how this process will be communicated to entities.

Article 10 - Requirements of Computer Security Incident Response Teams (CSIRTs)

31. **Scope of requirements**: Clarification on whether these apply to all CSIRTs.

32. **Outsourcing**: Further clarification on whether outsourcing of CSIRT services is allowed.

Article 11 – Tasks of CSIRTMalta

33. **Scope of operation**: Recommended that CSIRTMalta should only operate under the obligations set out by NIS2.

34. **Proactive scanning coordination**: Adequate coordination needed, agreed upon with the entity.

35. **Applicability to entity CSIRTs**: Clarification on whether all tasks apply to entity CSIRTs.

Article 12 – Resources

36. **Resource needs**: Stressed the need for adequate human, financial, and technical resources for essential entities and competent authorities.

Article 14 – Coordinated Vulnerability Disclosure

37. **Reporting deadline**: No statutory deadline for security researchers, leading to potential abuse and inconsistency.

38. **ICT definitions**: Discrepancy between the order and Chapter 9 of the Laws of Malta - the Criminal Code.

39. **Researcher Authorisation**: Recommended inserting a provision equating CVDP policy compliance to authorisation.

40. **Entity lacking CVDP**: Order does not specify actions, creating potential gaps for when an entity does not have a CVDP set up.

41. **Baseline CVDP**: Suggested establishment of minimum requirements for a CVDP.

42. **CVDP Definition**: Lacking clear definition, discouraging disclosure.

43. **Enforcement**: Suggested that order would not sufficiently improve the current landscape unless enforcement is increased.

44. **Guidelines and mandatory CVDPs**: Crucial for a secure and standardized approach.

45. **CSIRTMalta capabilities**: Necessary to confirm reported vulnerabilities.

Article 15 – Auditors

46. **Approval process**: Clarification needed on how auditors would require approval.

47. **Mandatory or alternatives**: Whether approval is mandatory, and if not, what alternatives exist.

48. **Appointment and qualifications**: Clear guidelines needed to ensure effective compliance.

49. **Procedure availability**: When the procedure will become available.

50. **Accreditation requirements**: Suggested replacing current wording with one highlighting required knowledge and expertise approved by the Department.

51. **Cybersecurity risk management**: Methodology for confirming implementation of cybersecurity risk management measures is unclear.

PART III- NATIONAL CYBERSECURITY STRATEGY

Article 16 – National Cybersecurity Strategy

52. **Strategy revision**: Whether a revision will be published before the implementation of the transposed law.

53. **Responsibility and establishment**: Who will be responsible for the strategy and when will it be established.

Article 17 - National Cyber Crisis Management Framework

54. **Crisis management authorities**: Required to be identified and designated in law.

PART IV – CYBERSECURITY RISK-MANAGEMENT MEASURES AND REPORTING OBLIGATIONS

Article 19 – Governance

55. **Management bodies**: Clarification on which individuals are considered management bodies; this term should be defined under Article 3.

56. **Personal liability**: Concerns that personal liability may discourage proactive decision-making and innovation.

57. **Cybersecurity insurance**: Government should facilitate cybersecurity insurance for executives.

58. **Role of management bodies**: Incorrect transposition regarding their role in approving cybersecurity measures; 'to approve' implies higher involvement and accountability.

59. **Public officials**: Clarification on exemption for public officials serving in management bodies.

Article 20 – Cybersecurity risk-management measures

60. **ISO-27001**: Whether it would be considered adequate for ensuring network and information systems security, aligning reporting requirements with ISO standards to avoid duplication.

61. **Operator security plans**: Clarification needed.

62. **Internal vs. autonomous CSIRT**: Clarification on the distinction.

Article 21 – Reporting Obligations

63. **Incident notification templates**: Requests for templates to be provided.

64. **Significant incidents**: Should be defined in Article 3.

65. **Centralised approach**: Recommended that the designated competent authority should be the primary receiver of incident notifications, communicated to CSIRTMalta, to streamline the process and reduce bureaucracy.

66. **Incident management**: Recommended that this should be assigned to the designated competent authority, with clear guidelines on communication protocols.

67. **Ambiguity**: Clarification needed on who should receive incident reports.

Article 22 - Use of European Cybersecurity Certification Schemes

68. **Voluntary use**: Should not be mandatory for entities to use specific ICT services, products, or services unless it is a Commission delegated act.

PART V – JURISDICTION AND REGISTRATION

Article 24 – Jurisdiction and Territoriality

69. **Jurisdiction clarification**: Whether entities in or with primary establishments in other Member States could fall under Maltese jurisdiction.

Article 25 – Registry of Entities

70. **National requirements**: Concern that additional national requirements not found in NIS2 Directive add unnecessary compliance burdens.

Article 26 – Database of Domain Name Registration Data

71. **Transparency requirements**: Data of the beneficial user of the domain name should be provided, not just the privacy or proxy registration service provider.

72. **DNS Abuse**: Article 26 should allow legitimate access seekers to obtain a list of all domain names registered with the same data (reverse WHOIS lookup) when illegal activities are suspected.

73. **WHOIS data**: WHOIS data of legal entities should be free of charge to legitimate access seekers and publicly available, including name, verified telephone number, and contact email address.

74. **Verification procedures**: Robust and continually updated procedures to verify WHOIS data should be mandatory, with consequences for incorrect or incomplete data.

75. **WHOIS system improvements**: Suggested improvements to streamline the process and enhance cybersecurity efforts for .com and .net domains.

PART VI – INFORMATION SHARING

No comments.

PARTI VII – SUPERVISION AND ENFORCEMENT

Article 30 - Supervisory and Enforcement Measures in Relation to Essential Entities

76. **Faithful transposition**: Equivalent article in NIS2 should be transposed faithfully.

77. **Enforcement tools**: Clarification needed on who will conduct actions, associated costs, timelines, and applicability to all entities or specific incidents.

Article 31 - Supervisory and Enforcement Measures in Relation to Important Entities

78. **Faithful transposition**: Equivalent article in NIS2 should be transposed faithfully.

Article 32 – Proceedings for the Imposition of Enforcement Measures

79. **Courts or Tribunals**: Recommended to retain 'courts or tribunals' in sub-article 32(10).

PART VIII – ADMINISTRATIVE REVIEW TRIBUNAL

Article 41 – Administrative Review Tribunal

80. **Imposition of fines**: Suggested that the Tribunal, not the Civil Court, should impose administrative fines.

Miscellaneous Feedback

81. **Timeline concerns**: The timeline from publication to enforcement was thought to be unrealistic; recommended extending the period and providing a six-month grace period post-enactment.

82. **Phased implementation**: Suggested establishing different dates for various provisions to allow entities to comply.

83. **Guidance documents**: Need for guidance documents from the Department and designated competent authorities before key aspects of the transposition come into effect.

84. **Revised version**: Inquiry on whether a revised version will be available to the public.

85. **SME compliance challenges**: NIS2 poses challenges for SMEs due to limited resources and expertise; support mechanisms like training programs and tailored guidelines are essential.

86. **Additional costs**: Businesses will face additional costs for staffing, services, software, and hardware; smaller businesses may incur higher costs.

87. **Impact on competition**: Increased costs could limit innovation; monitoring implementation across Member States is important to avoid disadvantaging Maltese businesses.

8. Your assessment and the Government's decision (list the Government's decisions).

Following an assessment taken on the feedback provided from the respondents, the Government has decided to take the following decisions as summarised below according to the structure of the draft legal text:

PART I – PRELIMINARY

Article 2 – Repeal and saving.

1. 'Saving' is to be replaced with the word 'replace'.

2. Sub-article 2(1) is to be deleted.

Article 3 – Definitions

3. The definition ‘auditor’ shall be amended as follows:

   “qualified auditor” means a natural person who satisfies the requirements under article 15;

4. The definition ‘audit firm’ shall be deleted.

5. The definition ‘autonomous CSIRT shall be amended as follows:

   “autonomous CSIRT” means an outsourced CSIRT which provides a monitoring function of CSIRT services to its own business or essential or important entities;

6. The definition ‘cloud computing service’ shall be amended as follows:

   “cloud computing service” means a digital service that enables on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources, including where such resources are distributed across several locations. Computing resources shall include resources such as networks, servers or other infrastructure, operating systems, software, storage, applications and services. The service models of cloud computing include, inter alia, Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS) and Network as a Service (NaaS). The deployment models of cloud computing should include private, community, public and hybrid cloud. The cloud computing service and deployment models have the same meaning as the terms of service and deployment models defined under ISO/IEC 17788:2014 standard. The capability of the cloud computing user to unilaterally self-provision computing capabilities, such as server time or network storage, without any human interaction by the cloud computing service provider could be described as on-demand administration. The term ‘broad remote access’ is used to describe that the cloud capabilities are provided over the network and accessed through mechanisms promoting use of heterogeneous thin or thick client platforms, including mobile phones, tablets, laptops and workstations. The term ‘scalable’ refers to computing resources that are flexibly allocated by the cloud service provider, irrespective of the geographical location of the resources, in order to handle fluctuations in demand. The term ‘elastic pool’ is used to describe computing resources that are provided and released according to demand in order to rapidly increase and decrease resources available depending on workload. The term ‘shareable’ is used to describe computing resources that are provided to multiple users who share a common access to the service, but where the processing is carried out separately for each user, although the service is provided from the same electronic equipment. The term ‘distributed’ is used to describe computing resources that are located on different networked computers or devices and which communicate and coordinate among themselves by message passing;”

7. The definition ‘connected undertaking’ shall be deleted.

8. A new definition ‘coordinated vulnerability disclosure’ shall be created as follows:

9. “coordinated vulnerability disclosure” means a structured process through which vulnerabilities are reported to the manufacturer or provider of the potentially vulnerable ICT products or ICT services in a manner to allow it to diagnose and remedy the vulnerability before detailed vulnerability information is disclosed to third parties or to the public. Coordinated vulnerability disclosure also includes coordination between the reporting person and the manufacturer or provider of the potentially vulnerable ICT products or ICT services as regards the timing of remediation and publication of vulnerabilities;

10. In the definition ‘Director’, the word ‘Department’ shall immediately follow the wording ‘…Infrastructure Protection;…’

11. A new definition ‘Local Government’ shall be created as follows:

    “Local Government” includes the Regional Councils only;

12. A new definition ‘legitimate access seekers’ shall be created as follows:

    “legitimate access seekers” means any person making a request in accordance with national or Union law. They can include authorities that are competent under this order and those that are competent under national law or Union law for the prevention, investigation, detection or prosecution of criminal offences, and CERTs or CSIRTs;

13. A new definition ‘management body’ shall be created as follows:

    “management body” shall include the head of the essential and important entity and any other officers appointed by the head for the purpose of carrying out sub-article 19(1) of this order.

14. In the definition ‘operator security plan’ the word ‘is’ shall be replaced by the word ‘means’.

15. A new definition ‘person’ shall be created as follows:

    “person” means a person as defined in article 4 of the Interpretation Act;

16. A new definition ‘significant incident’ shall be created as follows:

    “significant incident” means an incident which:

    (a) has caused or is capable of causing severe operational disruption of the service or financial loss for the entity concerned:

    (b) has affected or is capable of affecting other persons by causing considerable material or non-material damage;

17. A new definition ‘traffic light protocol’ shall be created as follows:

    “traffic light protocol” means the provision of information about any limitations with regard to the further spreading of information. It is used in almost all computer security incident response teams (CSIRTs) and in some information analysis and sharing centres.

18. The definition ‘trust service’ shall be amended as follows:

    “trust service” means a trust service as defined in article 3(16) of the Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework);

19. The definition ‘trust service providers’ shall be amended as follows:

    “trust service provider” means a trust service provider as defined in article 3(19), Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework;

Article 4 – Applicability

20. In sub-article 4(1), the wording ‘the Companies Act’ shall be replaced with the wording ‘Recommendation 2003/361/EC’.

21. Sub-article 4(2) shall be amended as follows:

    (2) Article 3(4) of the Annex to that Recommendation shall not apply for the purposes of this order.

22. In sub-article 4(3)((f)(ii) the word ‘regional’ shall be replaced with the wording ‘local government’.

23. Sub-article 4(6) is to be deleted.

Article 5 – Essential and important entities.

24. Sub-article 5(1)(a) shall be amended as follows:

    (a) entities of a type in the First Schedule which exceed the ceilings for medium-sized enterprises provided for under article 2(1) of the Annex to Recommendation 2003/361/EC;

25. Sub-article 5(1)(c) shall be amended as follows:

    (c) providers of public electronic communications networks or of publicly available electronic communications services which qualify as medium-sized enterprises under article 2 of the Annex to Recommendation 2003/361/EC;

PART II – CRITICAL INFRASTRUCTURE PROTECTION ADVISORY BOARD, CRITICAL INFRASTRUCTURE PROTECTION DEPARTMENT and CSIRTMalta

Article 6 – Critical Infrastructure Protection Advisory Board

26. Sub-article 6(1)(d) shall be amended as follows:

    (d) a secretary who shall be a public official from within the ministry responsible for critical infrastructure protection, but who shall not have any voting rights.

    Provided that a lawyer shall not be qualified to act as a Chairperson to the Advisory Board unless he has practised as an advocate in Malta for a period of, or periods amounting in the aggregate to, not less than seven years.

    Provided further that a person appointed in terms of sub-articles (b) and (c) shall have at least four (4) years of experience.

27. In sub-article 6(11), the word 'or advisers' shall be deleted.

Article 8 – Critical Infrastructure Protection Department

28. In sub-article 8(1)(i), the wording 'following areas within the' shall immediately precede the wording 'Digital Infrastructure'.

29. Sub-article 8(2) shall be amended as follows:

    Unless otherwise expressly provided in this order or any other law, and unless another designated competent authority is responsible for the sector, subsector or type of entity in the First or Second Schedule, the Malta CIP Department shall be responsible for:

30. Sub-article 8(2)(e) shall be amended as follows:

    (e) ensuring that operator security plans, business continuity plans, and, where necessary, termination plans are drawn up and maintained by essential and important entities;

31. Sub-article 8(2)(j) shall be amended to as follows:

    (j) adopting a strategy on the security of network and information systems, under the national cybersecurity strategy pursuant to article 16;

32. The provision of sub-article 8(2) shall be amended as follows:

Provided that in accordance with article 47(1) of Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011, the Malta Financial Services Authority may participate in the activities of the Cooperation Group for matters that concern its supervisory activities in relation to financial entities.

Provided that the Malta Financial Services Authority may request the Malta CIP Department, to participate in the activities of the Cooperation Group for matters pertaining to essential or important entities, subject to such entities having been designated under this order as critical ICT third-party service providers pursuant to Article 31 of that Regulation.

33. Sub-article 8(3)(b) shall be amended as follows:

(b) the name of the CSIRT providing monitoring services to the entity and whether it is an internal or autonomous CSIRT;

34. A new sub-article 8(6) shall be inserted as follows:

(6) The Director shall represent the Malta CIP Department in any judicial proceedings.

35. Heading of article 11 shall be amended as follows:

Tasks of CSIRTMalta and internal and autonomous CSIRTs.

36. Sub-article 11(2) shall be amended as follows:

(2) Internal and autonomous CSIRTs shall have at least the following tasks:

(a) monitoring and analysing cyber threats, vulnerabilities and incidents of the essential and important entities and providing real-time or near real-time monitoring of their network and information systems;

(b) providing early warnings, alerts, announcements and dissemination of information on cyber threats, vulnerabilities and incidents, if possible in near real-time to the essential and important entities;

(c) responding to incidents and providing assistance to the essential and important entities;

(d) collecting and analysing forensic data and providing dynamic risk and incident analysis and situational awareness regarding cybersecurity of the essential and important entities;

(e) providing, a proactive scanning of the network and information systems of the essential and important entities to detect vulnerabilities with a potential significant impact.

Provided that the tasks in sub-article (2) shall be carried out by internal and autonomous CSIRTs providing CSIRT monitoring services to essential and important entities in terms of sub-article 20(1)(d).

37. A new proviso shall be added to sub-article 11(3) as follows:

Provided that the essential and important entities shall be notified in writing of the proactive, non-intrusive scanning of their publicly accessible network and information systems, and following such scanning, shall be notified in writing of any vulnerable or insecurely configured network and information systems.

38. Sub-article 13(5)(a) shall be amended as follows:

(a) the Malta Communications Authority under the Electronic Communications (Regulations) Act and the Electronic Commerce Act; and

39. The heading of article 15 shall be amended as follows:

Article 15 - Qualified auditors.

40. Article 15 shall be amended as follows:

15. (1) An essential or important entity shall appoint a qualified auditor which shall verify if the entity has implemented the cybersecurity risk-management measures under article 20.

Provided that the qualified auditor shall satisfy the requirements under sub-article (4) before being appointed.

Provided further that if the qualified auditor satisfies the requirements under sub-article (4), the appointment must be approved by the Malta CIP Department, or where designated the competent authority.

(2) If the qualified auditor is unable to verify whether the essential or important entity has implemented the cybersecurity risk-management measures under article 20, he shall notify this in writing to the essential or important entity and the Malta CIP Department, or where designated the competent authority.

(3) The Malta CIP Department, or where designated the competent authority, shall ensure that the essential or important entity takes, without undue delay, all necessary, appropriate and proportionate corrective measures.

(4) The Malta CIP Department, or where designated the competent authority, shall approve an appointment pursuant to sub-article (1), if the qualified auditor submits a reasoned request with accompanying documentation to the Malta CIP Department, or where designated the competent authority, demonstrating that he is:

(a) in possession of a background check issued by the competent authority under the Resilience of Critical Entities & Infrastructures (Identification, Designation and Protection) Order; or

(b) in possession of a valid European and, or international cybersecurity certification or cybersecurity standard; or

(c) experience and skillset as determined by the Malta CIP Department.

Provided that in the case of essential entities, the qualified auditor shall satisfy all of the above requirements.

(5) The Malta CIP Department shall maintain a list of qualified auditors and make this list available to essential and important entities.

(6) The Malta CIP Department shall lay down the procedure for the approval of the qualified auditor under sub-article (1).

PART III – NATIONAL CYBERSECURITY STRATEGY

Article 16 - National cybersecurity strategy.

41. Sub-article 16(1) shall be amended as follows:

    16. (1) The National Cyber Security Steering Committee shall oversee the national cybersecurity strategy that lays down the strategic objectives, the resources required to achieve those objectives and policy and regulatory measures with a view to achieving and maintaining a high level of cybersecurity in Malta.

Article 17 – National cyber crisis management framework.

42. In sub-article 17(1) the wording 'or in one or more Member States' shall be deleted.

43. A new sub-article 17(2) is to be created following sub-article 17(1)(b).

Article 18 – Peer reviews.

44. Sub-article 18(1) shall be amended as follows:

    18. (1) Prior to a commencement of a peer review on Malta, a self-assessment of the reviewed aspects may be carried out by the Malta CIP Department in cooperation with CSIRTMalta, designated competent entities and other entities and stakeholders where necessary and as appropriate. The Department shall provide that self-assessment to the designated cybersecurity experts in accordance with article 19 of the Directive.

45. Sub-article 18(2) shall be deleted.

PART IV – CYBERSECURITY RISK-MANAGEMENT MEASURES AND REPORTING OBLIGATIONS

Article 19 - Governance.

46. Sub-article 19(1) shall be amended as follows:

    19. (1) The Malta CIP Department, or where designated the competent authority, shall ensure that management bodies of such essential and important entities approve the cybersecurity risk-management measures pursuant to article 20 and oversee their implementation. The natural persons composing the management bodies may be held liable for infringements by the aforesaid entities of that article in accordance with sub-articles 32(10)(b) and 34.

47. The proviso to sub-article 19(1) shall be deleted.

Article 20 - Cybersecurity risk-management measures.

48. Sub-article 20(1)(c)(i) shall be amended as follows:

    (i) facilitate the development, implementation, maintenance and review of business continuity plans and where necessary termination plans that include the preparedness, processes and solutions of the essential or important entity;

49. A new sub-article 20(2)(l) shall be created as follows:

    (l) termination plans, where necessary.

Article 21 – Reporting obligations.

50. In sub-article 21(1), the wording 'immediately' shall immediately precede the wording '…notify CSIRTMalta of any incident…'.

51. In the second proviso of sub-article 21(1), the wording 'or authorities as the case may be' shall immediately precede the wording '…of any incident that has a significant impact…'.

52. In sub-article 21(6), the wording '(6)(b)' shall be replaced with '(5)(b)'.

53. In sub-article 21(7), the wording '(6)(a)' shall be replaced with (5)(a)'

54. In sub-article 21(8), the word 'designated' shall immediately precede the wording '…competent authority in cooperation with CSIRTMalta.

55. In sub-article 21(9) the word 'of' shall be deleted and the word 'offence' shall replace the word 'nature.

Article 22 - Use of European cybersecurity certification schemes.

56. A new first proviso shall be inserted in sub-article 22(1) as follows:

    Provided that the Department, or where designated the competent authority, shall require, where applicable, essential and important entities to use such ICT products, ICT services and ICT processes.

PART V – JURISDICTION AND REGISTRATION

Article 25 – Registry of entities.

57. A new proviso shall be added to sub-article 25(2) as follows:

    Provided that the entity shall provide information under sub-article (1)(g) to the Malta CIP Department upon request.

Article 26 – Database of domain name registration data.

58. In sub-article 26(2), the wording 'for legitimate seekers' shall immediately precede '…to identify and contact the holders of the domain names…'.

59. A new proviso shall be inserted in sub-article 26(5) as follows:

    Provided that domain name registration data shall be free of charge to legitimate access seekers upon lawful and duly substantiated requests.

PART VI – INFORMATION SHARING

Article 27 – Cybersecurity information-sharing arrangements.

60. In sub-article 27(1), the wording 'in collaboration with other entities and stakeholders,' shall be deleted.

61. In sub-article 27(2), the wording 'in collaboration with other entities and stakeholders,' shall be deleted.

62. In sub-article 27(3), the wording 'in collaboration with other entities and stakeholders,' shall be deleted.

Article 28 – Voluntary notification of relevant information.

63. Sub-article 28(1) shall be amended as follows:

28. (1) In addition to the notification obligation provided for in article 21, notifications may be submitted to CSIRTMalta on a voluntary basis, by:

64. Sub-article 28(3) shall be amended as follows:

(3) Where applicable, CSIRTMalta shall provide the Malta CIP Department and where designated the competent authority, with the information about notifications received pursuant to this article, while ensuring the confidentiality and appropriate protection of the information provided by the notifying entity.

PART VII – SUPERVISION AND ENFORCEMENT

Article 29 – General aspects concerning supervision and enforcement.

65. In sub-article 29(3) the word 'Directorate' shall be replaced by the word 'Malta CIP Department'.

Article 30 – Supervisory and enforcement measures in relation to essential entities.

66. In sub-article 30(2)(b) the wording 'audit firm' shall be replaced by the wording 'independent body'.

67. In sub-article 30(2)(g) the wording 'audit firm' shall be replaced by the wording 'qualified auditor'.

68. Sub-article 30(2)(j) shall be amended as follows:

(j) requests for evidence of operator security plans, business continuity plans and where necessary termination plans;

69. Sub-article 30(2)(k) shall be amended as follows:

(k) any other supervisory measures which the Malta CIP Department, or where designated the competent authority shall consider necessary in accordance with its powers at law.

70. Sub-article 30(4) shall be amended as follows:

(4) The results of any targeted security audit in sub-articles (2)(b) and (3), shall be made available to the Malta CIP Department, or where designated the competent authority. The costs of such targeted security audit carried out by an independent body shall be paid by the audited essential entity, except in duly substantiated cases when the Malta CIP Department, or where designated the competent authority shall decide otherwise:

Provided that the Malta CIP Department shall establish the principles in relation to targeted security audits, which may qualify for an exception under this sub-article:

71. In the proviso to sub-article 30(4) the wording 'before the Administrative Review Tribunal' shall immediately follow the wording '…allocation of cost can be appealed'.

72. In sub-article 30(6)(k) the wording 'in accordance with its powers at law' shall immediately follow the wording '…competent authority considers necessary.'

Article 31 - Supervisory and enforcement measures in relation to important entities.

73. In sub-article 31(2)(b) the wording 'audit firm' shall be replaced with the wording 'independent body'.

74. In sub-article 31(2)(f) the wording 'audit firm' shall be replaced with the wording 'qualified auditor'.

75. Sub-article 31(2)(j) shall be amended as follows:

    (j) requests for evidence of operator security plans, business continuity plans and where necessary termination plans;

76. In sub-article 31(2)(k) the wording 'in accordance with its powers at law' shall immediately follow '…competent authority considers necessary.'

77. In sub-article 31(4) the wording 'audit firm' shall be replaced with the wording 'independent body'.

78. In the proviso to sub-article 31(4) the wording 'before the Administrative Review Tribunal' shall immediately follow the wording '…allocation of cost can be appealed'.

79. In sub-article 31(6)(j) the wording 'in accordance with its powers at law' shall immediately follow the wording '…competent authority considers necessary.'

Article 32 - Proceedings for the imposition of enforcement measures.

80. In sub-article 32(10)(b) the wording ', courts or tribunals' shall immediately follow the wording '…certification or authorisation body'.

Article 34 - Recommendations by the Advisory Board on the imposition of administrative fines.

81. The proviso in sub-article 34(2) shall be amended as follows:

    Provided that the Advisory Board may, if it deems necessary, ask for more information or documentation from the Malta CIP Department.

Article 35 – Sworn application for the imposition of an administrative fine.

82. In sub-article 35(1), the wording '32(2)(i)' shall be replaced by the wording '30(7) or 31(7)'.

Article 39 – Daily administrative fine payments.

83. Sub-article 39(1) shall be amended as follows:

    (1) The Malta CIP Department, or where designated the competent authority, may request the imposition by the Civil Court of daily administrative penalty payments for each infringement which the essential or important entity concerned repeatedly fails to cease and, or rectify, in accordance with a prior decision of the Malta CIP Department, or where designated the competent authority.

Article 40 – Mutual assistance.

84. A new second proviso shall be added to sub-article 40(1)(b) as follows:

    Provided further that if the Malta CIP Department is not responsible for the sector, sub-sector, or type of entity under the First or Second Schedule, the Department shall cooperate with and coordinate measures arising from this sub-article with the designated competent authority in Malta.

85. In sub-article 40(3), the wording ', or the designated competent authority' shall immediately precede the wording '…shall not refuse the request…'.

86. In sub-article 40(3)(c), the word ', or the designated competent authority' shall immediately precede the wording '…shall consult the other competent authorities…'.

87. A new second proviso shall be added to sub-article 40(3) as follows:

Provided further that notification of such a request to the competent authority of the other Member State shall be done by the Malta CIP Department.

88. In sub-article 40(4), the wording ‘, or the designated competent authority’ shall be immediately precede the wording ‘…may carry out joint supervisory actions…’.

89. In the proviso to sub-article 40(4), the wording ‘, or the designated competent authority’ shall be immediately precede the wording ‘…may, where appropriate, confer powers…’.

90. A new second provision shall be added to sub-article 40(4) as follows:

Provided further that the joint supervisory actions shall be coordinated by the Malta CIP Department.

Implementation

9. When you intend to implement the decisions

Government entities intend to implement the decisions upon Cabinet approval.

Contact Details

If you have any questions regarding this response, please contact: nis2.consultation@gov.mt